Claude Carlet
Alexander Pott (Eds.)

Sequences and Their Applications – SETA 2010

LNCS 6338

6th International Conference
Paris, France, September 2010
Proceedings

Springer

Lecture Notes in Computer Science 6338

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Claude Carlet Alexander Pott (Eds.)

Sequences and Their Applications – SETA 2010

6th International Conference
Paris, France, September 13-17, 2010
Proceedings

Springer

Volume Editors

Claude Carlet
LAGA
Universities of Paris 8 and Paris 13
and CNRS, France
E-mail: claude.carlet@inria.fr

Alexander Pott
Institute for Algebra and Geometry
Otto-von-Guericke-University
Magdeburg, Germany
E-mail: alexander.pott@ovgu.de

Library of Congress Control Number: 2010934258

CR Subject Classification (1998): G.2, E.3, C.2, K.6.5, D.4.6, J.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-642-15873-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-15873-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

This volume contains the refereed proceedings of the *Sixth International Conference on Sequences and Their Applications (SETA 2010)*, held in Paris, France, September 13-17, 2010. The previous five conferences were held in Singapore (Republic of Singapore), Bergen (Norway), Seoul (South Korea), Beijing (China) and Lexington (USA). Topics of SETA include:

- Randomness of sequences
- Correlation (periodic and aperiodic types) and combinatorial aspects of sequences (difference sets)
- Sequences with applications in coding theory and cryptography
- Sequences over finite fields/rings/function fields
- Linear and nonlinear feedback shift register sequences
- Sequences for radar distance ranging, synchronization, identification, and hardware testing
- Sequences for wireless communication
- Pseudorandom sequence generators
- Boolean and vectorial functions for sequences, coding and/or cryptography
- Multidimensional sequences and their correlation properties
- Linear and nonlinear complexity of sequences

The Technical Program Committee of SETA 2010 refereed 56 submitted papers. Each paper was reviewed by at least 2 referees (at least 3 when an author was a TPC member) and the TPC selected 33 papers to be presented at the conference. In addition, we had 4 invited papers, by Robert Calderbank (Princeton University, USA), James Massey (retired from ETH Zurich, Switzerland), Jong-Seon No (Seoul National University, South Korea) and Arne Winterhof (Österreichische Akademie der Wissenschaften, Austria).

The Co-chairs of the TPC were Claude Carlet (Université Paris 8, France) and Alexander Pott (Otto-von-Guericke-Universität, Magdeburg, Germany). They wish to thank the other members of the Program Committee: Thierry P. Berger (Université de Limoges, France); Serdar Boztas (Royal Melbourne Institute of Technology, Australia); Lilya Budaghyan (University of Bergen, Norway); Pascale Charpin (INRIA, France) ; Gérard Cohen (Télécom ParisTech, France); Cunsheng Ding (Hong Kong University of Science and Technology, PR of China); Pingzhi Fan (Southwest Jiaotong University Chengdu, PR of China); Philippe Gaborit (Université de Limoges, France); Guang Gong (University of Waterloo, Canada); Tor Helleseth (University of Bergen, Norway); Jonathan Jedwab (Simon Fraser University, Canada); Thomas Johansson (Lund University, Sweden); Andrew Klapper (University of Kentucky, USA); Gohar Kyureghyan (Otto-von-Guericke-Universität, Germany); Gregor Leander (Technical University of Denmark); Wilfried Meidl (Sabanci University, Turkey); Sihem Mesnager (Université Paris 8, France); Gary McGuire (University College Dublin, Ireland);

Udaya Parampalli (University of Melbourne, Australia); Matthew Parker (University of Bergen, Norway); Bernhard Schmidt (Nanyang Technological University, Singapore, Republic of Singapore); Kai-Uwe Schmidt (Simon Fraser University, Canada); Hong-Yeop Song (Yonsei University, Korea); Kyeongcheol Yang (Pohang University of Science and Technology, Korea) and Nam Yul Yu (Lakehead University, Canada).

The editors are also grateful to Nina Brandstätter, Yuqing Chen, Jin-Ho Chung, Gary Greenfield, Yun Kyoung Han, Kathy Horadam, Honggang Hu, Ramakanth Kavuluru, Alexander Kholosha, Mels Kyuregyan, Petr Lisonek, Wai Ho Mow, Asha Rao, Xiaohu Tang, Andrew Turpin, Huaxiong Wang, Ruizhong Wei, Tony Wirth and Zhengchun Zhou for their help and assistance in the reviewing of papers.

We thank Springer for financing the best paper award, given by the Journal *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences* (CCDS) and awarded to the paper "Appended m-Sequences with Merit Factor Greater Than 3.34", by Jonathan Jedwab and Kai-Uwe Schmidt.

We wish to thank Patrick Solé for his support as General Chair, Jean-Claude Belfiore for handling the EasyChair system, the webmaster Stephane Boucart, and Valérie Alidor, Nicolas Beaude (SEE), Danielle Childz, Zouina Sahnoune and Bruno Thedrez (Télécom ParisTech) for their kind help. Finally we would like to thank Télécom ParisTech for hosting the conference and Digiteo, CNRS and LAGA for their financial support.

September 2010

Claude Carlet
Alexander Pott

Table of Contents

Linear Complexity

Finite Fields

Character Sums

Merit Factor

FCSR

Hadamard Matrices and Transforms

Cryptography

Invited Paper

Statistical Analysis

Boolean Functions and Related Problems

Nonbinary Sequences

Infinite Sequences

Invited Paper

Low Correlation Zone Sequences
(Invited Paper)

Jung-Soo Chung and Jong-Seon No

Department of Electrical Engineering and Computer Science,
Institute of New Media and Communications,
Seoul National University, Seoul 151-744, Korea
integer@ccl.snu.ac.kr, jsno@snu.ac.kr

Abstract. It is well known that low correlation zone sequences have been adopted as spreading sequences in the quasi-synchronous code division multiple access (QS-CDMA) systems of wireless communication systems, where time delay among different users is allowed to be within a few chips. In this paper, numerical analysis shows that the QS-CDMA systems using low correlation zone (LCZ) sequences outperform the conventional code division multiple access (CDMA) systems. Also, several LCZ sequences are revisited and a new extension method for the construction of LCZ sequences is proposed.

Keywords: Autocorrelation, Code division multiple access (CDMA), Cross-correlation, Low correlation zone (LCZ) sequence, Pseudo noise (PN) sequence, Quasi-synchronous code division multiple access (QS-CDMA) system, Spreading sequence.

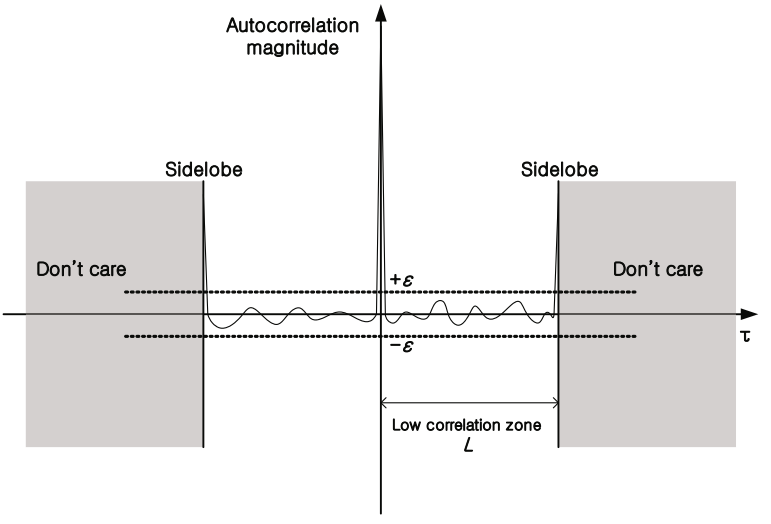
1 Introduction

Spread spectrum communication systems such as direct sequence code division multiple access (CDMA) communication systems require each signal to be easily distinguished from a time shifted version of itself or from the other signals in the signal set. In order to satisfy these requirements, pseudo noise (PN) sequences with good correlation property have been used as spreading sequences in the CDMA communication systems. In CDMA communication systems, many users can share frequency spectrum and time using spreading sequences with good correlation property such as the Gold sequences. The Gold sequence set are optimal with respect to the Sidel'nikov bound in the sense that the maximum magnitude of correlation values achieves theoretical lower bound for a given set size and period [28]. This lower bound is approximately equal to the square root of twice the period of sequences. Thus, even though the sequence set is optimal, the autocorrelation and the cross-correlation values have relatively large magnitude. Therefore, considerable amount of multiple access interference (MAI) could be introduced even though the optimal sequence set is used in the CDMA systems.

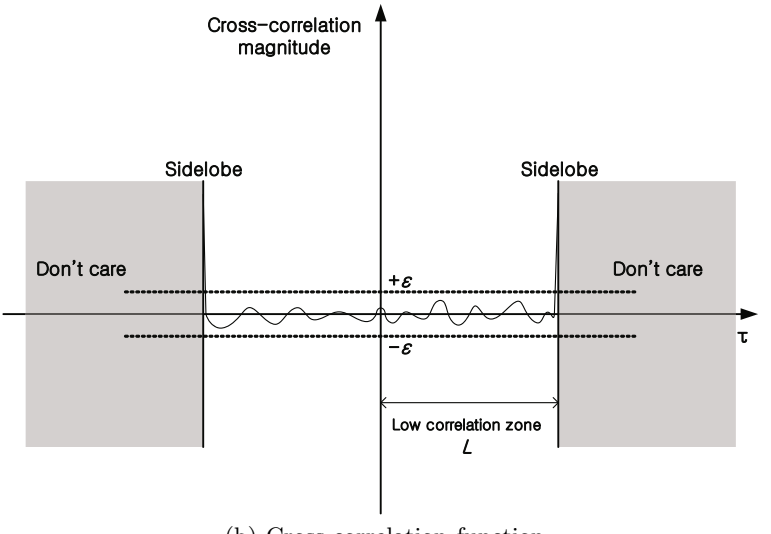
C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 1–29, 2010.

In the reverse link of CDMA systems in the cellular communication systems, synchronization within a few chips can be maintained due to the relatively small transmission delay, in which spreading sequences with good correlation property around the origin are needed. Specially, in the microcellular, femtocell, or indoor environments, where the cell size is very small, transmission delays are relatively small and thus, it may be feasible to maintain synchronization within a chip or a few chips in the reverse link. Gaudenzi, Elia, and Viola proposed quasi-synchronous code division multiple access (QS-CDMA) systems [5]. In such systems, the time delay is allowed to be within a few chips among different users, which gives more capacity and flexibility in designing wireless communication systems.

In the design of sequence sets for QS-CDMA systems, what matters most is to have a low correlation zone (LCZ) around the origin rather than to minimize the overall maximum nontrivial correlation value [32]. Fig. 1 shows the correlation functions of LCZ sequences. Long, Zhang, and Hu proposed sequence sets that have low-correlation values around the origin, which can be used as spreading sequences in the QS-CDMA systems [32]. A sequence set with this property is called an LCZ sequence set. They also have shown that LCZ sequence sets have better performance than other well-known sequence sets with optimal correlation property in the wireless communication systems with a few chip delay among different users [32]. For a prime p, Tang and Fan [42] proposed p-ary LCZ sequence sets by extending the alphabet size of each sequence in Long's work. Kim, Jang, No, and Chung proposed a new construction method of quaternary LCZ sequence sets by using a binary sequence of the same period with ideal autocorrelation, and they also calculated the correlation distributions of their sequence sets constructed from an m-sequence or a GMW sequence [20]. Their quaternary LCZ sequence sets are optimal with respect to the bound by Tang, Fan, and Matsufuji [43]. For zero correlation zone (ZCZ) sequence sets with zero correlation values around the origin, Wang and Qi proposed the concept of D-matrix. Using interleaved structure and D-matrix, they calculated the ZCZ length of the interleaved ZCZ sequence sets [47]. Kim, Jang, No, and Chung proposed several new construction methods of LCZ sequence sets [23]. In their design scheme of the binary LCZ sequence sets, the LCZ length can be freely selected and the resulting LCZ sequence sets have the set sizes that are almost optimal with respect to Tang, Fan, and Matsufuji bound. Using interleaving techniques, Hu and Gong presented a construction of sequence sets with zero or low correlation zone using interleaving techniques and complex Hadamard matrices [11]. Jang, No, Chung, and Tang constructed the optimal p-ary LCZ sequence sets [18] and a construction method of $p^n \times p^n$ p-ary Hadamard matrices from the optimal LCZ sequence sets is proposed. Jang, No, and Chung proposed a new construction method for Butson Hadamard matrices from the optimal balanced LCZ sequence set which has a correlation value of -1 within LCZ [17]. Jang, No, and Chung [16] also found a new construction method of the optimal p^2-ary LCZ sequence sets using unified sequences [34]. Yang, Jin, Song, No, and



(a) Autocorrelation function



(b) Cross-correlation function

Fig. 1. Correlation functions of LCZ sequences

Shin proposed multicode multiple-input multiple-output (MIMO) systems with quaternary LCZ and ZCZ sequences as spreading codes [49].

This paper is organized as follows. In Section 2, PN sequences are presented. The CDMA and QS-CDMA systems are described in Section 3. Construction and extension methods for LCZ sequence sets are proposed in Section 4. Finally, the conclusion is given in Section 5.

2 PN Sequences

PN sequences have been used in various wireless communication systems, in which the individual sequences and sets of PN sequences with good correlation property play an important role. In the CDMA communication systems such as the second generation and the third generation wireless communication systems, they are usually employed as signature sequences in order to distinguish each user. The PN sequences with good correlation property can minimize other user interference in the multiuser environments of CDMA communication systems. PN sequences have been also used in the radar and sonar systems. In the area of cryptography, the PN sequences have been adopted as a key stream in the stream cipher, a session key generator, various functions in the block cipher, a digital water mark, and a random number generator in the digital signature standard.

Researches on the PN sequences can be categorized into two parts. One is research on the sequences with good autocorrelation property, which can make a sequence easily distinguishable from its shifted version. The other is research on the sets of sequences with low autocorrelation and cross-correlation. It is desirable for a set of sequences to have the properties of low cross-correlation between sequences in a set as well as low out-of-phase autocorrelation.

There are many desirable properties for PN sequences such as low correlation, large linear span, balance, and randomness. One of the most important properties of the PN sequences in the application of CDMA communication systems is low correlation. For a q-ary sequence $s_u(t)$ of period N, the autocorrelation function $R_u(\tau)$ is defined as

$$R_u(\tau) = \sum_{t=0}^{N-1} \omega_q^{s_u(t+\tau)-s_u(t)}, \quad 0 \le \tau \le N-1$$

where $\omega_q = e^{j2\pi/q}$ and $j = \sqrt{-1}$. For two q-ary sequences $s_u(t)$ and $s_v(t)$ of period N, the cross-correlation function $R_{u,v}(\tau)$ of $s_u(t)$ and $s_v(t)$ is defined as

$$R_{u,v}(\tau) = \sum_{t=0}^{N-1} \omega_q^{s_u(t+\tau)-s_v(t)}. \tag{1}$$

For a q-ary sequence set S, the maximum magnitude of correlation functions can be defined as

$$R_{\max} = \max\{\left|R_{u,v}(\tau)\right| | s_u(t), s_v(t) \in S, 0 \le \tau \le N-1, \text{ except } u = v \text{ and } \tau = 0\}.$$

Most of the researches on the PN sequences have been done on the binary case ($q = 2$) because wireless communication systems have used binary signaling systems as their modulation schemes. With the growing need for high-speed data communications, which usually adopt q-ary modulation schemes, it becomes more important to find q-ary sequences with good correlation property and q-ary codes with good error correctability.

There are lots of research results on the sequences with low autocorrelation property. The m-sequences [10,39] and GMW sequences [1,7,40] are well-known sequences with ideal autocorrelation property, which exist for binary and p-ary cases. Some of the binary sequences with ideal autocorrelation property are constructed from power residues. For example, Legendre sequences and Hall's sextic residue sequences are constructed from quadratic and sextic residues of integer ring [8], respectively.

The other research areas on the sequences are the construction of the sets of sequences with low correlation. The low correlation property makes each sequence to be easily distinguished from the other sequences in the set. Low cross-correlation of the sequence sets is the most important property of the CDMA systems as well as the simultaneous ranging of several targets. There are several bounds on the correlation values of the sets of sequences introduced by Welch [48], Sidel'nikov [41], and Levenshtein [30].

In 1966, Kasami [24,25] proposed a set of binary sequences that is optimal with respect to the Welch bound [48]. Although the maximum magnitude of cross-correlation values of Kasami sequences is optimal, their set size is very small relative to their period. At the cost of the optimal correlation, the set size of Kasami sequences can be extended to a large set of Kasami sequences. Liu and Komo [31] introduced the p-ary Kasami sequences by generalizing their alphabet size.

In 1968, Gold [6] constructed a set of binary sequences of period $2^n - 1$. This sequence set is optimal with respect to Sidel'nikov bound for an odd integer n but has short linear complexity. In 1994, Boztas and Kumar [2] presented the Gold-like sequence sets, which are identical to the Gold sequence sets in terms of the set size, the maximum correlation value, and the range of symbol imbalance, but have larger linear complexity. Later, Kim and No [21] constructed two sets of binary sequences with low correlation by generalizing the set of Gold-like sequences and the sequence set by Udaya [46].

In 1970, for an odd integer n and an odd prime p, Trachtenberg [45] constructed the set of p-ary sequences using the p-ary m-sequences and their decimated sequences by $d = p^{2k} - p^k + 1$ or $d = (p^{2k} + 1)/2$, which is relatively prime to its period $p^n - 1$. This set of p-ary sequences has the maximum magnitude $\sqrt{p^{n+e}}$ of correlation values, where $e = \gcd(n, k)$.

Table 1. Parameters of some known sets of sequences

Set of sequences	Alphabet	Period N	Set size	$R_{\max}$
Kasami [24]–[31]	p	$p^n - 1$	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Gold (n odd) [6]	2	$2^n - 1$	$N+2$	$\sqrt{2(N+1)}+1$
Gold (n even) [6]	2	$2^n - 1$	$N+2$	$2\sqrt{(N+1)}+1$
Trachtenberg [45]	odd p	$p^n - 1$	$N+1$	$\sqrt{p(N+1)}+1$
Sidel'nikov [41]	odd p	$p^n - 1$	$N+1$	$\sqrt{N+1}+1$
$A = S(0)$ [27]	4	$2^n - 1$	$N+2$	$\sqrt{N+1}+1$
$S(1)$ [27]	4	$2^n - 1$	$\geq N^2 + 3N + 2$	$2\sqrt{N+1}+1$
$S(2)$ [27]	4	$2^n - 1$	$\geq N^3 + 4N^2 + 5N + 2$	$4\sqrt{N+1}+1$

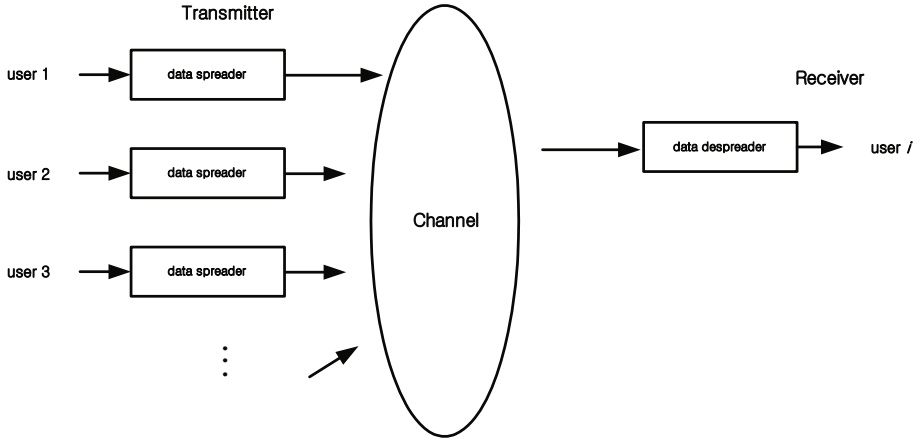


Fig. 2. Code division multiple access communication systems

For an alphabet size other than prime, Boztas, Hammons, and Kumar [3] proposed quaternary sequence sets with near-optimum cross-correlation property. And Kumar, Helleseth, Calderbank, and Hammons [27] constructed the large sets of quaternary sequences with low cross-correlation. These sequences have relatively large magnitude of out-of-phase autocorrelation values, but low cross-correlation values. Table 1 summarizes some known sets of sequences with low correlation.

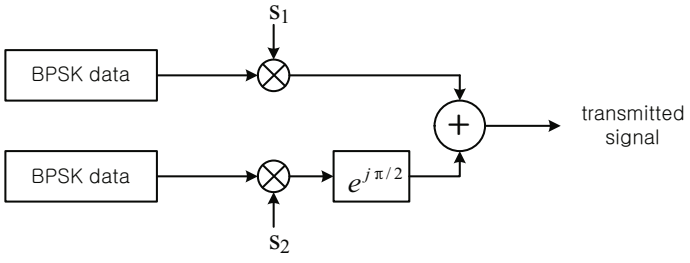
3 CDMA and QS-CDMA Systems

3.1 CDMA Systems

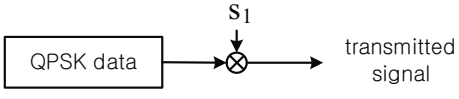
In the CDMA systems, many users can share the radio resources using PN sequences with good correlation property such as the sets of Gold sequences and Kasami sequences. Fig. 2 shows CDMA communication systems, where the data is multiplied by spreading sequences and then transmitted through the channel. We assume that the data of each user is asynchronously transmitted and that the signal power is the same. Fig. 3 shows data spreaders for binary and quaternary cases.

We consider a CDMA system with U users. Let $m_u(i)$ be a message data and $s_u(k)$ be a spreading sequence of period N. Then the spreaded signals for U users are given as

$$\begin{aligned} x_1(l = iN + k) &= m_1(i) \cdot s_1(k) \\ x_2(l = iN + k) &= m_2(i) \cdot s_2(k) \\ &\vdots \\ x_U(l = iN + k) &= m_U(i) \cdot s_U(k). \end{aligned}$$



(a) Data spreader using binary sequence.



(b) Data spreader using quaternary sequence.

Fig. 3. Data spreader for CDMA systems

We assume the additive white Gaussian noise (AWGN) channel and quadrature phase shift keying (QPSK) modulation. Then, the received signal in the receiver 1 is given as

$$y_1(l = iN + k) = x_1(l) + \sum_{u=2}^{U} \theta_u \cdot x_u(l - \phi_u) + n(l)$$

where θ_u denotes the channel constant of each channel, ϕ_u denotes the time shift of each user, and $n(l)$ denotes the AWGN.

The i-th despreaded data of the user 1 is given as

$$\begin{aligned}\hat{m}_1(i) = \frac{1}{N} \sum_{l=iN}^{iN+N-1} y_1(l) s_1(l - iN)^* + \theta_2 \sum_{k=\phi_2}^{N-1} m_2(i) s_2(k) \\ + \theta_2 \sum_{k=0}^{\phi_2} m_2(i-1) s_2(k) + \cdots \\ = m_1(i) + I(i) + n'(i)\end{aligned}$$

where $s_1^*(k)$ denotes the complex conjugate of $s_1(k)$, $I(i)$ denotes the total interference, and $n'(i)$ denotes the despreaded noise.

No et al. compared the performance of CDMA communication systems using the sequence set A, Gold sequence set, and Kasami sequence set [37]. For the performance comparison of CDMA systems with various PN sequences, we assume:

- AWGN channel
- Asynchronous CDMA system

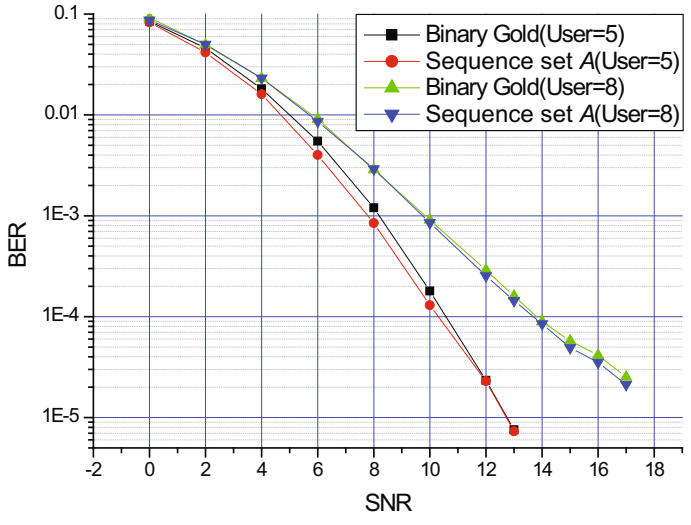


Fig. 4. Performance comparison of CDMA systems with sequence set A and Gold sequence set for 5 and 8 users with spreading factor 128 (No et al. [37])

- Packet size: 40 symbols
- Spreading sequences: sequence set A, Gold sequence set, Kasami sequence set
- Last symbol: zero padding
- Spreading factor: 128, 64
- One spreading sequence allocated to each user.

From Figs. 4 and 5, the CDMA systems with sequence set A have almost the same performance as those with Gold sequence set for spreading factor 128. Figs. 6 and 7 show that the CDMA systems with sequence set A also have almost the same performance as those with Gold sequence set and Kasami sequence set for spreading factor 64.

The $R_{\max}$ of the sequence set A is $\sqrt{N+1}+1$, but the $R_{\max}$ of the Gold sequence set is $\sqrt{2(N+1)}+1$ or $2\sqrt{N+1}+1$ in Table 1. In terms of $R_{\max}$, the sequence set A is better than the Gold sequence set by $\sqrt{2}$. But there is no significant performance difference between the CDMA systems with sequence set A and those with the Gold sequence set even though the improvement of $R_{\max}$ by $\sqrt{2}$ is significant in the sequence design . Therefore, we should find something more important than $R_{\max}$ for the CDMA communication systems.

3.2 QS-CDMA Systems

If the cell size is very small and thus transmission delay is relatively small, it is possible to maintain the time delay within a few chips in the asynchronous CDMA systems such as the reverse link of CDMA cellular systems, microcellular,

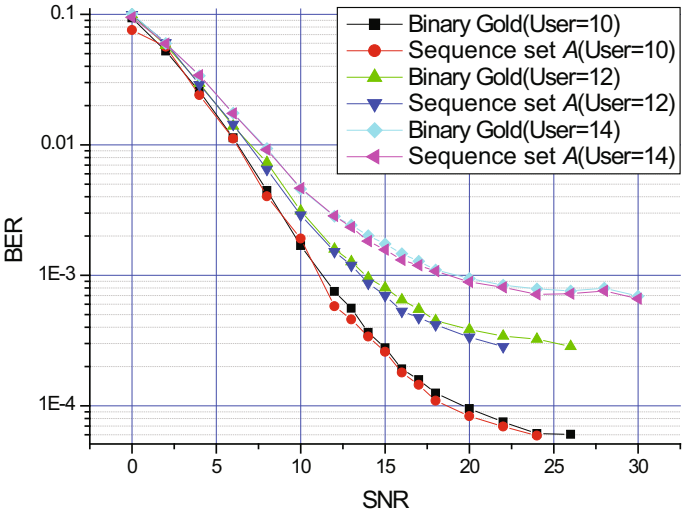


Fig. 5. Performance comparison of CDMA systems with sequence set A and Gold sequence set for 10 , 12, and 14 users with spreading factor 128 (No et al. [37])

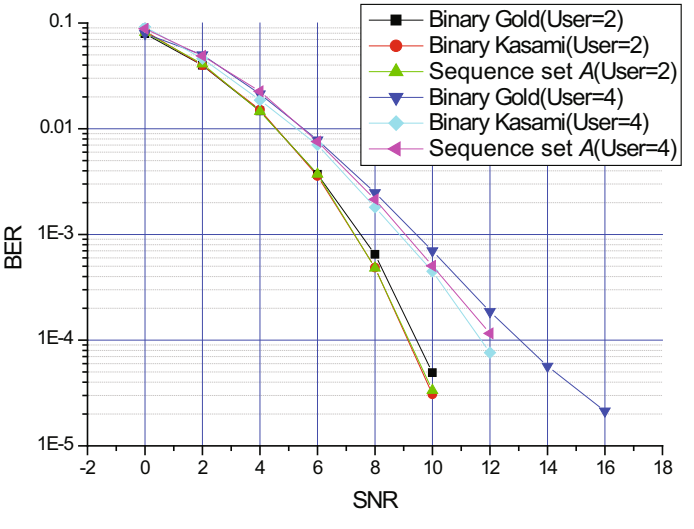


Fig. 6. Performance comparison of CDMA systems with sequence set A, Kasami sequence set, and Gold sequence set for 2 and 4 users with spreading factor 64 (No et al. [37])

femtocell, or indoor wireless communication systems. The QS-CDMA system can be a good candidate for such multiuser CDMA communication systems with a few chip delay among users. The QS-CDMA system was proposed by Gaudenzi, Elia, and Viola [5], where the design of spreading sequences can have more flexibility.

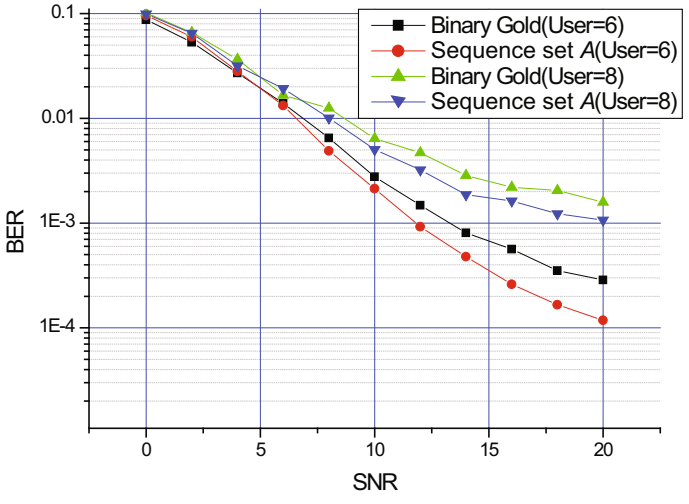


Fig. 7. Performance comparison of CDMA systems with sequence set A and Gold sequence set for 6 and 8 users with spreading factor 64 (No et al. [37])

Long, Zhang, and Hu proposed a system model of QS-CDMA using the sequence sets that have low-correlation values around the origin as spreading sequences, called LCZ sequences [32]. Let $m_u(t)$ and $s_u(t)$ be a data and a spreading sequence. Then, the received signal in the QS-CDMA systems with U users can be written as

$$r(t) = \sum_{u=1}^{U} \sqrt{2P} m_u(t - \tau_u) s_u(t - \tau_u) \cos(\omega_c t + \phi_u) + n(t)$$

where P is the signal power, ω_c is the carrier frequency, ϕ_u is the phase, τ_u is the time delay, and $n(t)$ is the white Gaussian noise with two-sided spectral density $N_0/2$. The spreading sequence $s_u(t)$ is a sequence of rectangular pulses with unit amplitude and chip period T_c and the data $m_u(t)$ is composed of the rectangular pulses with unit amplitude and symbol period T_b. Then, the spreading sequence $s_u(t)$ has period $N = T_b/T_c$.

Let $E_b = PT_b$ be the energy per bit and $m_{u,0}$ be the desired data of the user u in the decision internal $[0, T_b]$. Then the output data of the u-th user in the receiver can be written as

$$Z_u = \sqrt{P/2} T_b \left(m_{u,0} + \sum_{i=1, i \neq u}^{U} I_{i,u} + \eta \right)$$

where η denotes the zero mean Gaussian random variable with the variance $(2E_b/N_0)^{-1}$ and $\sum_{i \neq u} I_{i,u}$ denotes the MAI from the other users' interference.

From Gaussian approximation by Long, Zhang, and Hu [32], the variance of MAI depends on the cross-correlation functions of spreading sequences around the origin and the distribution of the time delay among users in the QS-CDMA system. They also showed that in the QS-CDMA systems, LCZ sequences as spreading sequences have better performance than other well-known sequence sets with optimal correlation property [32].

No and Jang also showed that the QS-CDMA systems using the LCZ sequences outperformed those using the conventional spreading sequences [35]. They assumed that the spreading factor is 256 and the time delay is maintained within 16 chips. And the additional channel coding was not used. According to the number of users, Figs. 8(a)–8(c) show BER performance of the QS-CDMA systems with LCZ sequence set, Kasami sequence set, and the sequence set A. They showed that the QS-CDMA systems with LCZ sequence set outperform those with Kasami sequence set or sequence set A. Fig. 9 shows that the QS-CDMA systems with LCZ sequences do not depend on MAI and that there is almost no deterioration as the number of users increases.

Yang, Jin, Song, No, and Shin proposed the multicode multiple-input multiple-output (MIMO) systems with quaternary LCZ and ZCZ sequences as spreading sequences [49] shown in Fig. 10, where $K = U$, $h_{ij}(t)$ denotes the channel gain, d_{ik} denotes the data, and $c_k(t)$ denotes the spreading sequences. The MIMO systems by Yang, Jin, Song, No, and Shin can be applied to the fourth generation wireless communication systems. Fig. 11 shows that the performance of the multicode MIMO systems with quaternary LCZ sequence set is better than that of the conventional multicode MIMO systems with quaternary spreading codes constructed from pairs of binary Hadamard codes.

Therefore, in the design of the set of spreading sequences for the QS-CDMA system, what matters most is to have a low correlation zone around the origin rather than to minimize the overall maximum nontrivial correlation value [32]. In fact, LCZ sequence sets with smaller correlation magnitude within the zone show better performance than other well-known sequence sets with optimal correlation property [32].

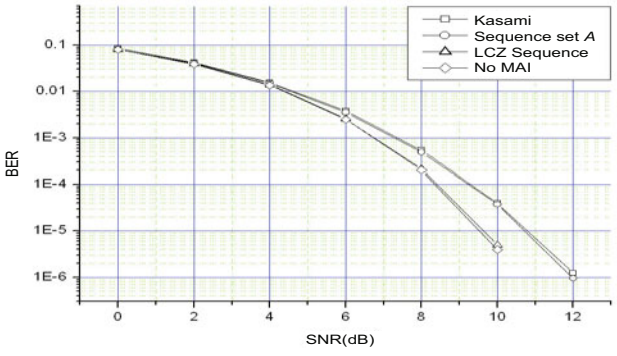
4 Construction of LCZ Sequences

Let $\mathcal{S}$ be a set of M sequences of period N. If the magnitude of correlation function between any two sequences in $\mathcal{S}$ takes the values less than or equal to ϵ within the range $-L < \tau < L$ of the offset τ, then $\mathcal{S}$ is called an (N, M, L, ϵ) LCZ sequence set. Let $\mathcal{S}$ be the q-ary LCZ sequence set with parameters (N, M, L, ϵ) given by

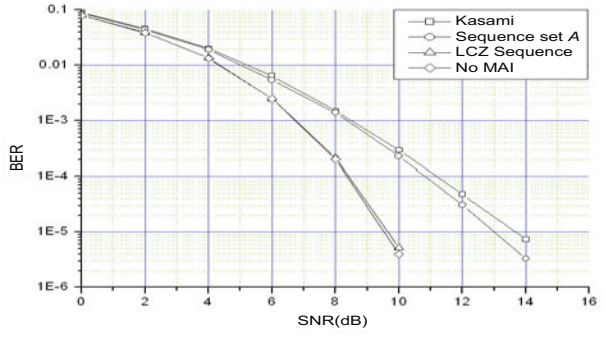
$$\mathcal{S} = \{f_l(t) \mid 0 \le l \le M-1,\ 0 \le t \le N-1\} \tag{2}$$

where L is the maximum value such that $|R_{i,j}(\tau)| \le \epsilon$ for all $0 \le i, j \le M-1$ and all $|\tau| < L$ except for the case of the inphase autocorrelation. When $\epsilon = 0$, $\mathcal{S}$ is called a q-ary ZCZ sequence set with parameters (N, M, L).

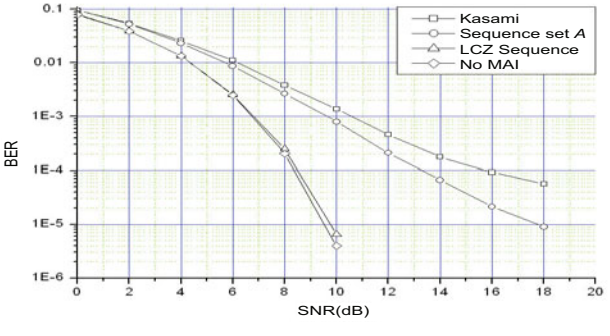
Tang, Fan, and Matsufuji derived a lower bound on LCZ sequence sets [43].



(a) 5 users.



(b) 10 users.



(c) 15 users.

Fig. 8. Performance comparison of the QS-CDMA systems (No and Jang [35])

Theorem 1 ([43]). *Let $\mathcal{S}$ be an LCZ sequence set with parameters (N, M, L, ϵ). Then, we have*

$$ML - 1 \leq \frac{N-1}{1-\epsilon^2/N}. \tag{3}$$

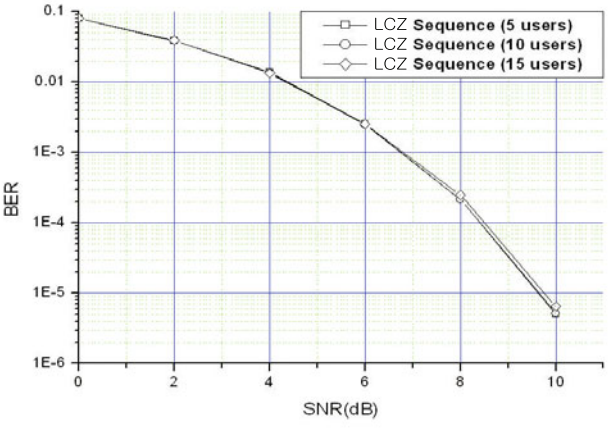


Fig. 9. BER of QS-CDMA systems using LCZ sequence set (No and Jang [35])

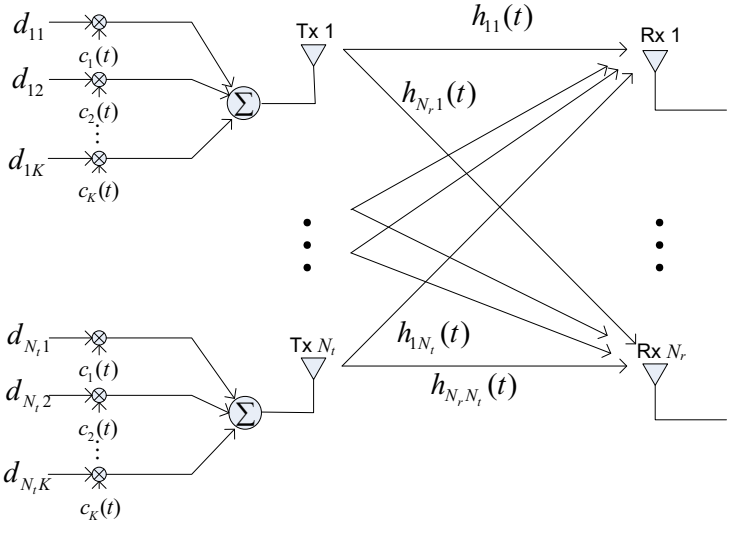


Fig. 10. Multicode MIMO system (Yang et al. [49])

For convenience, the construction of LCZ sequence sets can be classified into direct methods and extension methods. There are several optimal or almost optimal LCZ sequence sets with respect to the bound by Tang, Fan, and Matsufuji [43] constructed by the direct methods. The extension methods is composed of two different methods: the set size is kept unchangeable or the LCZ length is kept unchangeable or is slightly decreased.

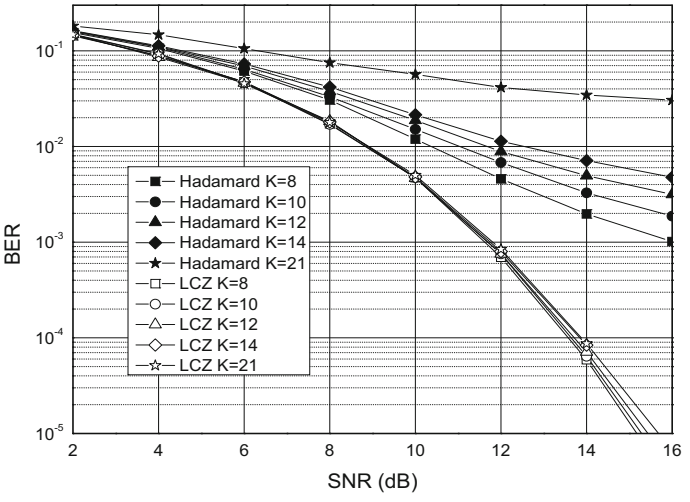


Fig. 11. 4×4 multicode MIMO systems with QPSK using LCZ sequence set with various K and $L = 3$ (Yang et al. [49])

4.1 Direct Methods of LCZ Sequence Sets

In this subsection, we will overview our new construction methods of LCZ sequence sets.

Construction 1 [20]:
The constructions of the quaternary LCZ sequence sets using the binary sequences with ideal autocorrelation of the same length are described in this construction.

In order to define m-sequences and GMW sequences, which have the ideal autocorrelation property, we will review the trace function over the finite field. Let F_{p^n} and F_{p^m} be the finite fields with p^n and p^m elements, respectively. The trace function $\mathrm{tr}_m^n(\cdot)$ is the mapping from F_{p^n} to F_{p^m} and is defined by

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

where $x \in F_{p^n}$ and $m|n$. Then, the trace function satisfies the following properties:

1. $\mathrm{tr}_m^n(x+y) = \mathrm{tr}_m^n(x) + \mathrm{tr}_m^n(y)$, for all $x, y \in F_{p^n}$;
2. $\mathrm{tr}_m^n(ax) = a\mathrm{tr}_m^n(x)$, for all $a \in F_{p^m}$, $x \in F_{p^n}$;
3. $\mathrm{tr}_m^n(x) = \mathrm{tr}_m^n(x^{p^{mi}})$, for all i and all $x \in F_{p^n}$;
4. $\mathrm{tr}_1^n(x) = \mathrm{tr}_1^m(\mathrm{tr}_m^n(x))$, for all $x \in F_{p^n}$.

Then, two constructions of quaternary LCZ sequence sets are given as in the following theorems:

Theorem 2 ([20]). *Let m and n be positive integers such that $m|n$. Let β be a primitive element in F_{2^m} and $T = (2^n-1)/(2^m-1)$. Let*

$$\mathcal{M} = \{s_i(x)|\ 0 \le i \le 2^m-2, x \in F_{2^n}^*\}$$

be the set of quaternary sequences defined by the functions

$$\begin{aligned} s_0(x) &= 2tr_1^n(x) \\ s_i(x) &= tr_1^n(x) \boxplus 2tr_1^n(\beta^i x),\ \text{for } 1 \le i \le 2^m-2 \end{aligned}$$

where $\boxplus$ denotes the addition in the ring $Z_4 = \{0,1,2,3\}$. Then, the set $\mathcal{M}$ is a $(2^n-1, 2^m-1, T, 1)$ quaternary LCZ sequence set and has the following correlation distribution:

$$R_{i,k}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{s_i(\delta x) - s_k(x)}$$

$$= \begin{cases} 2^n-1, & 2^m-1 \text{ times} \\ -1+j2^{n-1}, & (2^m-2)^2 \text{ times for } \delta \notin F_{2^m}\backslash F_2 \\ -1-j2^{n-1}, & (2^m-2)^2 \text{ times for } \delta \notin F_{2^m}\backslash F_2 \\ -1+2^{n-1}, & 2(2^m-2)(2^m-3) \text{ times for } \delta \notin F_{2^m}\backslash F_2 \\ 2^{n-1}-1+j2^{n-1}, & 2(2^m-2) \text{ times for } \delta \notin F_{2^m}\backslash F_2 \\ 2^{n-1}-1-j2^{n-1}, & 2(2^m-2) \text{ times for } \delta \notin F_{2^m}\backslash F_2 \\ -1, & \text{otherwise} \end{cases}$$

as δ varies over $F_{2^n}^*$ and $0 \le i,k \le 2^m-2$.

The set of quaternary LCZ sequences from GMW sequences can be also constructed by using the same method.

Theorem 3 ([20]). *Let m and n be positive integers such that $m|n$ and $T = (2^n-1)/(2^m-1)$. Let r be an integer such that $\gcd(r, 2^m-1) = 1$ and $1 \le r \le 2^m-2$. Let $g(x)$ be the GMW sequence defined by*

$$g(x) = \mathrm{tr}_1^m([\mathrm{tr}_m^n(x)]^r).$$

Let us define the set

$$\mathcal{G} = \{g_i(x)|\ 0 \le i \le 2^m-2,\ x \in F_{2^n}^*\}$$

of quaternary sequences defined by

$$\begin{aligned} g_0(x) &= 2\mathrm{tr}_1^m([\mathrm{tr}_m^n(x)]^r) \\ g_i(x) &= \mathrm{tr}_1^m([\mathrm{tr}_m^n(x)]^r) \boxplus 2\mathrm{tr}_1^m([\beta^i \mathrm{tr}_m^n(x)]^r),\ 1 \le i \le 2^m-2 \end{aligned}$$

where β is a primitive element in F_{2^m}. Then, $\mathcal{G}$ has the same correlation distribution as that of $\mathcal{M}$ and is a $(2^n-1, 2^m-1, T, 1)$ quaternary LCZ sequence set.

These quaternary LCZ sequence sets are constructed by using a binary sequence with ideal autocorrelation of the same period. These quaternary LCZ sequence sets are optimal with respect to the bound by Tang, Fan, and Matsufuji [43].

Construction 2 [23]:
In this construction, the construction method of binary LCZ sequence sets with flexible parameters is given.

Let $N = 2^{n+1} - 2$. Let Z_N be the set of integers modulo N, i.e., $Z_N = \{0, 1, \cdots, N-1\}$. Let $a(t)$ be a binary sequence of period $2^n - 1$ with ideal autocorrelation. Let D_u be the characteristic set of $a(t-u)$, i.e.,

$$D_u = \{t \mid a(t-u) = 1, 0 \le t \le 2^n - 2\} = D_0 + u$$

where $u \in Z_{2^n-1}$, $D_0 + u = \{d + u \mid d \in D_0\}$, and "+" means addition modulo $2^n - 1$. Let $\overline{D}_u = Z_{2^n-1} \backslash D_u$. From the balancedness of $a(t)$, we have

$$|D_u| = 2^{n-1}$$
$$|\overline{D}_u| = 2^{n-1} - 1.$$

From the difference-balance property of $a(t)$, for $u \neq v$, we have

$$|D_u \cap D_v| = 2^{n-2}$$
$$|D_u \cap \overline{D}_v| = 2^{n-2}$$
$$|\overline{D}_u \cap \overline{D}_v| = 2^{n-2} - 1.$$

By the Chinese remainder theorem, we have $Z_N \cong Z_2 \otimes Z_{2^n-1}$ under the isomorphism $\phi : w \mapsto (w \bmod 2, w \bmod 2^n - 1)$. In this construction, we use the notations $w \in Z_N$ and $(w \bmod 2, w \bmod 2^n - 1)$, interchangeably.

For $u \in Z_{2^n-1}$, let C_u be the subset of Z_N such that

$$C_u \cong \{0\} \otimes A_u \cup \{1\} \otimes D_{1-u} \tag{4}$$

where A_u can be either D_u or $\overline{D}_u$. Then we have

$$|C_u| = \begin{cases} |D_u| + |D_{1-u}| = 2^n, & \text{if } A_u = D_u \\ |\overline{D}_u| + |D_{1-u}| = 2^n - 1, & \text{if } A_u = \overline{D}_u. \end{cases} \tag{5}$$

Let $s_u(t)$ be the characteristic sequence of C_u. Note that just like C_u, which can be one of two distinct subsets of Z_N depending on A_u, the sequence $s_u(t)$ can also take one of the following two distinct sequences: one with 2^n 1's and the

other with $2^n - 1$ 1's. Let $d_{u,v}(\tau) = |C_u \cap (C_v + \tau)|$, where $\tau \in Z_N$, $C_v + \tau = \{c + \tau \mid c \in C_v\}$, and "+" means addition modulo N. Then we can easily check the following lemma:

Lemma 1. *The correlation function $R_{u,v}(\tau)$ can be expressed as*

$$R_{u,v}(\tau) = N - 2(|C_u| + |C_v| - 2d_{u,v}(\tau)).$$

Now, let us define two sets of characteristic sequences of C_u in (4).

Definition 1. *The set $\mathcal{U}_1$ is the collection of all the characteristic sequences $s_u(t)$, $1 \le u < 2^{n-1}$, of C_u with $A_u = D_u$. Similarly, the collection of all the characteristic sequences $s_u(t)$, $1 \le u < 2^{n-1}$, of C_u with $A_u = \overline{D}_u$ is called the set $\mathcal{U}_2$.*

The following theorem gives us the correlation values of the sequences in Definition 1:

Theorem 4 ([23]). *The correlation functions of two sequences $s_u(t)$ and $s_v(t)$ in $\mathcal{U}_1 \cup \mathcal{U}_2$ are as follows:*

Case 1) $s_u(t)$, $s_v(t) \in \mathcal{U}_1$;
i) $u \neq v$;

$$R_{u,v}(\tau) = \begin{cases} 2^n - 2, \text{ for } \tau = (0, u-v), (0, v-u), (1, u+v-1), (1, 1-u-v) \\ -2, \quad \text{otherwise.} \end{cases}$$

ii) $u = v$;

$$R_{u,u}(\tau) = \begin{cases} 2^{n+1} - 2, \text{ for } \tau = 0 \\ 2^n - 2, \quad \text{for } \tau = (1, 2u-1), (1, 1-2u) \\ -2, \quad \text{otherwise.} \end{cases}$$

Case 2) $s_u(t) \in \mathcal{U}_1$ *and* $s_v(t) \in \mathcal{U}_2$;
i) $u \neq v$;

$$R_{u,v}(\tau) = \begin{cases} -2^n, \text{ for } \tau = (0, u-v), (1, 1-u-v) \\ 2^n, \text{ for } \tau = (0, v-u), (1, u+v-1) \\ 0, \quad \text{otherwise.} \end{cases}$$

ii) $u = v$;

$$R_{u,u}(\tau) = \begin{cases} -2^n, \text{ for } \tau = (1, 1-2u) \\ 2^n, \text{ for } \tau = (1, 2u-1) \\ 0, \quad \text{otherwise.} \end{cases}$$

Case 3) $s_u(t),\ s_v(t) \in \mathcal{U}_2$;
i) $u \neq v$;

$$R_{u,v}(\tau) = \begin{cases} 2^n - 2, & \text{for } \tau = (0, u-v), (0, v-u) \\ -2^n + 2, & \text{for } \tau = (1, u+v-1), (1, 1-u-v) \\ -2, & \text{for } \tau = (0, \tau_2), \tau_2 \neq \pm(u-v) \\ 2, & \text{for } \tau = (1, \tau_2), \tau_2 \neq \pm(u+v-1). \end{cases}$$

ii) $u = v$;

$$R_{u,u}(\tau) = \begin{cases} 2^{n+1} - 2, & \text{for } \tau = 0 \\ -2^n + 2, & \text{for } \tau = (1, 2u-1), (1, 1-2u) \\ -2, & \text{for } \tau = (0, \tau_2), \tau_2 \neq 0 \\ 2, & \text{for } \tau = (1, \tau_2), \tau_2 \neq \pm(2u-1). \end{cases}$$

Therefore, there exist various LCZs in the correlation functions between sequences in $\mathcal{U}_1 \cup \mathcal{U}_2$.

We will explain two methods to select binary sequences in $\mathcal{U}_1 \cup \mathcal{U}_2$, so that the sets consisting of the selected sequences form binary LCZ sequence sets which are nearly optimal with respect to the following bound.

Since $\epsilon = 2$ in this case, (3) becomes

$$ML \leq N + 4 + \frac{12}{N-4}$$

and for $n \geq 4$, we have

$$M \leq \left\lfloor \frac{N+4}{L} \right\rfloor \tag{6}$$

where $\lfloor x \rfloor$ means the greatest integer less than or equal to x. When an $(N, M, L, 2)$ LCZ sequence set achieves the equality in (6), it is said to be optimal.

Recall that the locations of sidelobes are symmetric with respect to the origin. Thus, in terms of the distances to the sidelobes from the origin, there are at most two distinct distances. Let $L_{u,v}$ denote the distance to the nearest sidelobes from the origin in $R_{u,v}(\tau)$. Then, $L_{u,v}$ can be determined as in the following lemma.

Lemma 2. *For* $s_u(t), s_v(t) \in \mathcal{U}_1 \cup \mathcal{U}_2$, $1 \leq v \leq u < 2^{n-1}$, $L_{u,v}$ *is given as*

$$L_{u,v} = \begin{cases} \frac{N}{2} - u - v + 1, & \text{if } u-v \text{ is odd} \\ u - v, & \text{if } u-v \text{ is even and } u \neq v \\ 2u - 1, & \text{if } u = v. \end{cases} \tag{7}$$

Lemma 2 tells us that the LCZ of a set of sequences $s_u(t)$'s chosen from $\mathcal{U}_1 \cup \mathcal{U}_2$ is solely dependent on the index values u's regardless of whether the sequence $s_u(t)$ is from $\mathcal{U}_1$ or $\mathcal{U}_2$. Thus, what we are going to do now is to choose an index set $I \subset \{1, 2, \cdots, 2^{n-1} - 1\}$ and construct the set of sequences as

$$W_I = \{s_u(t) \in \mathcal{U}_1 \mid u \in I\} \cup \{s_u(t) \in \mathcal{U}_2 \mid u \in I\}$$

so that W_I becomes a good LCZ sequence set.

Lemma 2 tells us that the LCZ of the set W_I is the minimum of the following three values: $2^n - (u+v)$ for odd $|u-v|$, $|u-v|$ for nonzero even $|u-v|$, and $2u-1$ for $u=v$ as u and v run over I. At the same time, for a given L, we want to make the size of I as large as possible.

From these constraints, we can formulate fairly complex optimal design problem. The solution for this problem seems somewhat complicated, but the aforementioned constraints implicitly lead us to consider an index set I that forms an arithmetic progression with an odd value of common difference.

Proposition 1. *Pick an odd integer f and a nonnegative integer $f_0 < f$. Then, we make an index set I as*

$$I = \left\{ f_0 + mf \;\middle|\; m = 1, 2, \cdots, \left\lfloor \frac{2^{n-1} - f_0}{f} \right\rfloor \right\}.$$

Then, it is not difficult to show that the set size M and LCZ L of W_I in Proposition 1 are given as in the following theorem:

Theorem 5. *[23] Let q and r be the quotient and the remainder of 2^{n-1}, respectively, when divided by f, i.e., $2^{n-1} = qf + r$. Then, W_I from Proposition 1 becomes a binary LCZ sequence set with parameters $(2^{n+1} - 2, M, L, 2)$, where M and L are given as*

$$M = 2q$$

and if $f_0 = 0$,

$$L = \begin{cases} f + 2r, & \text{for } f \geq 2r+1 \\ 2f - 1, & \text{for } f < 2r+1 \end{cases} \tag{8}$$

and if $f_0 \neq 0$,

$$L = \begin{cases} f + 2r - 2f_0, & \text{for } f \geq 2r - 2f_0 \\ 2f, & \text{for } f < 2r - 2f_0. \end{cases} \tag{9}$$

Note that if f is even, then from Lemma 2, LCZ of the sequence set W_I becomes

$$L = \min_{u,v \in I, u \neq v} (u - v) = f.$$

But if f is odd, then from Theorem 5, LCZ is greater than f, which is the reason why we make the common difference f odd.

Now, we can easily obtain the following corollary and proposition:

Corollary 1. *The product of set size and LCZ in Proposition 1 is given as*

$$ML = \begin{cases} N - M(f - 2r) - 4r + 2, & \text{for } f \geq 2r+1 \text{ and } f_0 = 0 \\ N - M - 4r + 2, & \text{for } f < 2r+1 \text{ and } f_0 = 0 \\ N - M(f - 2r + 2f_0) - 4r + 2, & \text{for } f \geq 2(r - f_0) \text{ and } f_0 \neq 0 \\ N - 4r + 2, & \text{for } f < 2(r - f_0) \text{ and } f_0 \neq 0. \end{cases} \tag{10}$$

Proposition 2. *The indices u of the selected sequences $s_u(t)$ both in $\mathcal{U}_1$ and in $\mathcal{U}_2$ are chosen to form a progression starting from $f+2-f_0$ with differences f and $f+2$, alternately, i.e.,*

$$I = \{u_j \mid j = 0, 1, 2, \cdots, J,\ u_0 = f+2-f_0, \\ u_{2k+1} - u_{2k} = f,\ u_{2k+2} - u_{2k+1} = f+2\}$$

where J is the largest integer such that $u_J < 2^{n-1}$, f_0 is 0 or 1, and f is some odd integer.

The set size M and the LCZ L are given as in the following theorem:

Theorem 6. *Let q and r be the quotient and the remainder of $2^{n-1}-1$, respectively, when divided by $2(f+1)$, i.e., $2^{n-1}-1 = 2q(f+1)+r$. Then W_I from Proposition 2 becomes a binary LCZ sequence set with parameters $(2^{n+1}-2, M, L, 2)$, where M and L are given as*

$$M = \begin{cases} 4q, & \text{for } 0 \le r < f+2-f_0 \\ 4q+2, & \text{for } f+2-f_0 \le r < 2f+2 \end{cases}$$

and

$$L = \begin{cases} 2r+f+2+2f_0, & \text{for } 0 \le r < \frac{f-3f_0}{2} \\ 2f+2-f_0, & \text{for } \frac{f-3f_0}{2} \le r < f+2-f_0 \text{ and } \frac{3f+2-3f_0}{2} \le r < 2f+2 \\ 2r-f+2f_0, & \text{for } f+2-f_0 \le r < \frac{3f+2-3f_0}{2}. \end{cases} \tag{11}$$

In this construction method for binary LCZ sequence sets, the LCZ length can be freely selected and the resulting LCZ sequence sets have sizes that are almost optimal with respect to the Tang, Fan, and Matsufuji bound.

4.2 Extension Method of q-Ary LCZ Sequence Sets

In this subsection, the construction methods of the LCZ sequence sets by extending method are introduced. When we extend the period, the LCZ length is kept unchangeable or is slightly decreased.

Construction 3 [18]:
When a q-ary LCZ sequence set with parameters (N, M, L, ϵ) is given, we can construct a q-ary LCZ sequence set with parameters $(2N, 2M, L, 2\epsilon)$ or $(2N, 2M, L-1, 2\epsilon)$.

Proposition 3. *Let $\mathcal{T}_1$ be the set of q-ary sequences given as*

$$\mathcal{T}_1 = \{s_i(t) \mid 0 \le i \le 2M-1,\ 0 \le t \le 2N-1\}$$

where $s_i(t)$ is defined as

$$s_i(2t) = \begin{cases} v_i(t), & \text{for } 0 \le i \le M-1 \\ v_{i-M}(t) + \frac{q}{2}, & \text{for } M \le i \le 2M-1 \end{cases}$$

$$s_i(2t+1) = \begin{cases} v_i\left(t + \lceil \frac{L}{2} \rceil\right), & \text{for } 0 \le i \le M-1 \\ v_{i-M}\left(t + \lceil \frac{L}{2} \rceil\right), & \text{for } M \le i \le 2M-1 \end{cases}$$

where $\lceil x \rceil$ means the smallest integer greater than or equal to x.

Theorem 7. *$\mathcal{T}_1$ in Proposition 3 is a q-ary LCZ sequence set with parameters $(2N, 2M, L, 2\epsilon)$ if L is odd and with parameters $(2N, 2M, L-1, 2\epsilon)$ if L is even.*

The following construction is considered as a generalization of Construction 3.

Construction 4:
Using the q-ary LCZ sequence set with parameters (N, M, L, ϵ), a new extended q-ary LCZ sequence set can be constructed as in the following theorem:

Theorem 8. *Suppose that an $r \times r$ unitary matrix $\mathbf{D} = (d_{i,j})_{r\times r}$ over Z_q exists for some positive integer r such that $r|q$. Let $\mathcal{S}$ be an LCZ sequence set defined in (2). Let $\mathcal{T}$ be the q-ary sequence set given by*

$$\mathcal{T} = \{s_u(t) \mid 0 \le u \le rM-1,\ 0 \le t \le rN-1\}$$

$$s_u(t) = s_u(ri+j) = f_{u-kM}\left(i + j\left\lfloor \frac{L+1}{r} \right\rfloor\right) + d_{k,j},$$
$$\text{for } \ kM \le u \le (k+1)M-1$$

where $0 \le i \le N-1$, $0 \le j,k \le r-1$. Then $\mathcal{T}$ is a q-ary LCZ sequence set with parameters $(rN, rM, r\lfloor \frac{L+1}{r} \rfloor - 1, r\epsilon)$.

Proof. From the definition of the set $\mathcal{T}$, it is not difficult to see that the period of the sequences in $\mathcal{T}$ is rN and the size of $\mathcal{T}$ is rM. Thus, it is enough to show that $\left|R_{u,v}(\tau)\right|$ is less than or equal to $r\epsilon$ for $|\tau| < r\lfloor (L+1)/r \rfloor - 1$ except for the in-phase autocorrelation.

Let $L+1 = ra+b$, where a is a nonnegative integer and $0 \le b \le r-1$, so that we have $\lfloor \frac{L+1}{r} \rfloor = a$. In order to show that $|R_{u,v}(\tau)| \le r\epsilon$ for all $|\tau| < ar-1$, the following two cases should be separately considered.

Case 1) $\tau \equiv 0 \bmod r$;

The correlation function $R_{u,v}(\tau)$ in (1) between $s_u(t)$ and $s_v(t)$ such that $k_1M \le u \le (k_1+1)M-1$ and $k_2M \le v \le (k_2+1)M-1$ can be rewritten as

$$\begin{aligned} R_{u,v}(\tau) &= \sum_{j=0}^{r-1}\sum_{i=0}^{N-1} \omega_q^{f_{u-k_1M}(i+aj)+d_{k_1,j}-f_{v-k_2M}(i+aj+\frac{\tau}{r})-d_{k_2,j}} \\ &= \sum_{j=0}^{r-1} \omega_q^{(d_{k_1,j}-d_{k_2,j})} \sum_{i=0}^{N-1} \omega_q^{f_{u-k_1M}(i+aj)-f_{v-k_2M}(i+aj+\frac{\tau}{r})} \end{aligned} \tag{12}$$

where $\omega_q = e^{j2\pi/q}$.

Using the correlation property of LCZ sequence set $\mathcal{S}$, it is easy to check that the magnitude of the inner sum in (12) is less than or equal to ϵ for $-rL < \tau < rL$ unless $u - k_1 M = v - k_2 M$ and $\tau = 0$. Thus, we have $|R_{u,v}(\tau)| \leq r\epsilon$ for all $|\tau| < ar - 1$.

In the case when $u - k_1 M = v - k_2 M$ and $\tau = 0$, the inner sum in (12) becomes N and thus (12) can be rewritten as

$$R_{u,v}(0) = N \sum_{j=0}^{r-1} \omega_q^{(d_{k_1,j} - d_{k_2,j})}. \tag{13}$$

Note that in (13), we can assume that $k_1 \neq k_2$. Otherwise, $k_1 = k_2$ implies that $u = v$, which in turn implies that (13) is nothing but the in-phase autocorrelation. Now, since $\mathbf{D}$ is unitary, (13) becomes zero.

Case 2) $\tau \not\equiv 0 \bmod r$;

Set $\tau = r\tau_1 + \tau_2, 1 \leq \tau_2 \leq r - 1$. Then, we have

$$\begin{aligned} & R_{u,v}(\tau) \\ &= \sum_{j=0}^{r-1} \sum_{i=0}^{N-1} \omega_q^{f_{u-k_1 M}(i+aj) + d_{k_1,j} - f_{v-k_2 M}(i + \left\lfloor \frac{j+\tau_2}{r} \right\rfloor + (j \oplus \tau_2)a + \tau_1) - d_{k_2,(j\oplus\tau_2)}} \\ &= \sum_{j=0}^{r-1} \omega_q^{d_{k_1,j} - d_{k_2,(j\oplus\tau_2)}} \sum_{i=0}^{N-1} \omega_q^{f_{u-k_1 M}(i+aj) - f_{v-k_2 M}(i + \left\lfloor \frac{j+\tau_2}{r} \right\rfloor + (j\oplus\tau_2)a + \tau_1)} \end{aligned} \tag{14}$$

where $\oplus$ denotes the addition modulo r.

Again from the definition of the set $\mathcal{S}$, it is clear that the magnitude of inner sum in (14) is less than or equal to ϵ if the difference between $i + aj$ and $i + \left\lfloor \frac{j+\tau_2}{r} \right\rfloor + (j \oplus \tau_2)a + \tau_1$ is less than L. Thus, we have to show that

$$\left| \left\lfloor \frac{j + \tau_2}{r} \right\rfloor + (j \oplus \tau_2)a + \tau_1 - aj \right| < L \tag{15}$$

for $|\tau| < r \lfloor (L+1)/r \rfloor - 1 = ar - 1$.

The following two subcases should be considered.

2-i) $j + \tau_2 \geq r$;

The range of τ satisfying the inequality (15) can be rewritten as

$$\begin{aligned} & -L < 1 - (r - \tau_2)a + \frac{\tau - \tau_2}{r} < L \\ & \Leftrightarrow -Lr - r + (r - \tau_2)ar + \tau_2 < \tau < Lr - r + (r - \tau_2)ar + \tau_2 \\ & \Leftrightarrow -Lr + (r - \tau_2)(ar - 1) < \tau < Lr + (r - \tau_2)(ar - 1). \end{aligned}$$

In the above inequality, the upper bound is clearly greater than $ar - 1$ and from the fact that $L = ar + b - 1$, the lower bound can be rewritten as $-br - (ar - 1)\tau_2$, which is less than $-(ar - 1)$. Thus, we prove it.

2-ii) $j + k'' < r$;
Equation (15) can be rewritten as

$$-L < \tau_2 a + \frac{\tau - \tau_2}{r} < L$$
$$\Leftrightarrow -Lr - \tau_2(ar-1) < \tau < Lr - \tau_2(ar-1) = (r-\tau_2)(ar-1) + br.$$

Again, in the above inequality, the upper bound is greater than $ar-1$ and the lower bound is less than $-(ar-1)$. Thus, we prove it.

From the above two cases, we prove that $\mathcal{T}$ is an LCZ sequence set with parameters $(rN, rM, r\left\lfloor \frac{L+1}{r} \right\rfloor - 1, r\epsilon)$. □

When we apply the proposed r-extension method in Theorem 8, the period, the size, and the maximum correlation magnitude inside the correlation zone of the extended set are increased by the factor r, but the LCZ of the extended set cannot exceed that of the original set. In fact, when the extension factor is r and the LCZ of the original set is L, LCZ is slightly decreased by $(L+1) \bmod r$. Thus, in the case of applying the extension method successively, the LCZ of the finally obtained set can be dependent on the order of extension. Consider the following example.

Let $\mathcal{S}$ be a q-ary LCZ sequence set with parameters (N, M, L, ϵ). Assume that both $p_1 \times p_1$ unitary matrix $\mathbf{D}_{p_1}$ over Z_q and $p_2 \times p_2$ unitary matrix $\mathbf{D}_{p_2}$ over Z_q exist. There are three different ways of applying our extension method to $\mathcal{S}$ to obtain the set $\mathcal{S}'$ extended by $p_1 p_2$. We can obtain $\mathcal{S}'$ in a single step using the unitary matrix $\mathbf{D}_{p_1} \otimes \mathbf{D}_{p_2}$. Here, $\mathbf{D}_{p_1} \otimes \mathbf{D}_{p_2}$ represents the $p_1 p_2 \times p_1 p_2$ unitary matrix over Z_q obtained from the Kronecker product of $\mathbf{D}_{p_1}$ and $\mathbf{D}_{p_2}$. Then, the LCZ size of $\mathcal{S}'$ becomes $p_1 p_2 \left\lfloor \frac{L+1}{p_1 p_2} \right\rfloor - 1$. When we apply our extension method to $\mathcal{S}$ in the order of p_1-extension first and p_2-extension second, the final LCZ size becomes $p_2 \left\lfloor \frac{p_1}{p_2} \left\lfloor \frac{L+1}{p_1} \right\rfloor \right\rfloor - 1$. But, if we change the order of extension, it becomes $p_1 \left\lfloor \frac{p_2}{p_1} \left\lfloor \frac{L+1}{p_2} \right\rfloor \right\rfloor - 1$. Thus, in order to make the LCZ size the largest, we should be careful about the order of extension and it is summarized as in the following theorem:

Theorem 9. *Let $\mathcal{S}$ be a set of q-ary LCZ sequence set with parameters (N, M, L, ϵ). Let p_i, $1 \le i \le k$, be positive integers such that $p_i \times p_i$ unitary matrices $\mathbf{D}_{p_i}$ over Z_q exist. Define $h_a(x) = x \bmod a$ and $g_a(x) = x - h_a(x+1)$. Let $r = \prod_{i=1}^{k} p_i$. Assume that $h_{p_1}(L+1) \le h_{p_2}(L+1) \le \cdots \le h_{p_k}(L+1)$. If we extend $\mathcal{S}$ by r by applying the p_i-extension methods successively, the maximum LCZ size is achieved when the p_i-extension is done in the increasing order of i, i.e., the p_1-extension first and the p_2-extension next and so on. Then, the maximum LCZ size of the extended LCZ sequence set becomes*

$$L_r = g_{p_k}(L) = L - h_{p_k}(L+1). \tag{16}$$

Proof. It is not difficult to see that

$$h_a(x-y) = \begin{cases} h_a(x) - h_a(y) & \text{if } h_a(y) \le h_a(x) \\ h_a(x) - h_a(y) + a & \text{otherwise.} \end{cases} \tag{17}$$

Especially when $0 \le y \le h_a(x)$, we have

$$h_a(x-y) = h_a(x) - y. \tag{18}$$

In general, when we apply p_i-extension first and then p_j-extension to $\mathcal{S}$, the LCZ of the p_ip_j-extended set is bounded as

$$g_{p_j}\left(g_{p_i}(L)\right) \le g_{p_j}(L) \stackrel{\Delta}{=} L - h_{p_j}(L+1), \tag{19}$$

because $g_a(x)$ is a non-increasing function of x for any positive integer a.

The equality in (19) is achieved if and only if $h_{p_i}(L+1) \le h_{p_j}(L+1)$. This is because

$$\begin{aligned} g_{p_j}\left(g_{p_i}(L)\right) &= L - h_{p_i}(L+1) - h_{p_j}(L+1-h_{p_i}(L+1)) \\ &= L - h_{p_i}(L+1) - h_{p_j}(L+1) + h_{p_i}(L+1) \\ &= L - h_{p_j}(L+1) \\ &= g_{p_j}(L) \end{aligned}$$

from (18). Therefore, if we apply the p_i-extension successively in the increasing order of i, then the LCZ of the r-extended set becomes $g_{p_k}(L) = L - h_{p_k}(L+1)$.

From (17) and the fact that $g_a(\cdot)$ is a non-increasing function, it is obvious that this is the maximum achievable value. □

Note that if we construct an r-extended LCZ sequence set by a single-step extension using the $r \times r$ unitary matrix $\bigotimes_{i=1}^{k} \mathbf{D}_{p_i}$, its LCZ size becomes $L - h_r(L+1)$, which is smaller than or equal to L_r in (16).

For $r = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ and $m_i \ge 1$, the following corollary can be stated without proof.

Corollary 2. *Let $\mathcal{S}$ be a set of q-ary LCZ sequence set with parameters (N, M, L, ϵ). Let p_i, $1 \le i \le k$, be positive integers such that there exist $p_i \times p_i$ unitary matrices over Z_q. Let $r = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, $m_i \ge 1$ and $h_{p_i}(L+1) = L+1 \bmod p_i$. The maximum LCZ size of the extended LCZ sequence sets by r is given as*

$$L_r = L - \max_{1 \le i \le k} h_{p_i}(L+1).$$

Table 2 shows the LCZ lengths of extended LCZ sequence sets for the different methods.

Now, we will show the conditions for which the extension of LCZ sequence sets preserves the optimality of the LCZ sequence set in terms of the bound by Tang, Fan, and Matsufuji [43]. Using the bound in Theorem 1, the optimality of the extended LCZ sequence sets by Theorem 8 can be stated as in the following theorem:

Table 2. Comparison of the extended LCZ zones

p \ LCZ length	100	101	102	103	104	105	106	107	108	109
$p_1 = 3, p_2 = 5$	94	99	99	99	104	104	104	104	104	104
$p_1 = 5, p_2 = 3$	98	98	98	98	104	104	104	104	104	107
$p_1 = 15$	89	89	89	89	104	104	104	104	104	104

Theorem 10. *Let $\mathcal{S}$ be an optimal LCZ sequence set with parameters (N, M, L, ϵ) with respect to the bound by Tang, Fan, and Matsufuji. Then, the extended LCZ sequence set $\mathcal{T}$ with parameters $(rN, rM, r\left\lfloor \frac{L+1}{r} \right\rfloor - 1, r\epsilon)$ in Theorem 8 is optimal with respect to the bound by Tang, Fan, and Matsufuji if $L \equiv r - 1 \bmod r$ and $\left\lfloor \frac{1}{M} \frac{N^2-\epsilon^2}{N-\epsilon^2} \right\rfloor = \left\lfloor \frac{1}{M} \frac{N^2-\epsilon^2}{N-r\epsilon^2} \right\rfloor$.*

Proof. From (3), we have

$$L = \left\lfloor \frac{1}{M} \frac{N^2 - \epsilon^2}{N - \epsilon^2} \right\rfloor.$$

For an LCZ sequence set with parameters $(rN, rM, L', r\epsilon)$ to be optimal, L' should satisfy

$$L' = \left\lfloor \frac{1}{M} \frac{N^2 - \epsilon^2}{N - r\epsilon^2} \right\rfloor.$$

Since $\left\lfloor \frac{1}{M} \frac{N^2-\epsilon^2}{N-\epsilon^2} \right\rfloor \leq \left\lfloor \frac{1}{M} \frac{N^2-\epsilon^2}{N-r\epsilon^2} \right\rfloor$, for the set $\mathcal{T}$ to preserve its optimality, it is necessary that

$$L' = r \left\lfloor \frac{L+1}{r} \right\rfloor - 1 = L,$$

which implies that $L \equiv r - 1 \bmod r$ and

$$\left\lfloor \frac{1}{M} \frac{N^2 - \epsilon^2}{N - \epsilon^2} \right\rfloor = \left\lfloor \frac{1}{M} \frac{N^2 - \epsilon^2}{N - r\epsilon^2} \right\rfloor.$$

Let $\Delta = \frac{1}{M} \frac{N^2-\epsilon^2}{N-\epsilon^2} - \left\lfloor \frac{1}{M} \frac{N^2-\epsilon^2}{N-\epsilon^2} \right\rfloor$ so that $0 \leq \Delta < 1$. Then, we have

$$\left\lfloor \frac{1}{M} \frac{N^2 - \epsilon^2}{N - r\epsilon^2} \right\rfloor - \left\lfloor \frac{1}{M} \frac{N^2 - \epsilon^2}{N - \epsilon^2} \right\rfloor = \left\lfloor \Delta + \frac{1}{M} \frac{N^2 - \epsilon^2}{N - \epsilon^2} \frac{(r-1)\epsilon^2}{N - r\epsilon^2} \right\rfloor. \tag{20}$$

If $0 \leq \Delta + \frac{1}{M} \frac{N^2-\epsilon^2}{N-\epsilon^2} \frac{(r-1)\epsilon^2}{N-r\epsilon^2} < 1$, then the extended LCZ sequence set preserves the optimality. It is easy to check that for small values of N/M, ϵ, and r, the optimality of LCZ sequence sets is often preserved through the extension process. □

It is possible to enlarge the symbol alphabet of the extended sequence set in Theorem 8. Suppose that there exists an $r \times r$ unitary matrix over Z_p for some p divisible by q. We can convert the q-ary LCZ sequence set $\mathcal{S}$ into the p-ary LCZ sequence set $\mathcal{S}'$ by replacing the symbol k in Z_q by the symbol kp/q in Z_p. Then, we can apply our r-extension method to $\mathcal{S}'$ using the $r \times r$ unitary matrix Z_p to construct p-ary LCZ sequence set with parameters $(rN, rM, r\left\lfloor \frac{L+1}{r} \right\rfloor - 1, r\epsilon)$.

The same extension method as Theorem 8 can be applied to construct ZCZ sequence sets by setting $\epsilon = 0$. From Theorem 9, the extended ZCZ sequence set always preserves the optimality if $L \equiv r - 1 \bmod r$.

5 Conclusion

We reviewed our basic or general construction methods of LCZ sequence sets. Finally, the extending method of q-ary LCZ sequence sets is proposed, which can be considered as a generalization of the previous extension method. Using the proposed extending method, a q-ary LCZ sequence set with parameters (N, M, L, ϵ) can be extended to a q-ary LCZ sequence set with parameters $(rN, rM, r\left\lfloor \frac{L+1}{r} \right\rfloor - 1, r\epsilon)$, where r is a positive integer such that $r|q$. And we showed that the LCZ of the obtained set is dependent on the order of extension. When $L \equiv -1 \bmod r$ and $\left\lfloor \frac{1}{M} \frac{N^2-\epsilon^2}{N-\epsilon^2} \right\rfloor = \left\lfloor \frac{1}{M} \frac{N^2-\epsilon^2}{N-r\epsilon^2} \right\rfloor$, a q-ary LCZ sequence set with parameters $(rN, rM, L, r\epsilon)$ constructed by the proposed extension method preserves the optimality of the LCZ sequence set.

Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (MEST) (No. 2009-0081441) and the IT R&D program of MKE/KEIT. [2008-F-007-02, Intelligent Wireless Communication Systems in 3 Dimensional Environment].

References

1. Antweiler, M.: Cross-correlation of p-ary GMW sequences. IEEE Trans. Inf. Theory 40(4), 1253–1261 (1994)
2. Boztas, S., Kumar, P.V.: Binary sequences with Gold-like correlation but larger linear span. IEEE Trans. Inf. Theory 40(2), 532–537 (1994)
3. Boztas, S., Hammons, R., Kumar, P.V.: 4-phase sequences with near-optimum correlation properties. IEEE Trans. Inf. Theory 38(3), 1101–1113 (1992)
4. Chung, J.-S.: Properties of Sidel'nikov sequences and an extending method of LCZ sequence sets, Ph.D. dissertation, Seoul National Univ., Seoul, Korea (2010)
5. De Gaudenzi, R., Elia, C., Viola, R.: Bandlimited quasi-synchronous CDMA: A novel satellite access technique for mobile and personal communication systems. IEEE J. Sel. Areas Commun. 10(2), 328–343 (1992)

6. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inf. Theory 14, 154–156 (1968)
7. Gordon, B., Mills, W.H., Welch, L.R.: Some new difference sets. Canadian J. Math. 14, 614–625 (1962)
8. Hall Jr., M.: A Survey of Difference Sets. Proc. Amer. Math. Soc. 7, 975–986 (1956)
9. Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discrete Math. 16, 209–232 (1976)
10. Helleseth, T., Kumar, P.V.: Sequences with low correlation. In: Pless, V., Huffman, C. (eds.) Handbook of Coding Theory. Elsevier Science, Amsterdam (1998)
11. Hu, H., Gong, G.: New sets of zero or low correlation zone sequences via interleaving techniques. IEEE Trans. Inf. Theory 56(4), 1702–1713 (2010)
12. Jang, J.-W.: Families of sequences with optimal correlation property. Ph.D. dissertation, Seoul National Univ., Seoul, Korea (2006)
13. Jang, J.-W., Kim, S.-H., No, J.-S., Chung, H.: New constructions of quaternary Hadamard matrices. In: Helleseth, T., Sarwate, D., Song, H.-Y., Yang, K. (eds.) SETA 2004. LNCS, vol. 3486, pp. 361–372. Springer, Heidelberg (2005)
14. Jang, J.-W., Kim, S.-H., No, J.-S.: New construction of quaternary low correlation zone sequence sets from binary low correlation zone sequence sets. Accepted for Publication in Journal of Communications and Networks (January 2010)
15. Jang, J.-W., Kim, Y.-S., No, J.-S., Helleseth, T.: New family of p-ary sequences with optimal correlation property and large linear span. IEEE Trans. Inf. Theory 50(8), 1839–1844 (2004)
16. Jang, J.-W., No, J.-S., Chung, H.: A new construction of optimal p^2-ary low correlation zone sequences using unified sequences. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E89-A(10), 2656–2661 (2006)
17. Jang, J.-W., No, J.-S., Chung, H.: Butson Hadamard matrices with partially cyclic core. Designs, Codes and Cryptography 43(2-3), 93–101 (2007)
18. Jang, J.-W., No, J.-S., Chung, H., Tang, X.: New sets of optimal p-ary low correlation zone sequences. IEEE Trans. Inf. Theory 53(2), 815–821 (2007)
19. Kim, S.-H.: Trace representation of Lempel-Cohn-Eastman sequences and new families of binary sequences with low correlation. Ph.D. dissertation, Seoul National Univ., Seoul, Korea (2004)
20. Kim, S.-H., Jang, J.-W., No, J.-S., Chung, H.: New constructions of quaternary low correlation zone sequences. IEEE Trans. Inf. Theory 51(4), 1469–1477 (2005)
21. Kim, S.-H., No, J.-S.: New families of binary sequences with low correlation. IEEE Trans. Inf. Theory 49(11), 3059–3065 (2003)
22. Kim, Y.-S.: Properties of Sidel'nikov sequences and new sequence families with low correlation. Ph.D. dissertation, Seoul National Univ., Seoul, Korea (2007)
23. Kim, Y.-S., Jang, J.-W., No, J.-S., Chung, H.: New design of low correlation zone sequence sets. IEEE Trans. Inf. Theory 52(10), 4607–4616 (2006)
24. Kasami, T.: Weight distribution formular for some class of cyclic codes. Technical Report R-285 (AD 632574), Coordinated Science Laboratory, Univ. of Illinois, Urbana (April 1966)
25. Kasami, T.: Weight distribution of Bose-Chaudhuri-Hocquenghem codes. In: Cambinatorial Mathematics and Its Applications. Univ. of North Carolina Press, Chapel Hill (1969)

26. Kumar, P.V., Helleseth, T., Calderbank, A.R.: An upper bound for Weil exponential sums over Galois rings and applications. IEEE Trans. Inf. Theory 41(2), 456–468 (1995)
27. Kumar, P.V., Helleseth, T., Calderbank, A.R., Hammons Jr., A.R.: Large families of quaternary sequences with low correlation. IEEE Trans. Inf. Theory 42(2), 579–592 (1996)
28. Kumar, P.V., Liu, C.-M.: On lower bounds to the maximum correlation of complex roots-of unity sequences. IEEE Trans. Inf. Theory 36(3), 633–640 (1990)
29. Kumar, P.V., Moreno, O.: Prime-phase sequences with periodic correlation properties better than binary sequences. IEEE Trans. Inf. Theory 37, 603–616 (1991)
30. Levenshtein, V.I.: Bounds on the maximal cardinality of a code with bounded modules of the inner product. Soviet. Math. Dokl. 25, 526–531 (1982)
31. Liu, S.-C., Komo, J.F.: Nonbinary Kasami sequences over $GF(p)$. IEEE Trans. Inf. Theory 38, 1409–1412 (1992)
32. Long, B., Zhang, P., Hu, J.: A generalized QS-CDMA system and the design of new spreading codes. IEEE Trans. Veh. Technol. 47(4), 1268–1275 (1998)
33. Moriuchi, T., Imamura, K.: Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar-Moreno sequences. IEEE Trans. Inf. Theory 41, 572–576 (1995)
34. No, J.-S.: p-ary unified sequences: p-ary extended d-form sequences with the ideal autocorrelation property. IEEE Trans. Inf. Theory 48(9), 2540–2546 (2002)
35. No, J.-S., Jang, J.-W.: Performance analysis of quasi-synchronous code division multiple access systems using new set of LCZ sequences. Telecommunications Review 15(3), 447–456 (2005)
36. No, J.-S., Kumar, P.V.: A new family of binary pseudorandom sequences having optimal correlation properties and large linear span. IEEE Trans. Inf. Theory 35, 371–379 (1989)
37. No, J.-S., Ryu, J.-H., Moon, J., Kim, S.-H., Kim, S., Jang, J.-W., Kim, S.-K., Go, J.-Y.: Research of Signal design and high efficiency modulation/channel code for 4G mobile access, ETRI (2002)
38. Olsen, J.D., Scholtz, R.A., Welch, L.R.: Bent-function sequences. IEEE Trans. Inf. Theory 28, 858–864 (1982)
39. Sarwate, D.V., Pursley, M.B.: Crosscorrelation properties of pseudorandom and related sequences. Proc. IEEE 68(5), 593–619 (1980)
40. Scholtz, R., Welch, L.: GMW sequences. IEEE Trans. Inf. Theory 30(3), 548–553 (1984)
41. Sidel'nikov, V.M.: On mutual correlation of sequences. Soviet Math. Dokl. 12(1), 197–201 (1971)
42. Tang, X.H., Fan, P.Z.: A class of pseudonoise sequences over GF(p) with low correlation zone. IEEE Trans. Inf. Theory 47(4), 1644–1649 (2001)
43. Tang, X.H., Fan, P.Z., Matsufuji, S.: Lower bounds on correlation of spreading sequence set with low or zero correlation zone. Electron. Lett. 36(6), 551–552 (2000)
44. Torii, H., Nakamura, M., Suehiro, N.: A new class of zero-correlation zone sequences. IEEE Trans. Inf. Theory 50(3), 559–565 (2004)
45. Trachtenberg, H.M.: On the cross-correlation functions of maximal recurring sequences. Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA (1970)
46. Udaya, P.: Polyphase and frequency hopping sequences obtained from finite rings. Ph.D. dissertation, Indian Inst. Technol, Kanpur, India (1992)

47. Wang, J.-S., Qi, W.-F.: Analysis of designing interleaved ZCZ sequence families. In: Gong, G., Helleseth, T., Song, H.-Y., Yang, K. (eds.) SETA 2006. LNCS, vol. 4086, pp. 129–140. Springer, Heidelberg (2006)
48. Welch, L.R.: Lower bounds on the maximum cross correlation of signals. IEEE Trans. Inf. Theory 20, 397–399 (1974)
49. Yang, J.-D., Jin, X., Song, K.-Y., No, J.-S., Shin, D.-J.: Multicode MIMO systems with quaternary LCZ and ZCZ sequences. IEEE Trans. Veh. Technol. 57(4), 2334–2341 (2008)

Decimation Generator of Zadoff-Chu Sequences

Srdjan Budisin*

IMTEL, Bulevar Mihaila Pupina 165B, 11070 Novi Beograd, Serbia
budishin@yahoo.com

Abstract. A compact expression for Zadoff-Chu sequences is introduced and used to show that all sequences of a given odd prime length are permutations of two seed sequences. In addition, it helps us derive a decimation formula and demonstrate that when two pre-calculated seed sequences and stored in the memory, any desired Zadoff-Chu sequence of odd prime length can be generated, sample-by-sample, simply by incrementing the read index by a corresponding step value. In this manner no calculation of sequence elements is required. That is, this algorithm does not require any additions, multiplications, or trigonometric calculations to generate sequences in real-time. Furthermore, the proposed table-lookup requires storing only a single sequence pair for each desired Zadoff-Chu sequence family of odd prime length.

Keywords: Zadoff-Chu sequences, perfect poly-phase sequences, Long Term Evolution (LTE).

1 Introduction

Zadoff-Chu sequences [1] belong to the class of perfect (sometimes called ideal) poly-phase sequences. Other well-known perfect poly-phase sequences are Frank sequences [2] and their generalization - the GCL sequences (Generalized Chirp-Like sequences) [3]. Perfect sequences have the property that their periodic autocorrelation function is perfect, that is, it is zero for all time lags except for the zero lag. As a consequence, the Discrete Fourier Transform (DFT) of Zadoff-Chu sequences has constant amplitude.

Historically, chirp signals (characterized by a linear frequency sweep) were first used in radars [4] as the first pulse compression waveform. Later, with the emergence of digital signal processing, phase modulated sequences (mostly Binary Phase Modulated – BPSK) were largely used as opposed to the chirp signal which is a frequency modulated signal. At the same time, with the introduction of the spread spectrum in military applications, phase modulated sequences found an additional role. Later, spread spectrum (via Direct Sequence – Code Division Multiple Access - DS-CDMA) was also adopted in commercial applications as a standard for mobile/cellular networks. In the era of digital signal processing, chirp waveforms were reinvented first in the form of Frank sequences [2], where the frequency

* Special thanks to Prof. Predrag Spasojevic from WINLAB, Rutgers University, for valuable sugestions and help.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 30–40, 2010.

increases in discrete steps and later in the form of Zadoff-Chu sequences [1], where the frequency gradually increases but is not limited to the Nyquist frequency. In fact, for Zadoff-Chu sequences the frequency rise up to a value several times the Nyquist frequency resulting in aliasing which is not an unwanted effect but is an integral property of the sequence design. However, such a sequence have very strong mathematical properties such as the ideal periodic autocorrelation function and, also, acceptable aperiodic autocorrelation properties [8].

In radar applications variations of those sequences called P1, P2, P3, and P4 sequences [4] were proposed as aperiodic waveforms. In 1992 Popovic [3] gave a construction that generalizes both Frank sequences and Zadoff-Chu sequences and called them GCL (Generalized Chirp-Like) sequences for historical reasons. In 1996 Mow [5] gave a further generalization of perfect polyphase sequences which includes, besides GCL sequences, 3 other families of sequences. Today the prevailing terminology for perfect sequences is CAZAC (Constant Amplitude Zero Autocorrelation Sequences).

Recently, Zadoff-Chu sequences have been used in several blocks of the new 3GPP Long Term Evolution (LTE) standard [6] for wireless communication having several roles: the down-link primary synchronization signal, the ranging (PRACH) preamble, and the up-link reference signal. New hand held mobile devices have very high requirements on complexity, price and power consumption. Thus it is of great importance to simplify any algorithm which would result in higher value of the device.

The main contribution of this paper is achieved in three steps. First a new expression for Zadoff-Chu sequences is given. Based on this new expression the decimation formula is derived. This decimation formula allows us to relate the Zadoff-Chu sequences to the quadratic residues theory from the number theory. From this main result two consequences are derived. In the theoretical area it is shown that all Zadoff-Chu sequences can be divided into two groups depending on whether the root index is a quadratic residue or a quadratic non-residue and that all sequences from one group are permutationally equivalent. In the practical area it is shown that all Zadoff-Chu sequences of a given length can be generated from two seed sequences by simple permutation of sequence elements leading to an efficient generator.

Section 2 introduces the standard definition, proposes a new expression for Zadoff-Chu sequences, and also, illustrates their differences through examples. Section 3 derives the decimation formula that is the main theoretical result of this paper. Section 4 describes the algorithm for efficient generation and contrasts its implementation to a standard lookup-table implementation of the Zadoff-Chu sequence generator.

2 Zadoff-Chu Sequence Modeling

2.1 Standard Notation

In this work we consider only Zadoff-Chu sequences of length P, where P is an odd prime. Zadoff-Chu sequences are usually defined [1] for odd lengths as

$$y_U(n) = e^{-\frac{2\pi i}{P} \cdot U \cdot \frac{n(n+1)}{2}}, \tag{1}$$

where U is the "root index" that determines a specific sequence from the set of length-P sequences, n is the time index and $i = \sqrt{-1}$. For prime values of P, each $U = 1 \ldots P-1$ will generate a different Zadoff-Chu sequence. Hence, there are *P-1* different Zadoff-Chu sequences of length P. All cyclic time shifts (shift of the time index n) and phase shifts (shift of the phase angle of the complex exponential) of a sequence in (1) are considered equivalent and are *not* treated as essentially different sequences.

We use the notation and the terminology introduced by Frank [2]. Hence, the sequence phase is represented as a product of the *basic angle* $\phi_0 = 2\pi i/P$ and its *multiplicative coefficient:*

$$Y_U(n) = U \cdot \frac{n(n+1)}{2}. \tag{2}$$

Now, the complex Zadoff-Chu sequence elements are

$$y_U(n) = e^{-i\phi_0 \cdot Y_U(n)} = e^{-\frac{2\pi i}{P} \cdot Y_U(n)}. \tag{3}$$

Alternatively, Zadoff-Chu sequences are represented using sequences of roots of unity. Let the primitive P-th root of unity be $\mathrm{W}_P = e^{-i\phi_0} = e^{-2\pi i/P}$. In this case, the sequence elements can be expressed using powers of W_P, as follows

$$y_U(n) = \mathrm{W}_P^{Y_U(n)}. \tag{4}$$

In the rest of this paper we use small letters to denote the poly-phase (complex) sequence itself and capital letters to denote the *multiplicative coefficients* (which are integers). The *multiplicative coefficients* $Y_U(n)$ will be used in most expressions instead of the Zadoff-Chu sequence $y_U(n)$ itself, in order to simplify notation. Keep in mind that the *multiplicative coefficient* $Y_U(n)$ should always be viewed *modulo* P (because the complex exponential function is periodic with period 2π and, hence, $\mathrm{W}_P{}^{Y_U(n)}$ is periodic in $Y_U(n)$ with a period P). To stress this fact we will use "$\equiv$" (equivalence modulo P) instead of "$=$" (equality) in equations that are modulo P.

2.2 New Alternative Expression for Zadoff-Chu Sequences

The definition (1) is sometimes modified to include frequency shifted versions of those sequences. Those frequency shifted versions of the original sequences belong to the same equivalence class as the original sequences so they are not considered as separate sequences.

The extended expression for the *multiplicative coefficients* that include the frequency term $k \cdot n$ is[1]

[1] We use $X_U(n)$ to denote Zadoff-Chu sequences with a frequency shift as opposed to sequences without a frequency shift that we denote by $Y_U(n)$.

$$X_U(n) \equiv U \cdot \frac{n(n+1)}{2} + k \cdot n \equiv U \cdot \frac{n(n+1+2U^{-1} \cdot k)}{2}, \tag{5}$$

where U^{-1} is the inverse of U modulo P. We can note that $1 + 2U^{-1} \cdot k$ is an odd integer and we will denote it by K.

So (5) becomes

$$X_U(n) \equiv U \cdot \frac{n(n+K)}{2}. \tag{6}$$

Since K must be an odd integer we see that this expression reduces to (1) for $K = 1$.

Now we can introduce our new expression for Zadoff-Chu sequences which is obtained from (6) if we choose $K = P$, which is possible as P is an odd prime. So the new expression is

$$X_U(n) \equiv U \cdot \frac{n(n+P)}{2}\ . \tag{7}$$

The advantage of this new Zadoff-Chu expression, which will become clear in subsequent sections, is that it reveals the connection between Zadoff-Chu sequences and the Quadratic Residues Theory [7]. In addition, it is easy to see that the compact expression (7) is valid not only for odd length but also for even length Zadoff-Chu sequences, which is not the case with the standard definition (where, a separate expression is needed for even length[2]) [1]. However, in this paper we will not deal with even length sequences and we will only consider odd prime lengths.

2.3 Relation between New and Standard Definition

In order to be able to use our new results in systems that are based on the standard definition of Zadoff-Chu sequences, we relate the new and the standard expression in the following. We will denote the sequences generated by the standard definition by $y_U(n)$ and their *multiplicative coefficients* by $Y_U(n)$. We start the derivation form the cyclically time shifted version of the new Zadoff-Chu sequence $X_U(n)$ expression (7) as follows

$$\begin{aligned} X_U(n+m) &\equiv U \cdot \frac{(n+m)(n+m+P)}{2} \equiv U \cdot (n+m) \cdot \frac{(n+1)+(P-1+m)}{2} \\ &\equiv U \cdot \left(n\frac{(n+1)}{2} + n\frac{(P-1+m)}{2} + m\frac{(n+1)}{2} + m\frac{(P-1+m)}{2} \right) \\ &\equiv U \cdot \left(n\frac{(n+1)}{2} + n\frac{(P-1+m)}{2} + m\frac{n}{2} + \frac{m}{2} + m\frac{(P-1+m)}{2} \right) \\ &\equiv U \cdot \left(n\frac{(n+1)}{2} + n\frac{(P-1+2m)}{2} + m\frac{(P+m)}{2} \right). \end{aligned} \tag{8}$$

[2] According to the standard definition, Zadoff-Chu sequences are defined for even lengths by $Y_U(n) = U \cdot n^2/2$.

If we choose $m = \frac{P+1}{2}$ the second term vanishes because it is a multiple of P (which is equal to 0 mod P) and we obtain

$$X_U\left(n+\frac{P+1}{2}\right) \equiv Y_U(n) + U \cdot \frac{\frac{P+1}{2}(P+\frac{P+1}{2})}{2} \equiv Y_U(n) + X_U\left(\frac{P+1}{2}\right). \quad (9)$$

Hence, a sequence following the standard expression can be obtained from the corresponding sequence following the new expression as follows

$$\begin{aligned} Y_U(n) &\equiv X_U\left(n+\tfrac{P+1}{2}\right) - X_U\left(\tfrac{P+1}{2}\right) \\ &\equiv X_U\left(n+\tfrac{P+1}{2}\right) - U \cdot \tfrac{\frac{P+1}{2}(\frac{P+1}{2}+P)}{2} \ . \end{aligned} \quad (10)$$

We observe that the first term on the right hand side is a cyclically time shifted version of a Zadoff-Chu sequence following the new definition. The shift is approximately equal to half the sequence length $\frac{P+1}{2}$. The second term is an integer constant phase shift depending only on P and U.

2.4 Examples

Table 1. gives an example of Zadoff-Chu sequences of length 7 calculated using the standard expression (1) and Table 2. gives the same sequences calculated using the new proposed definition (7).

Table 1. Multiplicative coefficients of Zadoff-Chu sequences of length 7 - standard definition

n	**0**	**1**	**2**	**3**	**4**	**5**	**6**	Sequence Elements
$Y_1(n)$	0	1	3	6	3	1	0	0, 1, 3, 6
$Y_2(n)$	0	2	6	5	6	2	0	0, 2, 5, 6
$Y_3(n)$	0	3	2	4	2	3	0	0, 2, 3, 4
$Y_4(n)$	0	4	5	3	5	4	0	0, 3, 4, 5
$Y_5(n)$	0	5	1	2	1	5	0	0, 1, 2, 5
$Y_6(n)$	0	6	4	1	4	6	0	0, 1, 4, 6

The main difference that can be observed, from the above tables, is that the standard expression generates sequences whose elements constitute sets which are unique to each sequence. The new expression generates sequences having only two different sets[3] of elements **{0, 1, 2, 4}** and {*0, 3, 5, 6*}. So the sequences can be divided into two groups depending on the set of elements they contain. The first group of sequences $\{X_1(n), X_2(n), X_4(n)\}$ contains only elements **{0, 1, 2, 4}** and the second group of sequences $\{X_3(n), X_5(n), X_6(n)\}$ contains only elements {*0, 3, 5, 6*}. Note that the only element common to both sets is 0. The mathematical derivation of this property is given in the next section. Also note that the same numbers **{1, 2, 4}** and {*3, 5, 6*} appear in the sets of

[3] To make it more obvious one set is shown in bold and the other one in italic characters.

Table 2. Multiplicative coefficients of Zadoff-Chu sequences of length 7 - new definition ([7])

n	**0**	**1**	**2**	**3**	**4**	**5**	**6**	Sequence elements
$X_1(n)$	0	4	2	1	1	2	4	**0, 1, 2, 4**
$X_2(n)$	0	1	4	2	2	4	1	**0, 1, 2, 4**
$X_3(n)$	0	5	6	3	3	6	5	*0, 3, 5, 6*
$X_4(n)$	0	2	1	4	4	1	2	**0, 1, 2, 4**
$X_5(n)$	0	6	3	5	5	3	6	*0, 3, 5, 6*
$X_6(n)$	0	3	5	6	6	5	3	*0, 3, 5, 6*

sequence elements and also as the sequences root indexes U. We can also note that, mathematically, **{1, 2, 4}** are quadratic residues and that {*3, 5, 6*} are quadratic non-residues, while 0 is neither a residue nor a non-residue [7].

A general comparison of the standard and the new expression is given in Table 3.

Table 3. Comparison of the sequences generated by the standard and the new expression

	Standard expression	**New expression**
Symmetry	$Y_U(n-1) = Y_U(P-n)$	$X_U(n) = X_U(P-n)$
Unique element	$Y_U((P-1)/2)$	$X_U(0)$
Elements with value 0	$Y_U(0)$ and $Y_U(P-1)$	$X_U(0)$
Sets of values	All sets are different	Only 2 different sets

Finally we note that according to ([10]), sequences of length 7 given by the standard expression Y_U can be calculated from the sequences given by the new expression X_U by $Y_U(n) \equiv X_U(n+4) - U$ which is easily verified by checking Tables 1. and 2.

3 Decimation (Re-Sampling) of Zadoff-Chu Sequences

Here we show that a decimated (re-sampled) Zadoff-Chu sequence is also a Zadoff-Chu sequence. The resulting sequence is just another Zadoff-Chu sequence with a different root index U. The root index of the resulting sequence is equal to the original root index multiplied by the squared decimation factor.

3.1 The Decimation Formula

For a decimation factor K, we can write

$$\begin{aligned} X_U(K\cdot n) &\equiv U\cdot K\cdot n\cdot \frac{K\cdot n+P}{2} \equiv U\cdot K\cdot n\cdot \frac{K\cdot n+(K\cdot P-K\cdot P)+P}{2} \\ &\equiv U\cdot K\cdot n\cdot \frac{K\cdot n+K\cdot P}{2} - U\cdot K\cdot n\cdot \frac{K\cdot P-P}{2} \\ &\equiv U\cdot K^2\cdot \frac{n(n+P)}{2} - U\cdot P\cdot n\cdot \frac{K(K-1)}{2}. \end{aligned} \tag{11}$$

Since $\frac{K(K-1)}{2}$ is an integer, the second term is an integer multiple of P so it is equal to zero modulo P. Thus finally we have

$$X_U(K \cdot n) \equiv U \cdot K^2 \cdot \frac{n(n+P)}{2} \equiv X_{U \cdot K^2}(n) \tag{12}$$

and, hence, a decimated Zadoff-Chu sequence (with root index U) is equal to another Zadoff-Chu sequence with root index equal to: $UK^2 \bmod P$. By exchanging the left- and the right-hand side and replacing U by V we can write

$$X_{V \cdot K^2}(n) \equiv X_V(K \cdot n) \tag{13}$$

Hence, a sequence with the root index $U \equiv VK^2$ can be calculated by decimating the sequence $X_V(n)$.

For $V = 1$ we obtain

$$X_{K^2}(n) \equiv X_1(K \cdot n), \tag{14}$$

which is a very important special case. Finally, this means that any sequence with root index

$$U \equiv K^2 \tag{15}$$

can be obtained by decimating the seed sequence whose root index is $U = 1$.

The importance of this result lies in the fact that decimation does not require recalculation of sequence elements and that it is in fact just a reordering of sequence elements (in mathematical language - a permutation).

We note that a number U that satisfies the equation $U = K^2 \bmod P$ is a *quadratic residue* [7] and is studied in detail in modular arithmetic, which is a branch of number theory. Here, we do not use the usual terminology from this area of mathematics, but only note that many theoretical results from the theory of quadratic residues can be applied to Zadoff-Chu sequences, which will be the subject of future research.

Note that not all root indices can be expressed as $K^2 \bmod P$. In fact as $K^2 \equiv (P-K)^2$ we must restrict K to $K = 1,\ 2,\ \ldots (P-1)/2$ in order not to generate duplicate values. This means that the expression $K^2 \bmod P$ can produce only $(P-1)/2$ different values and there are $(P-1)/2$ values [7] that cannot be produced by this expression. If one such value is V then all other such values (called quadratic non-residues [7]) can be generated by

$$U = V \cdot K^2 \bmod P;\ K = 1, 2, \ldots (P-1)/2. \tag{16}$$

Now we can use (13) to generate the sequences when U is not a residue:

$$X_{V \cdot K^2}(n) \equiv X_V(K \cdot n) \tag{17}$$

This means that we need another complex Zadoff-Chu sequence $x_V(n)$ in order to generate all sequences with a root index which is a non-residue. In summary, we need the $x_1(n)$ sequence to generate $(P-1)/2$ sequences with a root index which is a residue and a $x_V(n)$ sequence to generate $(P-1)/2$ sequences with a root index which is a non-residue. We have to note that the value of V is not unique – we can choose any non-residue for V. Also it is not necessary to use $U = 1$ as the first seed sequence. Any U which is a residue can be chosen.

3.2 Decimation and the New Expression for Zadoff-Chu Sequences

Here we explain why we need the new expression for Zadoff-Chu sequences to derive the decimation formula a why the decimation formula does not hold for the standard definition.

The decimation formula states that the decimated sequences are rearranged versions (permutations) of the original sequence. This means that all decimated sequences have elements from the same set. We have seen that sequences following the new definition have this property. We can see from expression (10) why the decimation formula does not hold for the standard definition. According to (10) Y_U sequences are obtained from X_U by adding a term that depends on U, which results in a different set of elements for each U.

4 Efficient Calculation of Zadoff-Chu Sequences

Based in previous formula, we give a formulation of the algorithm for efficient generation of Zadoff-Chu sequences consisting of 4 off-line steps and the last step implemented in real-time.

4.1 The Generation Algorithm

The algorithm for the efficient generation of Zadoff-Chu sequences can be formulated in the following manner. Steps 1 - 4 are performed in design-time or during device initialization. Step 5 is performed in real-time. We illustrate the algorithm with sequences from the previous example for P=7

1. Choose V from the set of quadratic non-residues. (In our example we choose $V = 3$ but values 5 or 6 could also be used.)
2. Generate and store the two seed complex Zadoff-Chu sequences[4] $x_1(n)$ and $x_V(n)$ according to (7).
   (In our example let $\mathrm{W} = e^{-2\pi j/7}$ then $x_1 = [1, \mathrm{W}^4, \mathrm{W}^2, \mathrm{W}^1, \mathrm{W}^1, \mathrm{W}^2, \mathrm{W}^4]$ and $x_3 = [1,\ \mathrm{W}^5, \mathrm{W}^6, \mathrm{W}^3, \mathrm{W}^3, \mathrm{W}^6, \mathrm{W}^5]$.)
3. Generate a table which determines which U (excluding 0) is a quadratic residue "R" and which is a non-residue "N". In practice "R" and "N" would be represented by 0's and 1's. This table determines which seed sequence will be used.
   (For our example this table is [R, R, N, R, N, N] .)
4. Generate a table for the inverse mappings $U \rightarrow K_1$ ($K_1 = K_1(U)$) for the mapping $U \equiv {K_1}^2$ and $U \rightarrow K_2$ for the mapping $U \equiv V{K_2}^2$ ($K_2 = K_2(U)$) for $K_1, K_2 = 1 \ldots (P-1)/2$. Since each U is either a residue or non-residue these two mappings can be stored in a single combined table.
   (Table 4. summarizes all the tables from steps 1 - 5. from our example)

[4] Note here that because of the symmetry only half of the sequence needs to be stored. That is, we can store only $x_1(0, \ldots 3) = [1, \mathrm{W}^4, \mathrm{W}^2, \mathrm{W}^1]$ and $x_3(0, \ldots 3) = [1, \mathrm{W}^5, \mathrm{W}^6, \mathrm{W}^3]$.

Table 4. Tables needed for efficient generation of Zadoff-Chu sequences of length 7

1	**U**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
2	**Residue/Non-residue R/N**		R	R	N	R	N	N
3	K_1 **for residues**		*1*	*3*		*2*		
4	K_2 **for non-residues (V=3)**				**1**		**2**	**3**
5	**K combined table for** K_1 **and** K_2		*1*	*3*	**1**	*2*	**2**	**3**
6	**First seed sequence** x_1	W^0	W^4	W^2	W^1	W^1	W^2	W^4
7	**Second seed sequence** x_3	W^0	W^5	W^6	W^3	W^3	W^6	W^5

5. In real-time, read one of the two stored seed sequences (in our example rows 6 or 7 from Table 4.) beginning with the first element and by incrementing the index by $K(U)$ (in our example row 5 of Table 4.) depending on whether U is a residue or a non-residue (in our example row 2 of Table 4.).
   (In our example the sequences that can be generated from the two seed sequences $x_1(n)$ and $x_3(n)$ in this manner are:

   $x_2(n) \equiv x_1(3n)$; as 2 is a residue and $K_1(2) = 3$;
   $x_4(n) \equiv x_1(2n)$; as 4 is a residue and $K_1(4) = 2$;
   $x_5(n) \equiv x_3(2n)$; as 5 is non-residue and $K_2(5) = 2$;
   $x_6(n) \equiv x_3(3n)$; as 6 is non-residue and $K_2(6) = 3$.)

4.2 Hardware Implementation of the Proposed Algorithm

The hardware implementation requires address generating circuitry and memory for storing the two seed sequences. The address generator has to calculate the following address

$$X_U(n) = n \cdot K(U) \bmod P. \tag{18}$$

This address can recursively be calculated as follows

$$X_U(0) = 0;\ X_U(n) = X_U(n-1) + K(U) \bmod P. \tag{19}$$

We recognize this algorithm as a perfect integrator. So the address generator consists of a register and an adder modulo P (adding $K(U)$ to the previous value). Here we note that $X_U(0)$ can be preset to a non-zero value, thus generating different cyclic time shifts of the Zadoff-Chu sequence. For $X_U(0) = (P-1)/2$, we generate sequences according to the standard definition (2) except for the constant phase shift $X_U((P+1)/2)$ from (10). The entire sequences generator is shown in Figure 1.

We end this discussion with a remark concerning the storage requirement. Usually we need to store two Zadoff-Chu sequences of length P (one for residues and the other for non-residues). But in some special cases we can use only one sequence. We note the fact that $X_U(n) + X_{P-U}(n) \equiv 0$ or $X_U(n) \equiv -X_{P-U}(n)$ which is the consequence of the fact that $U + (P-U) = P = 0$. Then we use a result from quadratic residue theory which states that $P-1$ is a non-residue if $P = -1 \bmod 4$ [7]. It follows that, for P prime such that $P = 4n-1$, we can

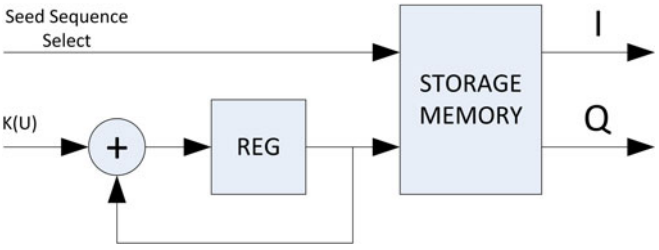


Fig. 1. Efficient generator

use $X_{P-1}(n)$ as our second seed sequence. The big advantage is that, because $X_{P-1}(n) = -X_1(n)$, we have $x_{P-1}(n) = \overline{x_1(n)}$. Hence, the second seed sequence is a complex conjugate of the first seed sequence $x_1(n)$ and it does not need to be stored separately. By adding an inverter (multiplier by -1) to the imaginary part of the first seed sequence, we obtain the second seed sequence.

Some examples of prime numbers of this form are: $3, 7, 11, 19, 23, 31, 43, \ldots$. It is interesting to note that the sequence lengths that are chosen for the LTE PRACH satisfy the above criterion: 139 ($139 = 4 \cdot 35 - 1$) and 839 ($839 = 4 \cdot 210 - 1$).

4.3 The Lookup Table Implementation

To see the advantage of this implementation we compare it to the standard lookup table implementation (using the standard definition). The lookup table implementation is based on the formula (11). We store in a memory (lookup table) all roots of unity $W_P{}^k$ for $k = 0, .. N - 1$. Then we generate the complex Zadoff-Chu sequence following the standard definition $y_U(n)$ from (11) by using the *multiplicative coefficients* $Y_U(n)$ as the address to the lookup table.

To implement the above approach we need to first generate the following address

$$Y_U(n) = U\frac{n(n+1)}{2} \bmod P. \tag{20}$$

Generating this address directly needs hardware multiplication and modulo P calculation of large numbers, which have large complexity. Fortunately, we can obtain the same result recursively by using only addition and modulo P calculation of small numbers. To derive the recursive algorithm we first calculate the difference

$$Y_U(n) - Y_U(n-1) = \left(U\frac{n(n+1)}{2} - U\frac{(n-1)n}{2}\right) \bmod P = U \cdot n \bmod P \tag{21}$$

so that $Y_U(n) = (Y_U \cdot (n-1) + U \cdot n) \bmod P$. Once again we can recognize this as a perfect integrator. The term $U \cdot n \bmod P$ can also be implemented recursively as an integrator so that the entire circuitry can be implemented as a double integrator. It goes without saying that each adder is modulo P. This implementation is shown in Figure 2.

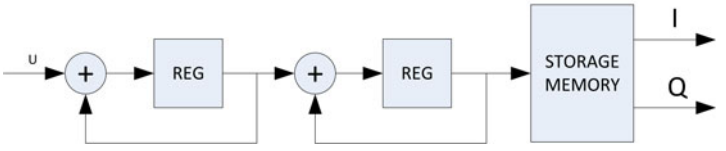


Fig. 2. Standard lookup table implementation

5 Conclusion

Two theoretical results and an efficient algorithm for generating Zadoff-Chu sequence are presented. The first result is an alternative expression for defining Zadoff-Chu sequences. This new expression reveals the internal structure of Zadoff-Chu sequences and leads to a decimation formula, which is the second contribution of this paper. Based on this new formula an efficient algorithm for generating Zadoff-Chu sequences of a given prime length is derived. Based on two pre-calculated seed sequences (stored in the memory), any desired Zadoff-Chu sequence can be generated, sample-by-sample, simply by incrementing the read index by a corresponding step value. In this manner no calculation of sequence elements is required. That is, this algorithm does not require any additions, multiplications, or trigonometric calculations to generate sequences in real-time. Finally a hardware implementation is proposed and compared to the standard lookup-table implementation to demonstrate its advantage.

We hope that this paper will influence future use of Zadoff-Chu sequences in radar and communication systems and, in particular, future wireless standards.

References

1. Chu, D.C.: Polyphase codes with good periodic correlation properties. IEEE Trans. on Information Theory 18, 531–532 (1972)
2. Frank, R.L., Zadoff, S.A.: Phase shift codes with good periodic correlation properties. IRE Trans. Inform. Theory 8, 381–382 (1962)
3. Popovic, B.M.: Generalized chirp-like Poly-phase Sequences with Optimum Correlation Properties. IEEE Trans. 38, 1406–1409 (1992)
4. Levanon, N., Mozeson, E.: Radar Signals. John Wiley & Sons, Inc., Chichester (2004)
5. Mow, W.H.: A New Unified Construction of Perfect Root-of-Unity Sequences. In: Proc. Spread Spectrum Techniques and its Applications (ISSSTA 1996), Mainz, Germany, pp. 955–959 (1996)
6. 3GPP TS 36.211 V9.0.0; 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation, Release 9 (2009)
7. Apostol, T.M.: Introduction to analytic number theory. In: Undergraduate Texts in Mathematics. Springer, New York (1976)
8. Frank, R.L.: Polyphase codes with Good Nonperiodic Correlation Properties. IEEE Trans. on Information Theory. 9, 43–45 (1963)

An Algorithm for Constructing a Fastest Galois NLFSR Generating a Given Sequence

Jean-Michel Chabloz, Shohreh Sharif Mansouri, and Elena Dubrova

Royal Institute of Technology, Forum 120
164 40 Kista, Sweden
{chabloz,shsm,dubrova}@kth.se

Abstract. The problem of efficient implementation of security mechanisms for advanced contactless technologies like RFID is gaining increasing attention. Severe constraints on resources such as area, power consumption, and production cost make the application of traditional cryptographic techniques to these technologies a challenging task. Non-Linear Feedback Shift Register (NLFSR)-based stream ciphers are promising candidates for cryptographic primitives for RFIDs because they have the smallest hardware footprint of all existing cryptographic systems. This paper presents a heuristic algorithm for constructing a fastest Galois NLFSR generating a given sequence. The algorithm takes an NLFSR in the Fibonacci configuration and transforms it to an equivalent Galois NLFSR which has the minimal delay. Our key idea is to find a best position for a given feedback connection without changing the positions of the other feedback connections. We use a technology dependent cost function which approximates the delay of an NLFSR after the technology mapping. The experimental results on 57 NLFSRs used in existing stream ciphers show that, on average, the presented algorithm allows us to decrease the delay by 25.5% as well as to reduce the area by 4.1%.

1 Introduction

Non-Linear Feedback Shift Registers (NLFSRs) are a generalization of Linear Feedback Shift Registers (LFSRs) in which the current state is a non-linear function of the previous state [10].

LFSRs are one of the most popular devices for generating pseudo-random sequences [2]. They are also used to perform data/test decompression and test/response compaction [19]. LFSRs are simple, fast, and easy to implement in software and hardware. Applications of LFSRs include error-detection and correction, data transmission, data compression, data hiding, white noise generation, Monte Carlo simulation, cryptography, and many others [8,10,2,19]. Therefore, LFSR synthesis has drawn considerable attention through the years.

NLFSRs have received much less attention compared to LFSRs. Previous works focused mostly on the problem of constructing an NLFSR with the maximum period (see [5] for an excellent overview), or on how to find an NLFSR with the smallest number of bits which generates a given sequence [15].

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 41–54, 2010.

The main application area of NLFSRs at present is cryptography [24]. Although LFSRs can generate pseudo-random sequences with the same uniform statistical distribution of 0's and 1's as in a sequence generated by a truly random method [10], they are not cryptographically secure. The structure of an n-bit LFSR can be easily deduced by observing $2n$ consecutive bit of its sequence [17]. On the contrary, an adversary might need $O(2^n)$ bits of a sequence to find the n-bit NLFSR which generates it [4]. Pseudo-random sequences generated by NLFSRs are normally hard to break with existing cryptanalytic methods [13,23].

A number of NLFSR-based stream ciphers for resource-constrained hardware applications have been designed [6,12,1,9,7]. An NLFSR-based stream cipher encrypts the information by combining plain text bits with a pseudo-random bit sequence generated by the NLFSR [21]. The resulting encrypted information can be transformed back into its original form only by an authorized user possessing the secret cryptographic key.

At present, NLFSR-based stream ciphers are the most promising candidates for cryptographic primitives for advanced contactless technologies like RFID because they have the smallest hardware footprint of all existing cryptographic systems [22]. The lack of adequate security and data-protection mechanisms for RFIDs blocks off a variety of potential applications of RFIDs in the pharmaceutical, medical, transportation, consumer-payment, and retail industries [14]. This motivates research on resource-efficient design and implementation of NLFSR-based stream ciphers.

Similarly to LFSRs, an NLFSR can be implemented either in the Fibonacci or in the Galois configuration (see Figures 1 and 2). In the former, the feedback is applied to the input bit of the shift register only, while in the latter the feedback can potentially be applied to every bit. The depth of the circuits implementing the feedback functions of the Galois configuration is usually smaller than the depth of the circuit implementing the feedback function of the Fibonacci configuration [3]. This makes the Galois configuration attractive for stream ciphers for which high throughput is very important. For example, by re-implementing the NLFSR-based stream cipher Grain-80 [12] from its original Fibonacci configuration to the Galois configuration, it is possible to double the throughput of the 1 bit/cycle version of Grain-80 with no penalty in area or power [16].

In [3], sufficient conditions for equivalence of NLFSRs in the Fibonacci and the Galois configurations have been formulated. This result laid a theoretical foundation of the transformation between the two configurations. However, it left open the problem of selecting a fastest Galois NLFSR generating a given sequence. This problem is addressed in this paper. We present a heuristic algorithm which takes an NLFSR in the Fibonacci configuration and transforms it to an equivalent Galois NLFSR which has the minimal delay. The key idea is to find a best position for a given feedback connection without changing the positions of the other connections. The "best" is defined as a position which minimizes the cost function approximating the delay of the NLFSR after the technology mapping. The experimental results on 57 NLFSRs used in existing

stream ciphers show that the presented approach allows us to decrease the delay of NLFSRs by 25% on average.

The paper is organized as follows. Section 2 gives an introduction to NLFSRs. Section 3 describes the presented transformation algorithm. Section 4 shows the experimental results. Section 5 concludes the paper and discusses open problems.

2 Background

In this section we describe basic definitions and notation used in the paper. Most of our terminology is from [10].

2.1 Non-linear Feedback Shift Registers

A *Non-Linear Feedback Shift Register (NLFSR)* consists of n binary storage elements, called *bits*. Each bit $i \in \{0, 1, \ldots, n-1\}$ has an associated *state variable* x_i which represents the current value of the bit i and a *feedback function* $f_i : \{0,1\}^n \rightarrow \{0,1\}$ which determines how the value of i is updated. For any $i \in \{0, 1, \ldots, n-1\}$, f_i depends on $x_{(i+1) mod\ n}$ and a subset of variables from the set $\{x_0, x_1, \ldots, x_i\}$.

A *state* of an NLFSR is a vector of values of its state variables $x = (x_0, x_1, \ldots, x_{n-1})$. At every clock cycle, the next state of an NLFSR is determined from the current state by simultaneously updating the value of each bit i to the value of f_i.

Feedback functions of NLFSRs are usually represented in the *Algebraic Normal Form (ANF)* which is a polynomial in $GF(2)$ of type

$$f(x) = \sum_{i=0}^{2^n-1} c_i \cdot x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{n-1}^{i_{n-1}},$$

where $c_i \in \{0,1\}$ and $(i_0 i_1 \ldots i_{n-1})$ is the binary expansion of i.

The *dependence set* of a Boolean function $f(x)$ is defined as

$$dep(f) = \{i \mid f|_{x_i=0}(x) \neq f|_{x_i=1}(x)\},$$

where $f|_{x_i=j}(x) = f(x_0, \ldots, x_{i-1}, j, x_{i+1}, \ldots, x_{n-1})$ for $j \in \{0,1\}$.

Two NLFSRs are *equivalent* if their sets of output sequences are equal. The conditions for equivalence of NLFSRs were presented in [3].

Similarly to LFSRs, an NLFSR can be implemented in two configurations shown in Figures 1 and 2: *Fibonacci* (also called *external feedback*), or *Galois*[1] (also called *internal feedback*).

In the Fibonacci configuration, the feedback can be applied from any bit to the left-most bit. Since all feedback functions except f_{n-1} are of type $f_i = x_{i+1}$, f_{n-1} is often called *the feedback function* of a Fibonacci NLFSR. We use this name throughout the paper when there is no ambiguity. In the Galois configuration, the feedback can be applied from any bit i, $i \in \{0, 1, \ldots, n-1\}$, to any bit j such that $j \geq i$.

[1] An LFSR in the Galois configuration implements the polynomial division in a Galois field, hence the name. The NLFSR in Figure 2 does not match this classical definition, therefore it is not entirely justified to call it "Galois".

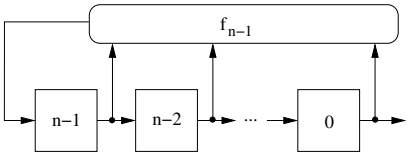


Fig. 1. The Fibonacci configuration of NLFSRs

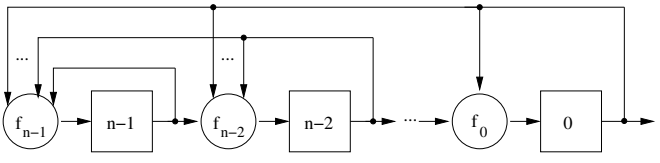


Fig. 2. The Galois configuration of NLFSRs

The operating speed of a Fibonacci NLFSR is limited by the depth of the circuit implementing its feedback function. A transformation to an equivalent Galois configuration can potentially reduce the depth of the circuits implementing feedback functions of the individual bits, thus increasing the operating speed. In the next section we describe a transformation introduced in [3] which we use as a basis of our algorithm.

Apart from the Fibonacci and the Galois configurations, there are also some other interesting types of NLFSRs which we do not consider in this paper, e.g. [18].

2.2 Transformation of NLFSRs

For LFSRs, the Fibonacci and the Galois configurations are unique. One configuration can be easily transformed into another by reversing the order of the feedback connections and adjusting the initial state [8].

For NLFSRs, however, the Galois configuration is not unique. Usually, there are many n-bit Galois NLFSRs which are equivalent to a given n-bit Fibonacci NLFSR. On the other hand, not every n-bit Galois NLFSR has an equivalent n-bit Fibonacci NLFSR.

The latter is because, while an output sequence of every n-bit Fibonacci NLFSR can be described by a non-linear recurrence of order n [20], for n-bit Galois NLFSRs such a recurrence does not always exist.

It was shown in [3] that one class of NLFSRs for which a recurrence of order n always exists is *uniform* NLFSRs, defined as follows.

Definition 1. *An n-bit NLFSR is uniform if, for some $n < \tau \leq 0$:*

$$(a)\quad f_i(x) = x_{i+1} \quad \textit{for} \quad 0 \leq i < \tau$$
$$(b)\quad f_i(x) = x_{(i+1) mod\ n} \oplus g_i(x_0, \ldots, x_\tau) \quad \textit{for} \quad \tau \leq i < n$$

where $dep(g_i) = \{0, 1, \ldots, \tau\} - \{(i+1) mod\ n\}$.

We can see that, in a uniform NLFSR, the feedback is taken only from bits in positions not greater than τ and it is fed only to bits in positions not smaller than τ. The bit τ is called the *terminal bit*.

A uniform Galois NLFSR can be constructed from a given Fibonacci NLFSR by repeatedly applying the following simple operation.

Definition 2. *Let f_i and f_j be feedback functions of the bits i and j of an n-bit NLFSR, respectively, represented in ANF. The operation shifting, denoted by $f_i \xrightarrow{M} f_j$, moves a set of monomials M from f_i to f_j. The index of each variable x_k of each monomial in M is changed to $x_{(k-i+j) mod\ n}$.*

As an example, consider a 4-bit NLFSR N_1 with the following feedback functions:

$$\begin{aligned} f_3 &= x_0 \oplus x_1 \\ f_2 &= x_3 \oplus x_1 \oplus x_0x_1 \\ f_1 &= x_2 \\ f_0 &= x_1. \end{aligned}$$

If we apply the shifting $f_2 \xrightarrow{\{x_1\}} f_1$ to N_1, we get an NLFSR N_2 with the following feedback functions:

$$\begin{aligned} f_3 &= x_0 \oplus x_1 \\ f_2 &= x_3 \oplus x_0x_1 \\ f_1 &= x_2 \oplus x_0 \\ f_0 &= x_1. \end{aligned}$$

The next theorem describes a sufficient condition for equivalence of NLFSRs before and after shifting.

Theorem 1. [3] *Given a uniform NLFSR with the terminal bit τ, a shifting $f_\tau \xrightarrow{M} f_{\tau'}$, $\tau' < \tau$, results in an equivalent NLFSR if the transformed NLFSR is uniform as well.*

In the example above, the NLFSRs N_1 is a uniform NLFSR with the terminal bit 2. As we can see, the shifting $f_2 \xrightarrow{\{x_1\}} f_1$ results in a uniform NLFSR N_2 with the terminal bit 1. Therefore, N_1 and N_2 are equivalent.

The work [3] laid a theoretical foundation of the transformation between the Fibonacci and the Galois configurations of NLFSRs. However, it left open the problem of selecting a "best" NLFSR for a given optimization target. In the next section, we present a heuristic algorithm for constructing Galois NLFSRs with a minimal delay.

3 Transformation Algorithm

In order to construct a Galois NLFSR which has the minimum delay, we have to search among different allocations of monomials to the feedback functions and evaluate the cost of each allocation. The search space consists of all possible n-bit

Algorithm 1. Estimation of the cost of a function f

```
1: M := {m_j | m_j is a monomial of the ANF of f}
2: for each m_j ∈ M do
3:    C(m_j) := C(AND) · ⌈log_2(|m_j|)⌉
                 /*|m_j| is the number of variables in m_j*/
4: end for
5: C := (C(m_0), C(m_1), ..., C(m_{|M|-1}))
6: while |C| > 1 do
7:    Find the lowest and the second lowest elements of C
8:    Delete the lowest element of C
9:    Add C(XOR) to the second lowest element in C
10: end while
11: C(f) := the single element of C
12: Return C(f)
```

Galois NLFSRs which are equivalent to a given n-bit Fibonacci NLFSR. The size of the search space is $O(n^k)$ where k is the number of monomials in the ANF of the feedback function of the Fibonacci NLFSR. Although in the worst case $k = O(2^n)$, in the NLFSRs used in existing stream ciphers k is usually smaller than 32 (for hardware efficiency reasons). On the other hand, n can be as large as 128 (for cryptographic security reasons). So, an exhaustive search is unfeasible.

We therefore designed a heuristic algorithm which explores only a part of the search space. The key idea is to find a best position for a given monomial without changing the positions of the other monomials. A "best" is defined as a position which minimizes the cost function approximating the delay of the NLFSR. We start with a description of the cost function and then, in Subsection 3.2, we present the strategy for allocating monomials.

3.1 Cost Function

Ideally, the cost function should return the maximum of all delays of the feedback functions of a given NLFSR, i.e. its critical path. However, the exact value of the delay can only be estimated after technology mapping. Performing technology mapping to evaluate each allocation of monomials is obviously too expensive. Instead, we approximate the delay by assuming that it is equal to the delay of a depth-optimal tree of 2-input AND and 2-input XOR gates implementing the function. The pseudo-code of the algorithm for constructing such a tree is shown in Algorithm 1.

For a given feedback function f_i, the algorithm first computes the cost $C(m_j)$ of each monomial m_j from the set M of all monomials of the ANF of f_i. The monomials are assumed to be implemented using 2-input AND gates. Let $C(AND)$ denote the delay of a 2-input AND gate. Then, the cost of a monomial m_j is given by the depth of the optimal AND-tree that implements it:

$$C(m_j) = C(AND) \cdot \lceil \log_2(|m_j|) \rceil$$

where $|m_j|$ is the number of variables in the monomial m_j.

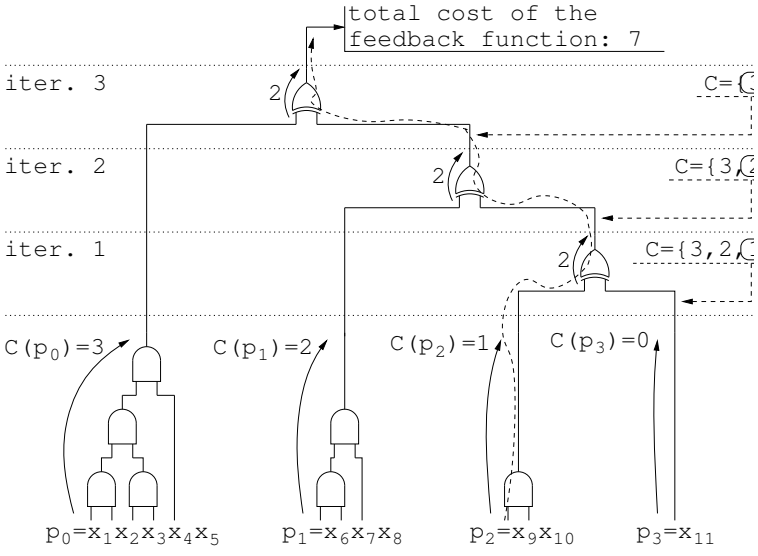


Fig. 3. An example of cost function calculation

Let $C = (C(m_0), C(m_1), \ldots, C(m_{|M|-1}))$ be an ordered vector of costs of the monomials of M. Next, the algorithm builds iteratively a depth-optimal XOR-tree on the top of the obtained AND-trees. At each step, one 2-input XOR gate fed by the sub-circuits corresponding to the two lowest-cost elements of C is added to the XOR-tree. The lowest-cost element of C is then removed from C and the delay of a 2-input XOR gate, $C(XOR)$, is added to the cost of the second lowest-cost element of C. The algorithm terminates when a single element is left in C. This element is the cost $C(f_i)$ of the feedback function f_i.

The worst-case complexity of Algorithm 1 is $O(|M| \log |M|))$.

The cost of an n-bit NLFSR is determined from the costs of its feedback functions as follows:

$$C(NLFSR) = \max_{0 \le i < n} (C(f_i)). \tag{1}$$

In our current implementation of Algorithm 1, the costs of the 2-input AND and XOR gates are set to $C(AND) = 1$ and $C(XOR) = 2$ to match the corresponding normalized delays in the TSMC 90nm CMOS technology library. By changing these parameters, the algorithm can be adjusted to other ASIC standard-cell technology libraries.

Figure 3 shows an example of the execution of Algorithm 1. At each iteration, two sub-circuits with the lowest cost are composed together using an XOR gate and the cost of the resulting circuit is computed. The dashed arrow shows the critical path determining the cost of the feedback function.

3.2 Allocation of Monomials

The pseudo-code of the algorithm for the allocation of monomials is summarized in Algorithm 2.

Let f be the feedback function of a Fibonacci NLFSR. Let M be a set containing all monomials of the ANF of f except x_0. Note that the monomial x_0 is usually contained in the feedback function of a Fibonacci NLFSR to make the NLFSR branchless [8].

The algorithm starts with an empty n-bit NLFSR in which all feedback functions are of type $f_i = x_{(i+1) mod\ n}$. Initially, the cost of each feedback function is 0. At every step, one monomial from the set M is shifted to one of the feedback functions until M is exhausted.

The shifting of monomials is performed in order of their priority. The priorities are assigned according to the following criteria:

- Priority is given to the monomials that can be shifted to only a few positions.
- Priority is given to the monomials whose shifting is expected to have a higher impact on the critical path of the NLFSR. Usually, these are larger monomials.

The number of Allowed Positions to which a monomial m_j can be shifted, $AP(m_j)$, is determined by the following factors:

1. The minimum terminal bit of the Galois NLFSR. According to [3], to guarantee the equivalence of NLFSRs before and after the transformation, monomials cannot be shifted to the positions lower that the minimum terminal bit τ_{min} which is given by:

$$\tau_{min} = \max_{0 \le i < |M|} (max\_index(m_i) - min\_index(m_i)),$$

   where $min\_index(m_i)$ ($max\_index(m_i)$) denotes the minimum (maximum) index of variables the monomial m_i.
2. Uniformity of NLFSRs. In our algorithm, we impose a requirement that a monomial m_j can be shifted to the bit position $n - 1 < k \le \tau_{min}$ only if the NLFSR after shifting $f_{n-1} \overset{m_j}{\rightarrow} f_k$ is uniform. By Theorem 1, this implies that the equivalence of NLFSRs is preserved after each shifting. Thus, the NLFSR obtained by the presented algorithm is equivalent to the original Fibonacci NLFSR by construction.
3. The desired degree of parallelization. It is common to increase the throughput of a stream cipher by introducing parallelism in its architecture [12,1,9]. In a k-bit/cycle version of a cipher, at each clock cycle, blocks of k duplicated feedback functions produce k output bits in parallel. It is easy to see that, to ensure k-bit/cycle degree of parallelization of an n-bit Galois NLFSR with the terminal bit τ, all bits except

$$n - i \cdot k - 1,\ \forall i = \{0, 1, \ldots, \lfloor (n - \tau - 1)/k \rfloor - 1\}$$

   should have the feedback functions of type $f = x_{(i+1) mod\ n}$.

Algorithm 2. Transformation of an n-bit Fibonacci NLFSR to the Galois configuration with a minimal delay

1: $f :=$ feedback function f_{n-1} of the Fibonacci NLFSR
2: $M := \{m_j |\ m_j$ is a monomials of the ANF of $f\} - \{x_0\}$
3: **for** each $i \in \{0, 1, \ldots, n-1\}$ **do**
4: $\quad f_i := x_{(i+1) mod\ n}$ /*Initialization of the Galois NLFSR*/
5: $\quad C(f_i) := 0$
6: **end for**
7: **while** $M \neq \emptyset$ **do**
8: $\quad$ **for** each $m_j \in M$ **do**
9: $\quad\quad$ Calculate $priority(m_j)$ using equation (2)
10: $\quad$ **end for**
11: $\quad$ Select m_i with the highest $priority(m_i)$
12: $\quad$ Shift m_i to f_k with the minimum cost $C(f_k \oplus m_i)$
13: $\quad M := M - \{m_i\}$
14: **end while**
15: Return $f_0, f_1, \ldots, f_{n-1}$

4. The NLFSR state bits used in combining functions. Some stream ciphers, e.g. Grain [12] and Trivium [1], use not only the output bit of the NLFSR, but also several other state bits to generate their pseudo-random sequences. Two equivalent NLFSRs in the Fibonacci and the Galois configurations follow different sequences of states. Therefore, in order to preserve the original encryption algorithm, the terminal bit of the Galois NLFSR should have a position not smaller than any bit position used in a combining function.

The Average Expected Cost of a monomial m_j, $AEC(m_j)$, is computed by shifting m_j to each of the allowed feedback functions, f_k, computing the new cost of the feedback function, $C(f_k \oplus m_j)$, and taking the average over all new costs.

The priority of a monomial m_j is computed from $AP(m_j)$ and $AEC(m_j)$ as follows:

$$priority(m_j) = \frac{AEC(m_j)}{\max\limits_{0 \leq i < |M|} (AEC(m_i))} + \frac{\max\limits_{0 \leq i < |M|} (AP(m_i))}{AP(m_j)} \tag{2}$$

The monomial m_i with highest $priority(m_i)$ is then shifted to the feedback function f_k which had the minimum cost $C(f_k \oplus m_i)$ during the computation of $AEC(m_j)$. Note that since shifting is always done from the feedback function f_{n-1} of the Fibonacci NLFSR, by Definition 2, the index of each variable x_j of m_i is reduced by $n - k - 1$. The algorithm terminates when all monomials are allocated.

The worst-case complexity of Algorithm 2 is $O(n|M|^2 \log |M|))$. A limitation of the presented algorithm is the requirement that an NLFSR should remain uniform after each shifting of a monomial. In some rare cases, a set of monomials

rather than a single monomial has to be shifted to preserve uniformity. For example, for the 4-bit Fibonacci NLFSR with the feedback function

$$f_3 = x_0 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2$$

shifting of either x_1x_3, or x_2x_3, or x_2 to any other feedback function gives us a non-uniform NLFSR. However, it is possible to construct a uniform NLFSR by shifting the set of monomials $\{x_1x_3, x_2x_3\}$ to the feedback function f_2:

$$f_3 = x_0 \oplus x_2$$
$$f_2 = x_3 \oplus x_0x_2 \oplus x_1x_2.$$

4 Experimental Results

In this section, we evaluate Algorithms 1 and 2 on random NLFSRs and well as on NLFSRs of existing stream ciphers.

4.1 Results for Random NLFSRs

To evaluate the presented cost function, we generated 2000 128-bit Fibonacci NLFSRs with random feedback functions. For each NLFSR, we compared the cost of its feedback function computed by Algorithm 1 to the delay of the NLFSR after technology mapping obtained by synthesizing the NLFSR with Cadence RTL compiler using the TSMC 90nm CMOS library.

The results are shown in Figure 4. We can see a good correlation between the cost function and the delay after the technology mapping. The dashed line shows the linear interpolation.

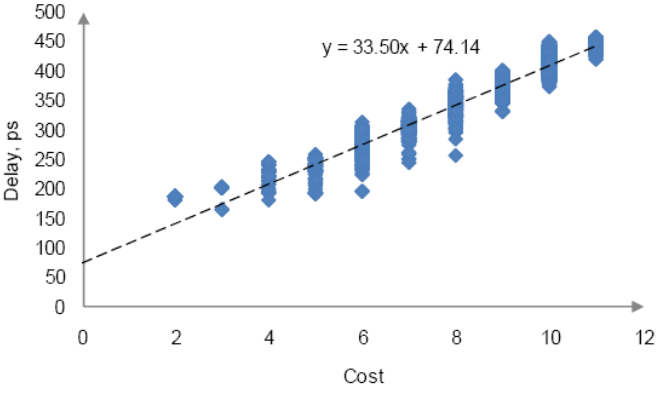


Fig. 4. Results for 2000 randomly generated NLFSRs

4.2 Results for Stream Ciphers

To further evaluate the presented approach, we applied Algorithm 2 to 57 Fibonacci NLFSRs used in the following stream ciphers:

1. Grain-80/128 [12]: It consists of one 80/128-bit NLFSR and one 80/128-bit LFSR connected in series, and two functions combining selected state bits and outputs.
2. VEST stream cipher [9]: It consists of 32 NLFSR of sizes 10 and 11 bits placed in parallel and several combining blocks.

Table 1. Results for NLFSRs used in existing stream ciphers (part 1)

NLFSR	n	$\lvert M\rvert$	Original Fibonacci NLFSR		Re-synthesized Galois NLFSR		$\frac{d_1-d_2}{d_1}$, %	$\frac{a_1-a_2}{a_1}$, %
			delay d_1, ps	area a_1, GE	delay d_2, ps	area a_2, GE		
Grain-80	80	22	433	1352	268	1390	38.1	-2.8
Grain-128	128	12	361	1915	231	2006	36.0	-4.8
VEST_1	10	16	366	151	296	177	19.1	-16.7
VEST_2	10	17	411	185	316	194	23.1	-5.1
VEST_3	10	15	381	170	310	170	18.6	0.0
VEST_4	10	17	348	150	311	193	10.6	-28.4
VEST_5	10	17	356	161	305	166	14.3	-2.9
VEST_6	10	17	410	189	311	177	24.1	6.5
VEST_7	10	17	411	183	313	179	23.8	2.4
VEST_8	10	15	378	167	305	166	19.3	0.4
VEST_9	10	15	376	160	288	166	23.4	-3.5
VEST_10	10	17	396	169	323	194	18.4	-14.8
VEST_11	10	17	361	148	315	186	12.7	-25.7
VEST_12	10	16	369	181	302	203	18.2	-11.9
VEST_13	10	15	393	172	292	172	25.7	0.0
VEST_14	10	17	369	160	313	189	15.2	-18.2
VEST_15	10	17	403	185	322	185	20.1	0.0
VEST_16	10	17	365	181	320	205	12.3	-13.3
VEST_17	9	17	382	160	307	170	19.6	-6.0
VEST_18	9	15	372	147	318	160	14.5	-8.6
VEST_19	9	15	366	149	316	170	13.7	-14.6
VEST_20	9	17	413	192	338	196	18.2	-2.4
VEST_21	9	17	391	171	328	186	16.1	-8.4
VEST_22	9	17	406	174	344	173	15.3	0.4
VEST_23	9	17	412	196	349	194	15.3	1.0
VEST_24	9	17	403	153	335	180	16.9	-17.4
VEST_25	9	17	379	164	327	179	13.7	-9.4
VEST_26	9	17	355	134	320	146	9.9	-8.9
VEST_27	9	17	379	142	322	201	15.0	-41.3
VEST_28	9	15	390	154	313	162	19.7	-5.2
VEST_29	9	17	407	156	353	156	13.3	0.0
VEST_30	9	16	394	165	301	177	23.6	-7.3
VEST_31	9	16	367	148	326	164	11.2	-10.8
VEST_32	9	17	418	185	322	178	23.0	3.8

3. Achterbahn-128/80 stream cipher [6]: It consists of 13 NLFSRs of sizes between 21 and 33 bits placed in parallel and several combining blocks.
4. Stream cipher from [7]: It consists of 10 NLFSRs of sizes 22-29, 31 and 32 bits placed in parallel and several combining blocks.

The list above contains all NLFSR-based stream ciphers which we know except Trivium [1]. Trivium consists of 3 NLFSRs which are already in a Galois configuration with the minimum delay. Their delay cannot be further reduced by shifting.

Tables 1 and 2 summarize the results. In the first three columns, we show the name of the NLFSR, the number of bits n, and the number of monomials $|M|$ in the ANF of the feedback function of the original Fibonacci NLFSR. In columns 4-7, we show the delay and the area of the original Fibonacci configuration and of the Galois configuration computed using the presented algorithm. For each NLFSR, the runtime to construct the Galois configuration was less than 0.0001 sec on a PC with Intel dual-core 1.8 GHz processor and 2 Gbytes of memory. For both configurations, the delay and the area were obtained by synthesizing

Table 2. Results for NLFSRs used in existing stream ciphers (part 2). The average is computed for all 57 NLFSR in Tables 1 and 2.

NLFSR	n	$\|M\|$	Original Fibonacci NLFSR		Re-synthesized Galois NLFSR		$\frac{d_1-d_2}{d_1}$, %	$\frac{a_1-a_2}{a_1}$, %
			delay d_1,ps	area a_1,GE	delay d_2,ps	area a_2, GE		
Achterbahn_1	21	24	444	371	320	294	27.9	20.8
Achterbahn_2	22	20	396	299	307	268	22.5	10.4
Achterbahn_3	23	18	409	341	301	300	26.4	12.1
Achterbahn_4	24	32	459	438	359	344	21.8	21.6
Achterbahn_5	25	30	459	377	326	385	29.0	-2.1
Achterbahn_6	26	30	451	397	315	367	30.2	7.6
Achterbahn_7	27	18	389	323	256	307	34.2	5.0
Achterbahn_8	28	16	374	323	241	318	35.6	1.4
Achterbahn_9	29	24	430	432	256	373	40.5	13.7
Achterbahn_10	30	32	482	432	328	428	32.0	0.9
Achterbahn_11	31	30	462	458	291	420	37.0	8.4
Achterbahn_12	32	22	419	446	257	356	38.7	20.1
Achterbahn_13	33	30	468	465	307	439	34.4	5.6
Cipher [7]_1	21	16	358	275	180	83	49.7	69.9
Cipher [7]_2	22	18	379	301	242	250	36.1	17.1
Cipher [7]_3	23	10	340	244	194	139	42.9	43.2
Cipher [7]_4	24	20	398	310	266	276	33.2	10.9
Cipher [7]_5	25	14	350	288	193	125	44.9	56.5
Cipher [7]_6	26	14	345	289	199	171	42.3	40.8
Cipher [7]_7	27	18	399	318	244	267	38.8	16.1
Cipher [7]_8	28	14	342	331	195	182	43.0	44.9
Cipher [7]_9	30	20	392	435	244	331	37.8	24.0
Cipher [7]_10	31	12	337	328	201	141	40.4	57.0
Average	19.6	18.3	393.0	291	294.4	275	25.5	4.06

NLFSRs with Cadence RTL compiler using the TSMC 90nm CMOS library. The synthesis tool was run with timing optimization as a primary target. 1 GE equals to the area of the smallest 2-input NAND gate in the TSMC 90nm CMOS library.

As we can see from the last two columns, on average, the presented approach decreases the delay of an NLFSR by 25.5% and improves its area by 4.1%. Shift registers dominate the total area of a stream cipher, e.g. they take 66% for Grain-80, and they determine its critical path. Therefore, an improvement in the delay of an NLFSR is likely to bring a comparable improvement in the delay of the overall system.

For LFSRs, the transformation from the Fibonacci to the Galois configuration is often known to cause a considerable increase in area due to a large fanout from the right-most bit of the Galois LFSR [19]. As we can see from Tables 1 and 2, this problem seems to be of less concern for NLFSRs. This is probably because in the Galois NLFSRs the feedback is taken not only from the right-most bit, but also from other bits.

5 Conclusion

In this paper, we present a fast heuristic algorithm which minimizes the delay of an NLFSR by transforming it from the Fibonacci to the Galois configuration. The experimental results on 57 NLFSRs from the stream ciphers Grain-80/128, VEST, Achterbahn, and [7] show that the presented approach decreases the delay of NLFSRs by 25.5% and improves the area by 4.1% on average.

One concern with the Galois configuration of LFSRs is signal degradation due to long feedback lines [11]. In our future work, we plan to investigate this problem for NLFSRs by implementing the original and the Galois versions of the above stream ciphers at the layout level.

References

1. Cannière, C., Preneel, B.: Trivium. In: Robshaw, M.J.B., Billet, O. (eds.) New Stream Cipher Designs. LNCS, vol. 4986, pp. 244–266. Springer, Heidelberg (2008)
2. David, R.: Random Testing of Digital Circuits. Marcel Dekker, New York (1998)
3. Dubrova, E.: A transformation from the Fibonacci to the Galois NLFSRs. IEEE Transactions on Information Theory, 5263–5271 (November 2009)
4. Dubrova, E., Teslenko, M., Tenhunen, H.: On analysis and synthesis of (n, k)-non-linear feedback shift registers. In: Proceedings of Design and Test in Europe Conference (DATE 2008), Munich, Germany, pp. 133–137 (March 2008)
5. Fredricksen, H.: A survey of full length nonlinear shift register cycle algorithms. SIAM Review 24(2), 195–221 (1982)
6. Gammel, B., Göttfert, R., Kniffler, O.: Achterbahn-128/80: Design and analysis. In: Workshop Record of The State of the Art of Stream Ciphers (SASC 2007), Bochum, Germany, pp. 152–165 (January 2007)
7. Gammel, B.M., Göttfert, R., Kniffler, O.: An NLFSR-based stream cipher. In: Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS 2006), Island of Kos, Greece, pp. 2920–2924 (May 2006)

8. Gill, A.: Linear Sequential Circuits. McGraw-Hill, New York (1966)
9. Gittins, B., Landman, H.A., O'Neil, S., Kelson, R.: A presentation on VEST hardware performance, chip area measurements, power consumption estimates and benchmarking in relation to the AES, SHA-256 and SHA-512. Cryptology ePrint Archive, Report 415 (2005)
10. Golomb, S.: Shift Register Sequences. Aegean Park Press (1982)
11. Hatayama, K., Nakao, M., Kiyoshige, Y., Natsume, K., Sato, Y., Nagumo, T.: Application of high-quality built-in test to industrial designs. In: Proceedings of International Test Conference (ITC 2002), Baltimore, MD, USA, pp. 1003–1012 (October 2002)
12. Hell, M., Johansson, T., Maximov, A., Meier, W.: The Grain family of stream ciphers. In: Robshaw, M.J.B., Billet, O. (eds.) New Stream Cipher Designs. LNCS, vol. 4986, pp. 179–190. Springer, Heidelberg (2008)
13. Jansen, C.J.: Investigations On Nonlinear Streamcipher Systems: Construction and Evaluation Methods. Ph.D. Thesis, Technical University of Delft (1989)
14. Juels, A.: RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications 24(2), 381–394 (2006)
15. Linardatos, D., Kalouptsidis, N.: Synthesis of minimal cost nonlinear feedback shift registers. Signal Process 82(2), 157–176 (2002)
16. Mansouri, S.: Re-Designing Grain Stream Cipher for Higher Throughput. M. Sc. Thesis, Royal Institute of Technology (KTH), Sweden (2009)
17. Massey, J.: Shift-register synthesis and BCH decoding. IEEE Transactions on Information Theory 15, 122–127 (1969)
18. Massey, J.L., Liu, R.: Equivalence of nonlinear-feedback shift-registers. IEEE Transactions on Information Theory 10, 378–379 (1964)
19. Mrugalski, G., Rajski, J., Tyszer, J.: Ring generators - New devices for embedded test applications. Transactions on Computer-Aided Design of Integrated Circuits and Systems 23(9), 1306–1320 (2004)
20. Mykkeltveit, J.: Nonlinear recurrences and arithmetic codes. Information and Control 33(3), 193–209 (1977)
21. Robshaw, M.: Stream ciphers. Technical Report TR - 701, RSA Laboratories (July 1994)
22. Robshaw, M.: The estream project. In: Robshaw, M.J.B., Billet, O. (eds.) New Stream Cipher Designs. LNCS, vol. 4986, pp. 1–6. Springer, Heidelberg (2008)
23. Ronce, C.A.: Feedback Shift Registers. LNCS, vol. 169. Springer, Heidelberg (1984)
24. Schneier, B.: Applied cryptography: protocols, algorithms, and source code in C, 2nd edn. John Wiley & Sons, Inc., New York (1995)

Acquisition Times of Contiguous and Distributed Marker Sequences: A Cross-Bifix Analysis

Čedomir Stefanović and Dragana Bajić

Department of Power, Electronics and Communication Engineering,
University of Novi Sad, Trg Dositeja Obradovića 6,
21000 Novi Sad, Serbia
cex@uns.ac.rs, dragana.bajic@gmail.com

Abstract. In this paper we present a cross-bifix analysis of contiguous and distributed marker sequences and apply it to the problem of acquisition of frame synchronization. The analysis establishes the relationship between the sequence period, structure, length, the amount of distortion and expected worst-case acquisition time. The provided study is general and can be applied to multilevel and unequally distributed data.

Keywords: frame synchronization, frame-synchronization acquisition, marker sequences.

1 Introduction

The design of marker sequences used for frame synchronization in a synchronous transmission is a problem with a rich and long history. Various classes of markers, optimal according to various design criteria, have been proposed so far - Barker [1], Turyn [2], Willard [3], Lindner [4], Legendre sequences [5], to name a few. A nice overview on the most frequently used design criteria and corresponding sequences is given in [6]. Besides standard, contiguous markers, a novel approach to marker design was introduced in [7], proposing distributed markers that consist both of synchronization and random data symbols. Distributed markers are an promising alternative to the contiguous ones, as for the same amount of synchronization symbols they show improved frame synchronization properties [7,8].

Design criteria of markers used for frame synchronization properties could be generally classified into two groups. In the first group are criteria based only on the properties of aperiodic autocorrelation of the marker and the goal is to minimize autocorrelation sidelobes [9]. This effectively means that the focus of marker design is just on the marker itself and the broader scope of the original problem of frame synchronization is somewhat neglected, i.e., the impact of the data symbols in the rest of the frame and possible transmission errors are disregarded. In the second group are criteria that, besides the marker, take into account data symbols in the *overlap* regions of the frame (Fig. 1). These criteria

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 55–66, 2010.

are based on the minimization of the probability of appearance of the same pattern as marker sequence in the overlap region, which can occur when data symbols in the overlap region combine with erroneously transmitted marker symbols. We will refer to these accident appearances of the same pattern as marker sequence as marker simulations, no matter whether they take place in the overlap or data region of the frame (Fig. 1).

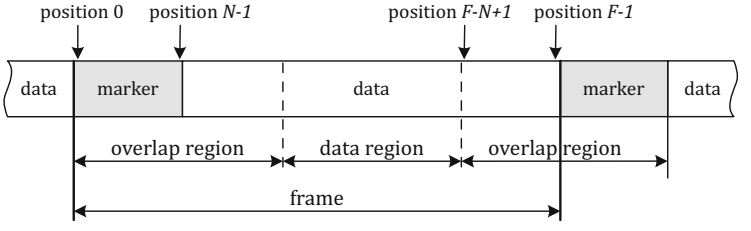


Fig. 1. Overlap and data regions of frame

The first attempt to design the marker by considering the whole frame and not just the overlap regions was given in [10], where markers are designed such that the probability of marker simulation in the frame is minimized and the probability of correct marker detection is maximized. However, the approach suggested in [10] does not provide any analytical results and optimum markers are found by extensive computer simulations.

On the other hand, probabilities of marker simulation in the frame can be analytically derived, enabling the comprehensive approach for evaluation of marker properties. The first step in this direction was taken in [11,12,13], where the expected time between simulations of a predefined sequence (i.e., marker) in a semi-infinite random symbol stream was derived. It was shown that mean time between simulations depends on sequence length and structure, where the latter is expressed through *bifices*. A bifix, as introduced in [11], is a subsequence that is both prefix and suffix of the given sequence. For example, sequence ABCABC has one bifix of length 3. The bifix analysis was extended further in [14] where the probability of marker simulation at a given position in a semi-infinite random symbol stream was derived. Finally, the probability of marker simulation at a given position in the frame was derived in [15], enabling further insight into marker design.

In this paper we exploit and extend bifix analysis of marker sequences in order to find optimal relationship between marker structure and length, frame length and sensitivity to marker distortions due to transmission errors. As an optimization criterion we use frame-synchronization acquisition time, i.e., time that receiver needs to lock on the correct frame starting position.

The organization of the rest of the paper is as follows. In the next section we give brief overview of the bifix analysis. In the third section we introduce the acquisition model and derive expected worst-case acquisition time. In the fourth section we present results for various classes of marker sequences, both contiguous and distributed. The final section concludes the paper.

2 Preliminaries

2.1 Probability of Marker Simulation

We consider a synchronous transmission, where the data stream consists of equal-length frames and every frame starts with a predefined marker; we denote frame and marker lengths by F and N, respectively. We assume that the receiver has already established symbol synchronization and is sliding through the received stream, searching for the marker sequence in order to acquire frame synchronization.

As depicted in Fig. 1, there are two regions in the frame regarding the search process described above - overlap and data regions. In overlap regions, the content of the sliding window that receiver uses to locate the marker sequence consists both of marker and data symbols. Only in the data region the content of the sliding window is purely random and composed just of data symbols.

In case of erroneous transmission, allowing certain amount of distortion when searching for the marker can speed-up the acquisition process [6]. If marker is considered to be correctly received if up to E symbol errors are allowed, than the search extends to all sequences that are up to Hamming distance E from the marker sequence. In other words, the search is performed for all the sequences in the closed ball of radius E with the center in marker sequence, totaling:

$$M = \sum_{e=0}^{E} \binom{N}{e} \tag{1}$$

sequences. We will denote this set of sequences as $S_{\mathbf{m}}(E) = \{\mathbf{s}_1 = \mathbf{m}, \mathbf{s}_2, ..., \mathbf{s}_M\}$, where $\mathbf{m}$ is the marker sequence. If marker is a distributed sequence consisting of $N - D$ synchronization symbols and D data symbols, the total number of sequences in the set $S_{\mathbf{m}}(E)$ is:

$$M = 2^D \sum_{e=0}^{E} \binom{N-D}{e}. \tag{2}$$

In order to probabilistically describe the search for set of sequences in frame, we introduce several concepts. The similarities of the sequences that form the set $S_{\mathbf{m}}(E)$ are expressed through *cross bifices* and *cross-bifix indicators*. Cross-bifix of length n, $0 \leq n \leq N$, is a subsequence of length n that is prefix of one sequence and suffix of another sequence from the set. Its existence is denoted by corresponding cross-bifix indicator $h_{ij}^{(n)}$, where subscripts i and j denote sequences $\mathbf{s}_i$ and $\mathbf{s}_j$ whose respective suffix and prefix are observed. Default values are $h_{ii}^{(N)} = 1$, $h_{ij}^{(N)} = 0$ and $h_{ij}^{(0)} = 1$; $1 \leq i, j \leq M$. We also introduce the notion of suffix probabilities $r_i^{(n)}$, $0 \leq n \leq N$, where $r_i^{(n)}$ is the product of the probabilities of last n symbols of the sequence $\mathbf{s}_i$. We assume $r_i^{(0)} = 1$, $1 \leq i \leq M$, by default.

The probability that any sequence from the set $S_{\mathbf{m}}(E)$ is simulated at position k in the frame under the conditions that the search has started at position S

and no sequence from the set has been simulated prior to k is derived in [15] (the special case of equiprobable data is presented in [16]), and given by the following expressions:

$$p(k/S) = \begin{cases} \sum_{i=1}^{M} p_i(k) & 1 \le k \le F-N, \\ \sum_{i=1}^{M} h_{i1}^{(N+S-F-1+k)} p_i(k) / r_i^{(N+S-F-1+k)} & F-N < k \le F. \end{cases} \tag{3}$$

where probabilities $p_i(k)$, $i \le M$ are, for $1 \le S < N$:

$$p_i(k) = \begin{cases} h_{1i}^{(N-k)} r_i^{(k)} \prod_{l=1}^{M} \prod_{d=1}^{k-1} \left(1 - \left(h_{1l}^{(N-d)} h_{li}^{(N-k+d)}\right)\right) & S \le k \le N, \\ \sum_{j=1}^{M} \sum_{m+1}^{min(k-S,N)} \left(h_{ji}^{(N+1-m)} r_i^{(m-1)} - h_{ji}^{(N-m)} r_i^{(m)}\right) p_j(k-m) & N < k \le F \end{cases} \tag{4}$$

and, for $N \le S < F$:

$$p_i(k) = \begin{cases} r_i^{(N)} & k = S, \\ \sum_{j=1}^{M} \sum_{m+1}^{\min(k-S,N)} \left(h_{ji}^{(N+1-m)} r_i^{(m-1)} - h_{ji}^{(N-m)} r_i^{(m)}\right) p_j(k-m) & S < k \le F \end{cases} \tag{5}$$

2.2 Cross-Bifix Spectrum

As presented in the previous subsection, the probabilities of sequences simulation depend on the set of cross-bifices that describe the sequences. In this section we introduce additional parameters based on cross-bifices that can be used for sequence comparisons; these are *cross-bifix spectrum* and *cross-bifix weights*.

We denote all cross bifices of the set $S_{\mathbf{m}}(E)$ using the corresponding matrices of the cross-bifix indicators $\mathbf{h}^{(n)} = [h_{ij}^{(n)}]$, $0 \le i, j \le M$ and $0 \le n \le N$. Cross-bifix spectrum of the set $S_{\mathbf{m}}(E)$ is given by set of weights $\mathbf{w} = [w^{(n)}]$, $0 \le n \le N$, where:

$$w^{(n)} = \mathbf{1}_M \mathbf{h}^{(n)} \mathbf{1}_M^T \tag{6}$$

and $\mathbf{1}_M$ is an all-ones vector of length M. In other words, $w^{(n)}$ is the number of non-zero elements in the matrix $\mathbf{h}^{(n)}$. The default values are $w^{(0)} = M^2$ and $w^{(N)} = M$. If no transmission errors are allowed when detecting a marker (i.e. $E = 0$, see Eqs. 1 and 2), contiguous and distributed markers used for practical purposes by design have all other weights equal to zero ($w^{(n)} = 0$, $0 < n < N$) and we say that they are (cross-)bifix free. However, if transmission errors are allowed ($E > 0$), the set of sequences that originates from a marker is not a cross-bifix free one. In order to prevent the simulations and hence speed-up the

frame-synchronization acquisition, natural choice would be to design marker such that the corresponding cross-bifix weights of the set $S_{\mathbf{m}}(E)$ are as low as possible; i.e., $w^{(n)} = 0$, $0 < n < N$ should be minimal. However, this design criteria is complex, since changes in the marker affect the whole cross-bifix spectrum in a hardly tractable manner, especially for longer markers (the number of sequences in the set grows exponentially with marker length).

A simplified approach can be taken by observing that the marker is by far the most probable sequence to appear in the correct position (i.e. beginning of the frame). The appearance of any other sequence at the beginning of the frame is due to the transmission errors and therefore less likely. Hence only the partial cross-bifix spectrum with respect to the marker could be considered, consisting of partial weights $\mathbf{w}_1 = [w_1^{(n)}]$, $0 \leq n \leq N$, evaluated as:

$$w_1^{(n)} = \sum_{i=1}^{M} \left(h_{1i}^{(n)} + (1 - \delta_{i1}) h_{i1}^{(n)} \right) \tag{7}$$

where δ_{ij} is the Kronecker delta. The usage of partial cross-bifix spectrum as a mean for marker comparisons is demonstrated in Section 4.

Finally, to illustrate the above expressions, we provide a simple example. Let us consider marker 100 and assume that one transmission error is allowed, i.e., $E = 1$. The search is then performed for the set $\{100, 000, 110, 101\}$, and cross-bifix matrices of the set are:

$$\mathbf{h}^{(0)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \mathbf{h}^{(1)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \mathbf{h}^{(2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \mathbf{h}^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Cross-bifix spectrum and partial cross-bifix spectrum with respect to sequence 100 are:

$$\mathbf{w} = [16\ 6\ 4\ 4]$$
$$\mathbf{w}_1 = [7\ 2\ 2\ 1]$$

3 Acquisition Model

The frame-synchronization acquisition scenario we consider is the one described in [17]. The search starts just one position next from the true marker position (position 1 in Fig. 1), which corresponds to the worst-case situation. The search progresses symbol-by-symbol, until any sequence from the set $S_{\mathbf{m}}(E)$ is encountered. When this happens, the receiver jumps to the same position in the next frame (i.e., shifts for F symbols), verifying the detected sequence. This process continues until the correct position is reached. In the best case, the correct position is reached in F shifts, when no simulations of the sequences from the set $S_{\mathbf{m}}(E)$ occur in the frame. However, any simulation will prolong acquisition for

another F symbols and we are interested to find the average (expected) acquisition time.

The graph of the acquisition model is depicted in Fig. 2. States of the search process are denoted by their selection probabilities π_{ij}, $1 \leq i < j \leq F$, and X_i, $1 \leq i < F$. States π_{ij} represent symbol by symbol shifts from position i to position j in the frame with no marker simulations in between; i.e., arrival to state π_{ij} means that the search has started at position i and no marker simulation has occurred in up to position j. States X_i correspond to marker simulations at position i, each time this happens a shift of F symbols to the same position in the next frame is made and the search stays in the same state X_i. Transitions denoted by dashed lines are introduced to describe the renewal property of the process, when the search eventually restarts due to the loss of frame synchronization. The initial state is π_{11}.

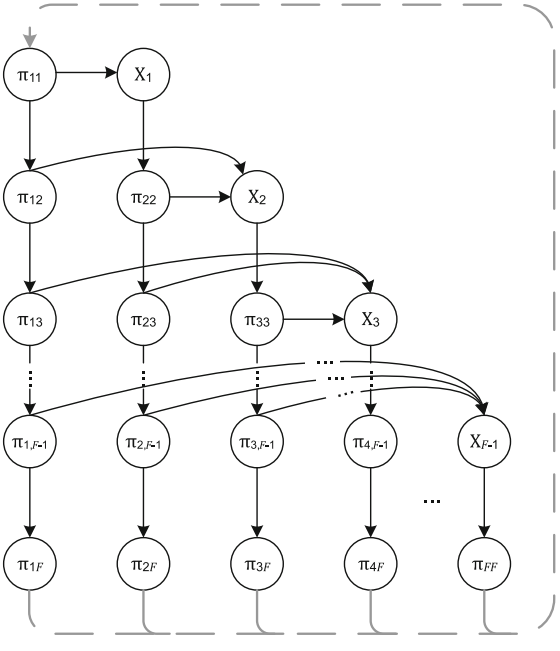


Fig. 2. Acquisition model

Dwelling times of states π_{ij}, are equal to symbol duration τ_S. Dwelling times of states X_i, incorporating repeated simulations in successive frames by their expected number, are simply:

$$\tau_i = \frac{\tau_F}{1 - p(i/i)} = \frac{F \cdot \tau_S}{1 - p(i/i)} \tag{8}$$

where probabilities $p(i/i)$ are given by Eq. 3.

The state selection probabilities can be evaluated as:

$$\pi_{ii} = \sum_{j=1}^{i-1} \pi_{jj} \cdot p(i/j),\ 1 \le i \le F \tag{9}$$

$$X_i = \sum_{j=1}^{i} \pi_{jj} \cdot p(i/j),\ 1 \le i \le F \tag{10}$$

$$\pi_{ij} = \pi_{ii}\Big(1 - \sum_{k=1}^{j-1} p(k/i)\Big),\ 1 \le i < j \le F \tag{11}$$

to the multiplicative constant π_{11} and where probabilities $p(i/j)$ are given by Eq. 3.

By using the above model, acquisition time is reduced the problem of the first passage time necessary to exit the set of states in Fig. 2. The simplest solution to it, as given in [18], is to compress the set of states to a single, equivalent state, with the equivalent dwelling time τ_{EQ} and exit probability p_{EQ}. The quantities τ_{EQ} and p_{EQ} are evaluated averaging state dwelling times and set of state exit probabilities over all state selection probabilities [18]:

$$\tau_{EQ} = \frac{\sum_{i=1}^{F-1}\left(X_i\tau_i + \sum_{j=i}^{F}\pi_{ij}\tau_S\right)}{\sum_{i=1}^{F-1}\left(X_i + \sum_{i=1}^{F-1}\pi_{ij}\right)} \tag{12}$$

$$p_{EQ} = \frac{X_{F-1} + \sum_{i=1}^{F-1}\pi_{ii}p(F/i)}{\sum_{i=1}^{F-1}\left(X_i + \sum_{j=i}^{F}\pi_{ij}\right)}\,. \tag{13}$$

The expected number of cycles spent in the equivalent state π_{EQ} is $E[n_{EQ}] = \frac{1}{p_{EQ}}$, and the corresponding expected time spent in π_{EQ} is $\tau_{EQ} \cdot E[n_{EQ}]$. This expected time is actually the expected *acquisition* time, i.e., time needed to reach the correct marker position F:

$$\begin{aligned} T_{ACQ} = \tau_{EQ}E[n_{EQ}] = \frac{\tau_{EQ}}{p_{EQ}} &= \frac{\sum_{i=1}^{F-1} X_i\tau_i + \sum_{i=1}^{F-1}\pi_{ji}\tau_S}{X_{F-1} + \sum_{i=1}^{F-1}\pi_{ii}p(F/i)} \\ &= \frac{\sum_{i=1}^{F-1}\left(\frac{X_iF}{1-p(i/i)} + \pi_{ii}\big(F-1-\sum_{k=i}^{F-1}(F-1-k)p(k/i)\big)\right)}{X_{F-1} + \sum_{i=1}^{F-1}\pi_{ii}p(F/i)}\,. \end{aligned} \tag{14}$$

4 Results

Within this section we compare a set of sequences with 7 synchronization symbols. Our focus is on binary sequences, as they are most studied in the literature. The examined sequences are:

1. Barker sequence 1110010 [1],
2. Jones sequence 0001011 [10],

3. CCITT sequence 0011011, used for frame-synchronization at the primary level of the plesiochronous digital hierarchy [19],
4. all-zeroes sequence 0000000,
5. periodical sequence 1010101,
6. Barker-like distributed sequence of maximal length[1] 111xx0xxx0x10 [7],
7. all-zeroes distributed sequence 000xx0xxx0x00,
8. periodical distributed sequence 101xx0xxx0x01.

Sequences 1, 2 and 3 are bifix-free, sequence 6 is cross-bifix free. Other sequences are examples of "bad" sequences, with plenty of (cross-)bifices.

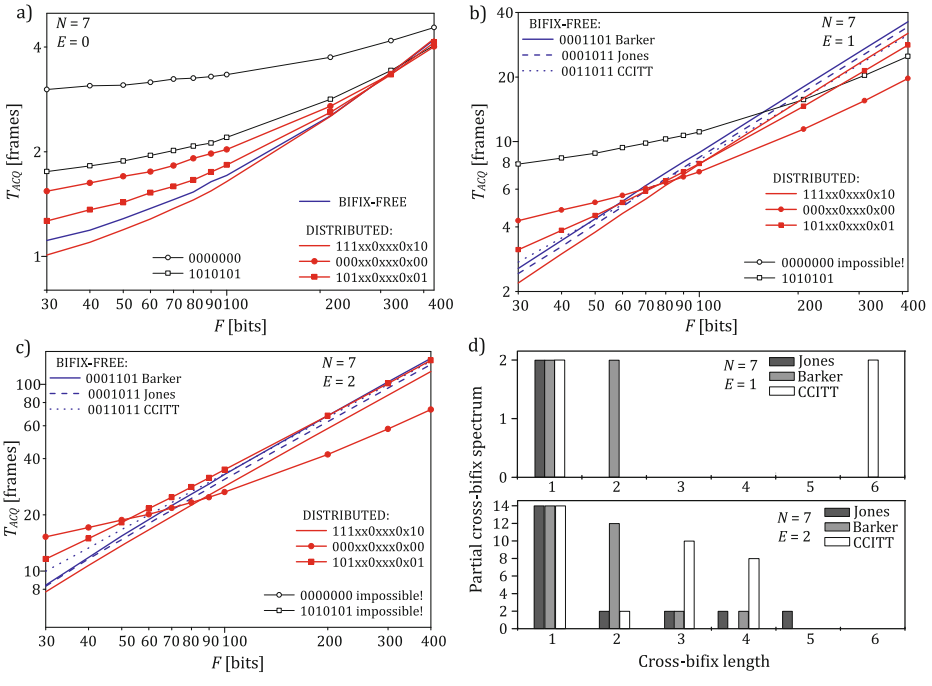


Fig. 3. Acquisition times of example sequences, for varying frame lengths and for a) $E = 0$, b) $E = 1$ and c) $E = 2$; d) Partial cross-bifix spectra of Jones, Barker and CCITT sequences for $E = 1$ and $E = 2$

Fig.3a depicts acquisition times of the example sequences for varying frame length when no distortions are allowed ($E = 0$). All bifix-free sequences show the same performance, however they fail to achieve minimal acquisition time (which is $T_{ACQ}^{min} = F$), even for very short frames. Distributed Barker-like sequence outperforms all contiguous ones due to its larger length and therefore larger overlap regions in the frame where marker simulations are suppressed. Sequences with (cross-)bifices at first perform worse than the (cross-)bifix free ones, the performance deteriorating as the number of (cross-)bifices grows. However, as the frame

[1] "x" denotes arbitrary data symbol.

length increases, their performance becomes better and the turning frame lengths for the considered example are roughly at $F = 300$. If the frame length was increased further, ultimately the all-zeros sequence (i.e., all-bifix sequence) will perform best. Although an interesting phenomenon, this reversal in performance has no practical value, as for the given frame length F one usually seeks to minimize acquisition time. This means that longer markers have to be employed and in that case bifix-free markers again become preferable choice.

Figs. 3b and 3c give the acquisition performance when errors are allowed ($E > 0$). Contiguous bifix-free sequences now show different behavior, due to the differences in the partial cross-bifix spectra of the corresponding sets of sequences that originates from each of them (as shown in Fig. 3d). By examining Figs. 3b and 3c and Fig. 3d, several important observations can be made. For shorter frame lengths, the more cross-bifices the worse the performance and Jones sequence, as the sequence with the lowest cross-bifix weights, performs best. When $E = 1$ (Fig. 3b), the number of cross-bifices in the partial spectrum for Barker and CCITT sequences is the same, but the performance of CCITT sequence is worse; this is obviously due to the influence of weights of larger cross-bifix lengths on the probability of simulation. The similar conclusion can be made for $E = 2$ (Fig. 3c), where the differences in the partial cross-bifix spectra and related performances are clearly observed. Finally, as the frame length increases, sequences with more cross-bifices become better choice and the turning frame lengths decrease as E increases.[2]

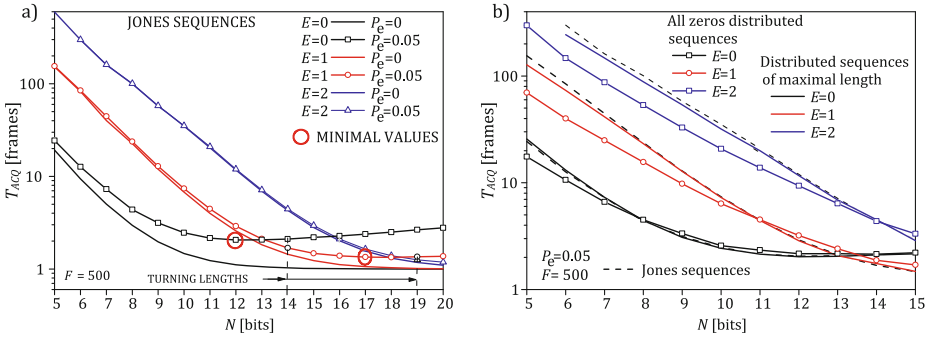


Fig. 4. Acquisition times for varying sequence lengths and $F = 500$; a) Jones sequences b) All-zeros distributed sequences and Barker-like distributed sequences of maximal length

Fig. 3a gives acquisition times for several contiguous and distributed markers with varying lengths and fixed frame length $F = 500$, in the case of error-free and erroneous transmission - probability of bit error is set to $P_e = 0$ and $P_e = 0.05$, respectively. As Fig. 4a shows, for $P_e = 0$ acquisition time of Jones

[2] For $E = 1$ and $E = 2$ all-zero sequence 0000000 can not be used for frame synchronization, since the receiver would certainly lock at the incorrect position. The same holds for periodical sequence 1010101 and $E = 2$.

Table 1. Turning lengths of Jones sequences and various frame lengths, $P_e = 0.05$

Frame length F	Turning length N_1	Turning length N_2
30	9	11
40	9	12
50	10	14
60	10	15
70	11	15
80	11	16
90	11	16
100	12	16
200	12	17
300	13	18
400	13	18
500	14	19

(contiguous) markers converges to its minimal value with the increase of the marker length, as expected. If the transmission is erroneous ($P_e = 0.05$), the increase of marker length at first reduces the acquisition time by reducing the probability of simulation. However, as the marker length further increases, the acquisition time starts to increase again, due to the increase in probability of skipping the correct position. The minimal acquisition times are encircled in Fig. 4a.

Fig. 4b is devoted to distributed sequences, compared to contiguous ones (dashed lines) for $F = 500$ and $P_e = 0.05$. It can be observed the distributed Barker-like sequences of maximal length [7] perform slightly better then contiguous sequences. If small amount of redundancy is reserved for marker and distortions are allowed, the all-zeros distributed sequences are obviously the best choice.

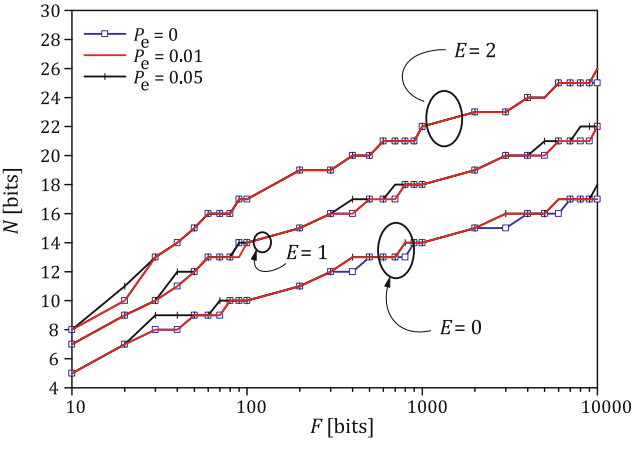


Fig. 5. Lengths of Jones sequences for which $T_{ACQ} \leq 1.1 \cdot F$

Turning marker lengths are another distinctive feature. These are marker lengths for which, for the given frame length and probability of transmission error, some amount of distortion should be allowed to shorten the acquisition time. As shown in Fig. 4a, for Jones sequences, $F = 500$ and $P_e = 0.05$, turning lengths are $N_1 = 14$, when $T_{ACQ}(E = 0)$ becomes larger then $T_{ACQ}(E = 1)$; and $N_2 = 19$ when $T_{ACQ}(E = 1)$ becomes larger then $T_{ACQ}(E = 2)$. Turning lengths for Jones sequences, $P_e = 0.05$ and various frame lengths F are given in Table 1.

Finally, Fig. 5 presents lengths of Jones sequences for which the acquisition time is smaller than 1.1 frames, as a function of the frame length and for several transmission-error probabilities. Results shown here can be taken as a guideline for the choice of the marker length.

5 Concluding Remarks

The cross-bifix analysis, when applied to the marker study, yields interesting results. The partial cross-bifix spectrum is tightly related with the acquisition time, and sequences (considering allowed distortion) should be designed with the least cross-bifices, preferably of the shortest possible lengths.

The amount of allowed marked distortion strongly depends upon the marker and frame lengths, and exact bounds (turning lengths) can be evaluated for each set of parameters, if the hard symbol detection is employed at receiver.

Distributed sequences deserve special attention as they generally outperform the contiguous ones of same redundancy; this suggests that their actual usage for the frame-syncronization purposes should be more frequent. Also, distributed sequences that have zeros at the positions of synchronization bits have interesting properties of their own - they combine the good characteristics of distributed sequences in overlap regions and small simulation probability of all zero sequences in data region. These features arise when marker is too short for the given frame length.

Finally, we note that the given analysis is applicable to the examination of multilevel sequences and their cross-bifix spectra.

References

1. Barker, R.H.: Group synchronization of binary digital systems. In: Communication Theory, pp. 273–287. Academic Press Inc., New York (1953)
2. Turyn, R.: Sequences with small corellation. In: Error Correcting Codes, pp. 195–228. Wiley, New York (1968)
3. Willard, M.W.: Optimum Code Patterns for PCM Synchronization. In: Proc. National Telemetry Conference (1962)
4. Lindner, J.: Binary sequences up to length 40 with best possible autocorellation function. Electron. Lett. 11(21), 507 (1975)
5. Schroeder, M.: Number theory in science and communication. Springer, Berlin (1984)

6. Scholtz, R.: Frame Synchronization Techniques. IEEE Trans. Comm. 28, 1204–1213 (1980)
7. de Lind van Wijngaarden, A.J., Willink, T.J.: Frame Synchronization Using Distributed Sequences. IEEE Trans. Comm. 48(12), 2127–2138 (2000)
8. Villanti, M., Iubatti, M., Vanelli-Coralli, A., Corazza, G.E.: Design of Distributed Unique Words for Enhanced Frame Synchronization. IEEE Trans. Comm. 57(8), 2430–2440 (2009)
9. Schotten, H.D., Lüke, H.D.: On the search for low correlated binary sequences. Int. J. Electron. Commun. 59(2), 67–78 (2005)
10. Al-Subbagh, M.N., Jones, E.V.: Optimum patterns for frame alignment. IEE Proc. part F - Commun., Radar & Signal Processing 135(6), 594–603 (1988)
11. Nielsen, P.T.: On the Expected Duration of a Search for a Fixed Pattern in Random Data. IEEE Trans. Inform. Theory 19, 702–704 (1973)
12. Nielsen, P.T.: A Note on Bifix-free Sequences. IEEE Trans. Inform. Theory 19, 704–706 (1973)
13. McConnell, T.R.: The Expected Time to Find a String in a Random Binary Sequence (2001), http://barnyard.syr.edu/cover.pdf
14. Bajic, D., Stefanovic, C., Vukobratovic, D.: Search Process and Probabilistic Bifix Approach. In: Proc. of IEEE ISIT 2005, Adelaide, Australia (September 2005)
15. Stefanovic, C.: Synchronization sequences and bifix analysis (in Serbian). Master's thesis, Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia (2006)
16. Bajic, D.: On Survival Probability of Alignment Sequences. In: Proc. of ISITA 2004, Parma, Italy (October 2004)
17. Häberle, H.: Frame Synchronizing PCM Systems. Electric. Comm. 44(4), 280–287 (1969)
18. Bajic, D.: New simple method for solving the first passage time problem. Electron. Lett. 27(16), 1419–1421 (1991)
19. CCITT Recommendation, C.: Blue Book III.4. Geneve, Switzerland (1988)

Lower Bounds on the Average Partial Hamming Correlations of Frequency Hopping Sequences with Low Hit Zone*

Xianhua Niu, Daiyuan Peng, and Fang Liu

Key Laboratory of Information Coding and Transmission,
Southwest Jiaotong University,
Chengdu, Sichuan, 610031, People's Republic of China
rurustef1212@gmail.com, dypeng@swjtu.edu.cn, hmimy5416@163.com

Abstract. Average Hamming correlation is an important performance indicator of frequency hopping sequences. Usually, the length of correlation window is shorter than the period of the chosen frequency hopping sequence, so the study of the partial Hamming correlations of frequency hopping sequences is particularly important. In this paper, the average partial Hamming correlation lower bounds of frequency hopping sequences with low hit zone, with respect to the size of frequency slot set, length of correlation window, family size, low hit zone, average partial Hamming autocorrelation and average partial Hamming crosscorrelation are established. It is shown that the new bounds include the Peng-Peng-Tang-Niu bounds for the conventional frequency hopping sequences as special cases.

Keywords: average partial Hamming correlation, correlation window, low hit zone, frequency hopping sequences.

1 Introduction

Frequency hopping (FH) multiple-access (MA) spread-spectrum (SS) systems, with their anti-jamming, secure, and MA properties, have found many applications in military radio communications, mobile communications, modern radar and sonar echolocation systems [1]. In such systems, the FH-SS technique, to spread the spectrum of a data-modulated carrier, is to switch the carrier frequency from one to another periodically. Usually, each carrier frequency is selected from a set of frequencies, which are spaced approximately the width of the data modulation bandwidth apart. The frequencies used are chosen pseudo-randomly by a code called FH sequence (FHS). As is often the case, in an MA environment, mutual interference occurs when two or more transmitters transmit in the same frequency at the same time. It is desirable to keep the mutual interference between transmitters at a level as low as possible. The degree of the

* This work was supported by the National Science Foundation of China (NSFC, 60872015).

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 67–75, 2010.

mutual interference is clearly related to the Hamming crosscorrelation properties of FHSs [1,2].

FHS design normally involves the following parameters: the size of frequency slot set, sequence length, family size, maximum (average) Hamming autocorrelation sidelobe and maximum (average) Hamming crosscorrelation. Generally speaking, these parameters are bounded by certain theoretical limits. In order to evaluate the theoretical performance of FHSs, it is important to find the theoretical limits which set bounded relations among these parameters.

As early as 1974, Lempel and Greenberger [2] established a bound on the maximum periodic Hamming correlation (MPHC) of an FHS. In 2004, Peng and Fan [3] obtained some bounds on MPHCs of an FHS set. In 2008, Peng *et al.* [4] obtained a bound on the average periodic Hamming correlations (APHCs) of an FHS set.

However, usually the length of correlation window is shorter than the period of the chosen FHS due to the limited synchronization time or hardware complexity. Moreover, the window length may vary from time to time depending on the channel conditions. In that case, the partial Hamming correlation (PHC), rather than the full period Hamming correlation, will play a major role in determining the synchronization performance. In 2004, Eun *et al.* [5] obtained a bound on the maximum PHC of an FHS.

Different from conventional FHS design, the FHS design with no hit zone (NHZ) or low hit zone (LHZ) aims at making Hamming correlation values equal to zero or a very low value within a correlation zone [6]. The significance of NHZ/LHZ sequence set is that, even when there are relative delays between the transmitted FHSs, there will be no hits or the number of hits will be kept at a very low level between different sequences as long as the relative delay does not exceed a certain limit (zone), thus reducing or eliminating the mutual interference. In 2006, Peng *et al.* [7] derived some bounds on MPHCs of the FHS set with LHZ. In 2009, Niu *et al.* [8] derived some bounds on the maximum PHCs of the FHS set with LHZ.

In this paper, we will pay particular attention to the average PHC bounds of the FHS set with LHZ. The rest of this paper is organized as follows: in Section 2, the related notations, definitions and bounds are introduced; in Section 3, the lower bounds on the average partial Hamming autocorrelation and average partial Hamming crosscorrelation of the FHS set with LHZ are derived; finally, the correspondence concludes with some remarks.

2 Preliminaries

Let $F=\{f_1, f_2,\ldots,f_q\}$ be a frequency slot set with size $|F|=q$, and S be a set of M FHSs of length N. For any two frequency slots f_i, $f_j \in F$, let

$$h(f_i, f_j) = \begin{cases} 1, \text{ if } f_i = f_j \\ 0, \text{ otherwise} \end{cases}$$

For any two FHSs, $x=(x_0, x_1, \ldots, x_{N-1})$, $y=(y_0, y_1, \ldots, y_{N-1}) \in S$, and any integer τ, $0 \leq \tau < N$, the periodic Hamming correlation function $H_{xy}(\tau)$ of x and y at time delay τ is defined as follows:

$$H_{xy}(\tau) = \sum_{i=0}^{N-1} h(x_i, y_{i+\tau}), \tau = 0, 1, \ldots, N-1. \tag{1}$$

where all operations among the position indices are performed modulo N.

For any given FHS set S, the maximum periodic Hamming autocorrelation sidelobe $H_a(S)$ and the maximum periodic Hamming crosscorrelation $H_c(S)$ are defined as follows, respectively:

$$H_a(S) = \max\{H_{xx}(\tau)|\ 0 < \tau < N, \forall x \in S\},$$
$$H_c(S) = \max\{H_{xy}(\tau)|\ 0 \leq \tau < N, \forall x, y \in S, x \neq y\}.$$

For simplicity, we will denote $H_a=H_a(S)$, $H_c=H_c(S)$.

Early in 1974, Lempel and Greenberger [2] established the following bound on MPHC of an FHS (Lempel-Greenberger bound):

$$H_a \geq \frac{(N-r)(N+r-q)}{(N-1)q}. \tag{2}$$

where r is the least nonnegative residue of N modulo q.

Let S be a set of M FHSs of length N. Peng and Fan [3] obtained the following bounds on MPHCs of S (Peng-Fan bounds):

$$q(N-1)H_a + Nq(M-1)H_c \geq (NM-q)N. \tag{3}$$

$$M(N-1)H_a + NM(M-1)H_c \geq 2INM - (I+1)Iq. \tag{4}$$

where I denotes the integer part of NM/q.

The Peng-Fan bounds include the Lempel-Greenberger bound as a special case. If the autocorrelation and crosscorrelation properties of an FHS set satisfy the Peng-Fan bounds with equality, then it is said that the sequences set is an optimal MPHC FHS set. There have been a number of optimal MPHC FHS sets [9,10,11,12] which satisfy the Peng-Fan bounds.

Let S be a set of M FHSs of length N. The average periodic Hamming autocorrelation $A_a(S)$ and average periodic Hamming crosscorrelation $A_c(S)$ are defined as follows, respectively:

$$A_a(S) = \frac{\sum_{x \in S} \sum_{\tau=1}^{N-1} H_{xx}(\tau)}{M(N-1)}. \tag{5}$$

$$A_c(S) = \frac{\sum_{x,y \in S, x \neq y} \sum_{\tau=0}^{N-1} H_{xy}(\tau)}{MN(M-1)}. \tag{6}$$

For simplicity, we will denote $A_a=A_a(S)$, $A_c=A_c(S)$.

For any FHS set S, Peng *et al.* [4] obtained a bound on APHCs of S (Peng-Peng-Tang-Niu bound):

$$q(N-1)A_a + Nq(M-1)A_c \geq (NM-q)N. \tag{7}$$

If the average Hamming correlation properties of an FHS set satisfy the Peng-Peng-Tang-Niu bound with equality, then it is said that the FHS set is an optimal APHC FHS set. There have been some optimal APHC FHS sets [4] which satisfy Peng-Peng-Tang-Niu bound.

The PHC function between two sequences $x, y \in S$, for a period N and the correlation window length L starting at j, is defined as follows:

$$H_{xy}(j|L;\tau) = \sum_{i=j}^{j+L-1} h(x_i, y_{i+\tau}), (0 \leq \tau < N, 0 \leq j < N, 0 < L \leq N). \tag{8}$$

where all operations among the position indices are performed modulo N. Moreover, $H_{xy}(j|L;\tau)$ is called the partial Hamming autocorrelation function when $x{=}y$ and the partial Hamming crosscorrelation function when $x{\neq}y$. If $j{=}0$ and $L{=}N$, (8) represents the conventional periodic Hamming correlation function $H_{xy}(\tau)$.

For any given FHS set S and a given correlation window length $L(L{\leq}N)$, the maximum partial Hamming autocorrelation $P_a(L)$ and maximum partial Hamming crosscorrelation $P_c(L)$ are defined as follows, respectively:

$$P_a(L) = \max\{H_{xx}(j|L;\tau)|\ 0 < \tau < N, 0 \leq j < N, \forall x \in S\},$$
$$P_c(L) = \max\{H_{xy}(j|L;\tau)|\ 0 \leq \tau < N, 0 \leq j < N, \forall x, y \in S, x \neq y\}.$$

For simplicity, we will denote $P_a{=}P_a(L)$, $P_c{=}P_c(L)$.

Eun *et al.* [5] obtained the following bound on the maximum PHC of an FHS (Eun-Jin-Hong-Song bound):

$$P_a \geq \frac{L}{N}\frac{(N-r)(N+r-q)}{(N-1)q}. \tag{9}$$

where r is the least nonnegative residue of N modulo q.

This bound includes the Lempel-Greenberger bound as a special case.

It is said that a sequence is strictly optimal if its maximum partial autocorrelation satisfies the Eun-Jin-Hong-Song bound with equality for all length of correlation window. It is demonstrated that there have been some sequences [5] satisfy the Eun-Jin-Hong-Song bound.

For any FHS set S, let integers $H_{La}{\geq}0$, $H_{Lc}{\geq}0$, then the low hit zone L_{HZ}, autocorrelation low hit zone L_{AHZ} and crosscorrelation low hit zone L_{CHZ} of S with respect to MPHC are defined as follows, respectively:

$$L_{HZ}{=}min\{L_{AHZ}, L_{CHZ}\},$$
$$L_{AHZ}{=}max\{T|H_{xx}(\tau) \leq H_{La}, 0 < \tau \leq T, \forall x \in S\},$$
$$L_{CHZ}{=}max\{T|H_{xy}(\tau) \leq H_{Lc}, 0 \leq \tau \leq T, \forall x, y \in S, x{\neq}y\}.$$

When H_{La}=H_{Lc}= 0, the low hit zone L_{HZ} of S is called the no hit zone N_{HZ} of S. An FHS set S with $L_{HZ}\geq 0$ or $N_{HZ}\geq 0$ is called an LHZ FHS set or a NHZ FHS set.

For any positive integer Z, $0\leq Z\leq L_{HZ}$, Peng *et al.* [7] obtained the following bounds on the LHZ FHS set (Peng-Fan-Lee bounds):

$$qZH_{La} + q(M-1)(Z+1)H_{Lc} \geq (Z+1)MN - Nq. \tag{10}$$

$$MNZH_{La} + MN(M-1)(Z+1)H_{Lc} \geq (Z+1)[(2I+1)MN-(I+1)Iq] - MN^2. \tag{11}$$

where I denotes the integer part of NM/q.

The Peng-Fan-Lee bounds include the Lempel-Greenberger bound and Peng-Fan bounds for the conventional FHS set as special cases. There have been some NHZ FHS sets [13,14] which satisfy the Peng-Fan-Lee bounds.

For any FHS set S of period N and a given correlation window length $L(L\leq N)$, let integers $P_{La}(L)\geq 0$, $P_{Lc}(L)\geq 0$, then the low hit zone L_{PHZ}, autocorrelation low hit zone L_{PAHZ} and crosscorrelation low hit zone L_{PCHZ} of S with respect to the maximum PHC are defined as follows, respectively:

$$\begin{aligned}
&L_{PHZ}(L)=min\{L_{PAHZ}(L), L_{PCHZ}(L)\},\\
&L_{PAHZ}(L)=max\{T|H_{xx}(j|L;\tau) \leq P_{La}(L), 0<\tau\leq T, 0\leq j<N, \forall x\in S\},\\
&L_{PCHZ}(L)=max\{T|H_{xy}(j|L;\tau) \leq P_{Lc}(L), 0\leq\tau\leq T, 0\leq j<N, \forall x,y\in S, x\neq y\}.
\end{aligned}$$

In particular, the low hit zone, autocorrelation low hit zone and crosscorrelation low hit zone of S with respect to MPHC are only the special cases of the low hit zone, autocorrelation low hit zone and crosscorrelation low hit zone of S with respect to the maximum PHC respectively for j=0 and L=N.

For simplicity, we will denote L_{PHZ}=$L_{PHZ}(L)$, P_{La}=$P_{La}(L)$, P_{Lc}=$P_{Lc}(L)$.

For any positive integer Z, $0\leq Z\leq L_{PHZ}$, Niu *et al.* [8] obtained the following bounds on the maximum PHC of FHS set with LHZ (Niu-Peng-Liu bounds):

$$qZP_{La} + q(M-1)(Z+1)P_{Lc} \geq (Z+1)LM - Lq. \tag{12}$$

$$MNZP_{La} + MN(M-1)(Z+1)P_{Lc} \geq (Z+1)L[(2I+1)M-(I+1)Iq/N] - MNL. \tag{13}$$

where I denotes the integer part of NM/q.

The Niu-Peng-Liu bounds include the Lempel-Greenberger bound, Peng-Fan bounds, Eun-Jin-Hong-Song bound and Peng-Fan-Lee bounds as special cases.

3 Lower Bounds on the Average PHCs of FHS Set with LHZ

As an important performance indicator of FHSs, the average PHCs of FHS set with LHZ are defined as follows.

Definition 1. *Let S be a set of M FHSs of length N over a given frequency slot set F with size q. For the given correlation window length L ($L \leq N$) and any positive integer Z, $0 \leq Z \leq L_{PHZ}$, we call*

$$S_a(L) = \sum_{x \in S} \sum_{\tau=1}^{Z} \sum_{j=0}^{N-1} H_{xx}(j|L;\tau), \tag{14}$$

$$S_c(L) = \frac{1}{2} \sum_{x,y \in S, x \neq y} \sum_{\tau=0}^{Z} \sum_{j=0}^{N-1} H_{xy}(j|L;\tau). \tag{15}$$

as the overall number of partial Hamming autocorrelation (auto-hits) and partial Hamming crosscorrelation (cross-hits) of S with LHZ respectively, and call

$$\overline{P}_a(L) = \frac{S_a(L)}{MNZ}, \tag{16}$$

$$\overline{P}_c(L) = \frac{2S_c(L)}{MN(M-1)(Z+1)}. \tag{17}$$

as the average partial Hamming autocorrelation (average of auto-hits) and average partial Hamming crosscorrelation (average of cross-hits) of S with LHZ respectively.

If $j=0$, $L=N$ and $Z=N-1$, $\overline{P}_a(L)$ and $\overline{P}_c(L)$ represent the conventional average Hamming autocorrelation A_a and average Hamming crosscorrelation A_c, respectively.

For simplicity, we will denote $S_a=S_a(L)$, $S_c=S_c(L)$, $\overline{P}_a=\overline{P}_a(L)$, $\overline{P}_c=\overline{P}_c(L)$.

We now state the theorem on the lower bounds on the average partial Hamming autocorrelation and average partial Hamming crosscorrelation of FHS set with LHZ.

Theorem 1. *Let S be a set of M FHSs of length N over a given frequency slot set F with size q, L_{PHZ} be the LHZ of S with respect to P_{La} and P_{Lc}. For any $\overline{P}_{La}$, $\overline{P}_{Lc}$, $0 \leq \overline{P}_{La} \leq P_{La}$, $0 \leq \overline{P}_{Lc} \leq P_{Lc}$, the given correlation window length L and any positive integer Z, $0 \leq Z \leq L_{PHZ}$, we have*

$$qZ\overline{P}_{La} + q(M-1)(Z+1)\overline{P}_{Lc} \geq (Z+1)LM - Lq. \tag{18}$$

$$MNZ\overline{P}_{La} + (M-1)(Z+1)MN\overline{P}_{Lc} \geq (Z+1)L[(2I+1)M - (I+1)Iq/N] - MNL. \tag{19}$$

where I denotes the integer part of NM/q.

Proof. For any positive integer Z, $0 \le Z \le L_{PHZ}$, we first have

$$\begin{aligned}
&\sum_{x,y\in S}\sum_{\tau=0}^{Z} H_{xy}(\tau) = MN + \sum_{x\in S}\sum_{\tau=1}^{Z} H_{xx}(\tau) + \sum_{x,y\in S, x\neq y}\sum_{\tau=0}^{Z} H_{xy}(\tau) \\
&= MN + \sum_{x\in S}\sum_{\tau=1}^{Z} H_{xx}(0|N;\tau) + \sum_{x,y\in S, x\neq y}\sum_{\tau=0}^{Z} H_{xy}(0|N;\tau) \\
&= MN + \frac{1}{L}\sum_{x\in S}\sum_{\tau=1}^{Z}\sum_{j=0}^{N-1} H_{xx}(j|L;\tau) + \frac{1}{L}\sum_{x,y\in S, x\neq y}\sum_{\tau=0}^{Z}\sum_{j=0}^{N-1} H_{xy}(j|L;\tau) \\
&= MN + \frac{1}{L}S_a + \frac{2}{L}S_c.
\end{aligned}$$

In [7], a lower bound on $\sum_{x,y\in S}\sum_{\tau=0}^{Z} H_{xy}(\tau)$ was given. Therefore, it follows that

$$\begin{aligned}
MN + \frac{1}{L}S_a + \frac{2}{L}S_c &\ge (Z+1)NM^2/q, \\
MN + \frac{1}{L}S_a + \frac{2}{L}S_c &\ge (Z+1)[(2I+1)M - (I+1)Iq/N].
\end{aligned}$$

where I denotes the integer part of NM/q.

Then, based on the definition of the average PHCs of FHS set with LHZ in (18) and (19), we have

$$\begin{aligned}
\frac{1}{Z(M-1)(Z+1)} + \frac{\overline{P}_{La}}{L(M-1)(Z+1)} + \frac{\overline{P}_{Lc}}{LZ} &\ge \frac{M}{qZ(M-1)}, \\
\frac{1}{Z(M-1)(Z+1)} + \frac{\overline{P}_{La}}{L(M-1)(Z+1)} + \frac{\overline{P}_{Lc}}{LZ} &\ge \frac{(2I+1)MN - (I+1)Iq}{MN^2Z(M-1)}.
\end{aligned}$$

This completes the proof.

■

Putting $j=0$ and $L=N$ in Theorem 1, we obtain the bounds on APHCs of FHS set with LHZ.

Corollary 1. *Let S be a set of M FHSs of length N over a given frequency slot set F with size q, L_{PHZ} be the LHZ of S with respect to P_{La} and P_{Lc}. For any $\overline{P}_{La}$, $\overline{P}_{Lc}$, $0 \le \overline{P}_{La} \le P_{La}$, $0 \le \overline{P}_{Lc} \le P_{Lc}$, and any positive integer Z, $0 \le Z \le L_{PHZ}$, we have*

$$qZ\overline{P}_{La} + (M-1)(Z+1)q\overline{P}_{Lc} \ge (Z+1)NM - Nq. \tag{20}$$

$$MZ\overline{P}_{La} + (M-1)(Z+1)M\overline{P}_{Lc} \ge (Z+1)[(2I+1)M - (I+1)Iq/N] - MN. \tag{21}$$

where I denotes the integer part of NM/q.

It should be noted that the Peng-Peng-Tang-Niu bound in (7) on APHCs of FHS set is only a special case of (20) of Corollary 1 for $Z=N-1$.

4 Conclusions

In this paper, based on the concepts of LHZ for FHS design, the lower bounds on the frequency slot set size, correlation window length, family size, LHZ, average partial Hamming autocorrelation and average partial Hamming crosscorrelation are derived. It has been shown that the new bounds are the generalization of the previous bounds. It is expected that the new bounds will be useful in designing and evaluating new FHS design.

In applications, it is generally desired that the FHS set S with LHZ has the following properties:

1) The LHZ should be as large as possible;
2) The maximum partial Hamming autocorrelation P_{La} within LHZ should be as small as possible;
3) The maximum partial Hamming crosscorrelation P_{Lc} within LHZ should be as small as possible;
4) The average partial Hamming autocorrelation $\overline{P}_{La}$ within LHZ should be as small as possible;
5) The average partial Hamming crosscorrelation $\overline{P}_{Lc}$ within LHZ should be as small as possible;
6) The family size M for given P_{La}, P_{Lc}, $\overline{P}_{La}$, $\overline{P}_{Lc}$, q, L and N should be as large as possible.

However, these parameters are not independent, and are bounded by the limit in (18) or (19). If the parameters q, L, N, M, $\overline{P}_{La}$ and $\overline{P}_{Lc}$ of the FHS set S satisfy inequality in (18) or (19) with equality, then it is said that the corresponding FHS set S is called an optimal average PHC FHS set with LHZ. If the sequence set S is an optimal average PHC FHS set with LHZ for all length of correlation window, then it is said that S is a strictly optimal average PHC FHS set with LHZ.

Example 1. *Let* q=7, N=7, M=6, L=7 *and* L_{PHZ}=6. *By Theorem* 1

$$6\overline{P}_{La} + 35\overline{P}_{Lc} \geq 35$$

Let F=$\{0, 1, 2, 3, 4, 5, 6\}$. *We construct the FHS set* S=$\{S_1, S_2, S_3, S_4, S_5, S_6\}$, *where*

$$S_1 = 0116166,\ S_2 = 0225255,\ S_3 = 0334344,$$
$$S_4 = 0443433,\ S_5 = 0552522,\ S_6 = 0661611.$$

and their PHCs are given by

$$H_{S_i,S_j}(0|7;\tau) = \begin{cases} \{7,2,2,2,2,2,2\}, i = j, \\ \{1,3,3,3,3,3,3\}, (i,j) = (1,6),(2,5),(3,4), \\ \{1,0,0,0,0,0,0\}, otherwise. \end{cases}$$

It can be checked that P_{La}=2, P_{Lc}=3, $\overline{P}_{La}$=2 *and* $\overline{P}_{Lc}$=23/35. *By a simple verification,* S *is an optimal average PHCs FHS set with LHZ for the correlation window length* L=7, *but not an optimal maximum PHCs FHS set with LHZ for the correlation window length* L=7.

References

1. Fan, P.Z., Darnell, M.: Sequence Design for Communications Applications. Research Studies Press. John Wiley & Sons Ltd., London (1996)
2. Lempel, A., Greenberger, H.: Families of sequence with optimal Hamming correlation properties. IEEE Trans. Inf. Theory 20, 90–94 (1974)
3. Peng, D.Y., Fan, P.Z.: Lower bounds on the Hamming auto- and cross correlations of frequency hopping sequences. IEEE Trans. Inf. Theory 50(9), 2149–2154 (2004)
4. Peng, D.Y., Peng, T., Tang, X.H., Niu, X.H.: A class of optimal frequency hopping sequences based upon the theory of power residues. In: Proceeding of the 5th International Conference on Sequences and Their Applications, pp. 188–196 (2008)
5. Eun, Y.C., Jin, S.Y., Hong, Y.P., Song, H.Y.: Frequency hopping sequences with optimal partial autocorrelation properties. IEEE Trans. Inf. Theory 50(10), 2438–2442 (2004)
6. Wang, X.N., Fan, P.Z.: A class of frequency hopping sequences with no hit zone. In: Proceeding of the 4th International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 896–898 (2003)
7. Peng, D.Y., Fan, P.Z., Lee, M.H.: Lower bounds on the periodic Hamming correlations of frequency hopping sequences with low hit zone. Science in China: Series F Information Sciences 49(2), 1–11 (2006)
8. Niu, X.H., Peng, D.Y., Liu, F.: Lower bounds on the periodic partial correlations of frequency hopping sequences with partial low hit zone. In: The Fourth International Workshop on Signal Design and Its Applications in Communications (IWSDA 2009), Fukuoka, Japan, pp. 84–87 (2009)
9. Ding, C.S., Moisio, M.J., Yuan, J.: Algebraic constructions of optimal frequency hopping sequences. IEEE Trans. Inf. Theory 53(7), 2606–2610 (2007)
10. Jia, H.D., Yuan, D., Peng, D.Y., Guo, L.: On a general class of quadratic hopping sequences. Science in China Series F: Information Sciences 51(12), 2101–2114 (2008)
11. Ge, G.N., Miao, Y., Yao, Z.X.: Optimal frequency hopping sequences: auto- and cross-correlation properties. IEEE Trans. Inf. Theory 55(2), 867–879 (2009)
12. Ding, C.S., Yin, J.X.: Sets of optimal frequency hopping sequences. IEEE Trans. Inf. Theory 54(8), 3741–3745 (2008)
13. Ye, W.X., Fan, P.Z., Gabidulin, E.M.: Construction of non-repeating frequency-hopping sequences with no-hit zone. Electronics Letters 42(12), 681–682 (2006)
14. Ye, W.X., Fan, P.Z.: Construction of frequency hopping sequences with no hit zone. Journal of Electronics (China) 24(3), 305–308 (2007)

New Families of Frequency-Hopping Sequences of Length mN Derived from the k-Fold Cyclotomy*

Jin-Ho Chung and Kyeongcheol Yang

Dept. of Electronics and Electrical Engineering
Pohang University of Science and Technology (POSTECH)
Pohang, Kyungbuk 790-784, Korea
{jinho,kcyang}@postech.ac.kr

Abstract. Let $N = p_1 \cdots p_k$ where p_i, $1 \le i \le k$, are odd primes such that $p_1 < \cdots < p_k$ and $p_i = M_i f + 1$ for some positive integers M_i and f. In this paper, we construct frequency-hopping sequence (FHS) sets by using the properties of the k-fold cycltomy. We give FHS sets with length $2N$ and frequency set size $(N-1)/f$, which are optimal with respect to the Peng-Fan bound if $k = 1$, and near-optimal if $k \ge 2$. We also present near-optimal FHS sets with length mN and frequency set size $(N-1)/f + 1$ for any integer m with $2 \le m \le M_1$. The FHS sets constructed in this paper have new parameters not covered in the literature.

Keywords: Cyclotomic numbers, frequency-hopping sequences, generalized cyclotomy, Hamming correlation, interleaved sequences.

1 Introduction

Frequency-hopping multiple-access (FHMA) has been widely employed in modern communication systems such as Bluetooth [1], ultra-wideband (UWB), military or radar applications, etc. For these systems, the receiver is confronted with the interference caused by hits of frequencies when it attempts to demodulate one of the signals sent from a number of transmitters. In order to reduce the multiple-access interference, it is desirable to employ frequency-hopping sequences (FHSs) having low Hamming correlation [2,3]. Hence, it is an important problem to construct FHS sets with large set size and low Hamming correlation. Cyclotomy [4] is one of the most frequently used techniques in design of FHSs [5]-[9].

The conventional cyclotomy is defined over a finite field. Let $\mathbb{F}_q$ be the finite field of q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, where q is a prime power. Let α be a

* This research was supported in part by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2010-(C1090-1011-0011)), and by Mid-career Researcher Program through NRF grant funded by the MEST (No. 2010-0000170).

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 76–87, 2010.

primitive element of $\mathbb{F}_q$. For a nonzero element β of $\mathbb{F}_q$, we have $\beta = \alpha^l$ for an integer $0 \le l \le q-2$, where the exponent is denoted by $l = \log_\alpha \beta$. Let M and f be positive integers such that $q = Mf + 1$. Then, $\mathbb{F}_q^*$ is decomposed into M disjoint subsets

$$C_r^M = \left\{\alpha^{Mj+r} \mid 0 \le j \le f-1\right\}, \quad r = 0, 1, \ldots, M-1$$

which are called the *cyclotomic classes* of $\mathbb{F}_q$ of order M. For two integers r and s in $\mathbb{Z}_M$, the ring of integers modulo M, the number defined by

$$(r,s)_M := |(C_r^M + 1) \cap C_s^M| \tag{1}$$

is called a *cyclotomic number* of $\mathbb{F}_q$ of order M [10].

Several types of generalized cyclotomies have been reported in the literature. Whiteman introduced a generalized cyclotomy in $\mathbb{Z}_{p_1 p_2}$ for two distinct primes p_1 and p_2 [11]. Ding and Helleseth gave another generalized cyclotomy in $\mathbb{Z}_{q_1 \cdots q_k}$ when $q_1, \ldots, q_k$ are powers of distinct primes [12]. Recently, Chung and Yang presented a k-fold cyclotomy in $\mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_k}$, which include the conventional cyclotomy as a special case [13]. Several optimal FHSs and FHS sets with new parameters were derived from the k-fold cyclotomy.

Let $N = p_1 \cdots p_k$ where p_i, $1 \le i \le k$, are odd primes such that $p_1 < \cdots < p_k$ and $p_i = M_i f + 1$ for some positive integers M_i and f. In this paper, we construct FHS sets by combining the interleaving techniques with the k-fold cycltomy. We give FHS sets with length $2N$ and frequency set size $(N-1)/f$, which are optimal with respect to the Peng-Fan bound [14] if $k = 1$, and near-optimal if $k \ge 2$. We also present near-optimal FHS sets with length mN and frequency set size $(N-1)/f + 1$ for any integer m with $2 \le m \le M_1$. In general, the existence of optimal FHSs (FHSs sets) with respect to the Lempel-Greenbeger bound (the Peng-Fan bound, respectively) is not guaranteed. Therefore, it is also important to find near-optimal FHSs (FHS sets) for a given length and a given frequency set size if there are no known optimal FHSs (FHS sets) with respect to the bound in the case. The parameters of new FHS sets constructed in this paper are not covered in the literature, and flexible in the sense that the frequency set size can take various values according to the choice of f.

The outline of the paper is as follows. In Section 2, we introduce k-fold cyclotomic numbers and briefly review their properties. We present two new near-optimal FHS sets of length mN with respect to the Peng-Fan bound in Section 3. Finally, some concluding remarks are given in Section 4.

2 k-Fold Cyclotomic Numbers

In [13], k-fold cyclotomic classes and numbers were introduced as a generalization of the conventional cyclotomic classes and numbers. We will briefly review their definitions and properties in this section.

Throughout the paper, we denote by $\lfloor x \rfloor$ the largest integer less than or equal to x. Similarly, $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. We also denote by $\langle x \rangle_y$ the least nonnegative residue of x modulo y for an integer x and a positive integer y.

2.1 Definition of k-Fold Cyclotomic Numbers

For an integer $k \geq 1$ and an integer i with $1 \leq i \leq k$, let $q_i = p_i^{e_i}$ and α_i a primitive element of $\mathbb{F}_{q_i}$ where p_i's are pairwise distinct odd primes and e_i's are positive integers. Let f be a positive integer such that there is an integer $M_i \geq 1$ satisfying $q_i = M_i f + 1$ for any $1 \leq i \leq k$. For $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_k}$ and $\mathbf{r} = (r_1, \ldots, r_k) \in \mathbb{Z}_{M_1} \times \cdots \times \mathbb{Z}_{M_k}$, we denote by $\mathbf{u} : \mathbf{r}$ a concatenation of $\mathbf{u}$ and $\mathbf{r}$, that is, $\mathbf{u} : \mathbf{r} = (u_1, \ldots, u_k) : (r_1, \ldots, r_k)$.

Definition 1. *Let $\mathcal{I}$ be the set of all vectors $\mathbf{u} : \mathbf{r} = (u_1, \ldots, u_k) : (r_1, \ldots, r_k)$ such that $u_i \in \{0, 1, \alpha_i^{M_i}, \ldots, \alpha_i^{M_i(f-1)}\} \subset \mathbb{F}_{q_i}$ and $r_i \in \mathbb{Z}_{M_i}$ for $1 \leq i \leq k$, satisfying the following conditions:*

(a) *there exists an integer i with $1 \leq i \leq k$ such that $u_i \neq 0$;*
(b) *$u_1 \in \{0, 1\}$;*
(c) *$u_i = 1$ if $u_1 = 0, \ldots, u_{i-1} = 0$, and $u_i \neq 0$; and*
(d) *if $u_i = 0$, then $r_i = 0$.*

The size of $\mathcal{I}$ is given by $|\mathcal{I}| = (q_1 \cdots q_k - 1)/f$. We define a binary operation between two elements in $\mathcal{I} \cup \{\mathbf{0} : \mathbf{0}\}$ to present the k-fold cyclotomy, where $\mathbf{0} : \mathbf{0} = (0, \ldots, 0) : (0, \ldots, 0)$.

Definition 2. *Let $\mathbf{u} : \mathbf{r} = (u_1, \ldots, u_k) : (r_1, \ldots, r_k)$ and $\mathbf{u}' : \mathbf{r}' = (u'_1, \ldots, u'_k) : (r'_1, \ldots, r'_k)$ be two elements in $\mathcal{I} \cup \{\mathbf{0} : \mathbf{0}\}$. If $u_i u'_i = 0$ for all $1 \leq i \leq k$, we define $\oplus$ as $\mathbf{u} : \mathbf{r} \oplus \mathbf{u}' : \mathbf{r}' = \mathbf{0} : \mathbf{0}$. If $u_i u'_i \neq 0$ for some i with $1 \leq i \leq k$, let*

$$\beta_i = \left\lfloor \frac{r_i + r'_i}{M_i} \right\rfloor - \left\lfloor \frac{r_{\hat{k}} + r'_{\hat{k}}}{M_{\hat{k}}} \right\rfloor - \epsilon_{\hat{k}}$$

where $\hat{k} = \min_{1 \leq i \leq k} \{i \mid u_i u'_i \neq 0\}$ and $\epsilon_{\hat{k}} = (\log_{\alpha_{\hat{k}}} u_{\hat{k}} + \log_{\alpha_{\hat{k}}} u'_{\hat{k}})/M_{\hat{k}} \mod f$. The operation $\oplus$ between $\mathbf{u} : \mathbf{r}$ and $\mathbf{u}' : \mathbf{r}'$ in $\mathcal{I}$ is defined as

$$\mathbf{u} : \mathbf{r} \oplus \mathbf{u}' : \mathbf{r}' = (u_1 u'_1 \sigma_1, \ldots, u_k u'_k \sigma_k) : ((r_1 + r'_1)_{M_1}, \ldots, (r_k + r'_k)_{M_k})$$

where $\sigma_i = \alpha_i^{M_i \beta_i}$, and

$$(r_i + r'_i)_{M_i} = \begin{cases} \langle r_i + r'_i \rangle_{M_i}, & \text{if } u_i u'_i \neq 0 \\ 0, & \text{otherwise} \end{cases}$$

for $1 \leq i \leq k$.

It is easily checked that the set $\mathcal{I} \cup \{\mathbf{0} : \mathbf{0}\}$ is closed, associative, and commutative under the operation $\oplus$. Furthermore, $\mathbf{1} : \mathbf{0} = (1, \ldots, 1) : (0, \ldots, 0)$ is the identity with respect to $\oplus$, that is,

$$\mathbf{u} : \mathbf{r} \oplus \mathbf{1} : \mathbf{0} = \mathbf{1} : \mathbf{0} \oplus \mathbf{u} : \mathbf{r} = \mathbf{u} : \mathbf{r}$$

for any $\mathbf{u} : \mathbf{r} \in \mathcal{I} \cup \{\mathbf{0} : \mathbf{0}\}$. Let $\mathcal{I}^*$ be the subset of $\mathcal{I}$, given by

$$\mathcal{I}^* = \{\mathbf{u} : \mathbf{r} \in \mathcal{I} \mid u_i \neq 0 \text{ for all } 1 \leq i \leq k\}.$$

Definition 3. *For any* $\mathbf{u}:\mathbf{r}=(u_1,\ldots,u_k):(r_1,\ldots,r_k)\in\mathcal{I}^*$, *its inverse* $\overline{\mathbf{u}:\mathbf{r}}$ *with respect to* $\oplus$ *is defined as* $\overline{\mathbf{u}:\mathbf{r}}=(\overline{u}_1,\ldots,\overline{u}_k):(\overline{r}_1,\ldots,\overline{r}_k)$, *where*

$$\overline{u}_i=\begin{cases} u_i^{-1}\alpha_i^{-M_i}, & \text{if } r_1=0 \text{ and } r_i\neq 0\\ u_i^{-1}\alpha_i^{M_i}, & \text{if } r_1\neq 0 \text{ and } r_i=0\\ u_i^{-1}, & \text{otherwise,}\end{cases}$$

and $\overline{r}_i=\langle M_i-r_i\rangle_{M_i}$ *for* $1\le i\le k$.

It is easily checked that $\mathbf{u}:\mathbf{r}\oplus\overline{\mathbf{u}:\mathbf{r}}=\overline{\mathbf{u}:\mathbf{r}}\oplus\mathbf{u}:\mathbf{r}=\mathbf{1}:\mathbf{0}$ for any $\mathbf{u}:\mathbf{r}\in\mathcal{I}^*$, i.e., every element of $\mathcal{I}^*$ has an inverse in $\mathcal{I}^*$. Therefore, $\mathcal{I}^*$ is a commutative group under the operation $\oplus$.

For any $\mathbf{a}=(a_1,\ldots,a_k)$ and $\mathbf{b}=(b_1,\ldots,b_k)$ in $\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}$, we define the binary operation $\circ$ as

$$\mathbf{a}\circ\mathbf{b}=(a_1b_1,\ldots,a_kb_k).$$

Given a nonempty subset S of $\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}$, the operation $\circ$ is naturally extended to

$$\mathbf{a}\circ S=\{\mathbf{a}\circ\mathbf{b}\,|\,\mathbf{b}\in S\}.$$

From the definition of $\mathcal{I}$, it is easily checked that any $\mathbf{a}\in\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}\setminus\{\mathbf{0}\}$ can be uniquely represented as

$$\mathbf{a}=(u_1,\ldots,u_k)\circ\left(\alpha_1^{M_1j+r_1},\ldots,\alpha_k^{M_kj+r_k}\right)$$

for some $\mathbf{u}:\mathbf{r}=(u_1,\ldots,u_k):(r_1,\ldots,r_k)\in\mathcal{I}$ and some $0\le j\le f-1$. In other words, there exists a unique pair of $\mathbf{u}:\mathbf{r}$ and j for $\mathbf{a}\in\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}\setminus\{\mathbf{0}\}$.

Definition 4. *Let* $\mathbf{u}:\mathbf{r}=(u_1,\ldots,u_k):(r_1,\ldots,r_k)\in\mathcal{I}\cup\{\mathbf{0}:\mathbf{0}\}$. *The subset* $C_{\mathbf{u}:\mathbf{r}}$ *of* $\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}$ *is defined as*

$$C_{\mathbf{u}:\mathbf{r}}=\left\{(u_1,\ldots,u_k)\circ\left(\alpha_1^{M_1j+r_1},\ldots,\alpha_k^{M_kj+r_k}\right)\;\middle|\;0\le j\le f-1\right\}.$$

Clearly, $|C_{\mathbf{u}:\mathbf{r}}|=f$ for any $\mathbf{u}:\mathbf{r}\in\mathcal{I}$ and $|C_{\mathbf{0}:\mathbf{0}}|=1$. Let $M=|\mathcal{I}|$, where $|\mathcal{I}|=(q_1\cdots q_k-1)/f$. For $\mathbf{u}:\mathbf{r}\in\mathcal{I}$, the set $C_{\mathbf{u}:\mathbf{r}}$ will be referred to as a *k-fold cyclotomic class of $\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}$ of order M*. Accordingly, $\mathcal{I}$ will be called *the set of indices for the k-fold cyclotomic classes of $\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}$ of order M*. It is easily checked that

$$\bigcup_{\mathbf{u}:\mathbf{r}\in\mathcal{I}}C_{\mathbf{u}:\mathbf{r}}=\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}\setminus\{\mathbf{0}\}.$$

Furthermore, for any $\mathbf{u}:\mathbf{r}$ and $\mathbf{u}':\mathbf{r}'$ in $\mathcal{I}$,

$$C_{\mathbf{u}:\mathbf{r}}\cap C_{\mathbf{u}':\mathbf{r}'}=\phi\quad\text{iff}\quad\mathbf{u}:\mathbf{r}\neq\mathbf{u}':\mathbf{r}',\tag{2}$$

and

$$\mathbf{a}\circ C_{\mathbf{u}:\mathbf{r}}=C_{\mathbf{u}:\mathbf{r}\oplus\mathbf{u}':\mathbf{r}'}\quad\text{if}\quad\mathbf{a}\in C_{\mathbf{u}':\mathbf{r}'}.\tag{3}$$

Generalizing the cyclotomic number given in (1), it is possible to define a k-fold cyclotomic number of $\mathbb{F}_{q_1}\times\cdots\times\mathbb{F}_{q_k}$ of order M in the following.

Definition 5. *For any* $\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}' \in \mathcal{I} \cup \{\mathbf{0}:\mathbf{0}\}$, *let*

$$(\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}')_M := |(C_{\mathbf{u}:\mathbf{r}} + \mathbf{1}) \cap C_{\mathbf{u}':\mathbf{r}'}| \tag{4}$$

where $\mathbf{1} = (1, \ldots, 1)$, *and*

$$C_{\mathbf{u}:\mathbf{r}} + \mathbf{1} = \{(a_1 + 1, \ldots, a_k + 1) \mid \mathbf{a} = (a_1, \ldots, a_k) \in C_{\mathbf{u}:\mathbf{r}}\}.$$

In particular, the number $(\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}')_M$ *is called a* k*-fold cyclotomic number of* $\mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_k}$ *of order* M, *when* $\mathbf{u}:\mathbf{r} \in \mathcal{I}$ *and* $\mathbf{u}':\mathbf{r}' \in \mathcal{I}$.

2.2 Properties of k-Fold Cyclotomic Numbers

In [13], the following properties of k-fold cyclotomic numbers were derived, which include the corresponding properties of the conventional cyclotomic numbers in (1) as a special case.

Theorem 6 ([13]). *Let* $(\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}')_M$ *be the* k*-fold cyclotomic number defined in* (4) *with* $\mathbf{u}:\mathbf{r} = (u_1, \ldots, u_k) : (r_1, \ldots, r_k)$ *and* $\mathbf{u}':\mathbf{r}' = (u'_1, \ldots, u'_k) : (r'_1, \ldots, r'_k)$ *in* $\mathcal{I}$. *Then the followings hold.*

(a) *For any* $\mathbf{u}:\mathbf{r} \in \mathcal{I}^*$ *and any* $\mathbf{u}':\mathbf{r}' \in \mathcal{I}$, *we have*

$$(\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}')_M = (\overline{\mathbf{u}:\mathbf{r}}, \mathbf{u}':\mathbf{r}' \oplus \overline{\mathbf{u}:\mathbf{r}})_M.$$

(b) *For any* $\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}' \in \mathcal{I}$, *we have*

$$(\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}')_M = \begin{cases} (\mathbf{u}':\mathbf{r}', \mathbf{u}:\mathbf{r})_M, & \text{if } 2 \mid f \\ (\mathbf{u}':\mathbf{r}' \oplus \Gamma_M, \mathbf{u}:\mathbf{r} \oplus \Gamma_M)_M, & \text{if } 2 \nmid f \end{cases}$$

where $\Gamma_M = (1, \ldots, 1) : \left(\frac{M_1}{2}, \ldots, \frac{M_k}{2}\right) \in \mathcal{I}^*$.

(c) *For any* $\mathbf{u}:\mathbf{r} \in \mathcal{I}$, *we have*

$$\sum_{\mathbf{u}':\mathbf{r}' \in \mathcal{I}} (\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}')_M = \begin{cases} f-1, & \text{if } \mathbf{u}:\mathbf{r} = \mathbf{1}:\mathbf{0} \text{ and } 2 \mid f \\ f-1, & \text{if } \mathbf{u}:\mathbf{r} = \Gamma_M \text{ and } 2 \nmid f \\ f, & \text{otherwise.} \end{cases}$$

(d) *For any* $\mathbf{u}':\mathbf{r}' \in \mathcal{I}$, *we have*

$$\sum_{\mathbf{u}:\mathbf{r} \in \mathcal{I}} (\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}')_M = \begin{cases} f-1, & \text{if } \mathbf{u}':\mathbf{r}' = \mathbf{1}:\mathbf{0} \\ f, & \text{otherwise.} \end{cases}$$

(e) (*k-fold diagonal sum*) *For any* $\mathbf{u}':\mathbf{r}' \in \mathcal{I}$, *we have*

$$\sum_{\mathbf{u}:\mathbf{r} \in \mathcal{I}} (\mathbf{u}:\mathbf{r}, \mathbf{u}:\mathbf{r} \oplus \mathbf{u}':\mathbf{r}')_M \le f.$$

Moreover,

$$\sum_{\mathbf{u}:\mathbf{r} \in \mathcal{I}} (\mathbf{u}:\mathbf{r}, \mathbf{u}:\mathbf{r})_M = f - 1 \tag{5}$$

and

$$\sum_{\mathbf{u}:\mathbf{r}\in\mathcal{I}} (\mathbf{u}:\mathbf{r}, \mathbf{u}:\ \mathbf{r}\oplus\mathbf{u}':\mathbf{r}')_M = f \tag{6}$$

if $\mathbf{u}':\mathbf{r}' \in \mathcal{I}^*$ *and* $r'_i \neq 0 \bmod M_i$ *for all* $1 \le i \le k$.

For a positive integer l with $1 \le l \le k$, let $S = \{i_1, \ldots, i_l\}$ be a subset of $\{1, 2, \ldots, k\}$, where $1 \le i_1 < \cdots < i_l \le k$. Let $\mathbf{d} = (d_1, \ldots, d_k) \in \mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_k}$ be the vector of length k, given by

$$d_i = \begin{cases} 1, & \text{if } i \in S \\ 0, & \text{otherwise.} \end{cases}$$

Then, it is natural to consider the number

$$|(C_{\mathbf{u}:\mathbf{r}} + \mathbf{d}) \cap C_{\mathbf{u}':\mathbf{r}'}|$$

for $\mathbf{u}:\mathbf{r}, \mathbf{u}':\mathbf{r}' \in \mathcal{I}$. When $d_i = 1$ for all $1 \le i \le k$, it is equal to the k-fold cyclotomic number defined in (4). In some cases, the sum of $|(C_{\mathbf{u}:\mathbf{r}} + \mathbf{d}) \cap C_{\mathbf{u}:\mathbf{r}\oplus\mathbf{u}':\mathbf{r}'}|$ over $\mathcal{I}$ corresponding to (5) or (6) is given as follows.

Theorem 7 ([13]). *Let* $\mathbf{u}':\mathbf{r}' \in \mathcal{I}^*$ *with* $r'_i \neq 0 \bmod M_i$ *for all* $1 \le i \le k$. *Then we have*

$$\sum_{\mathbf{u}:\mathbf{r}\in\mathcal{I}} |(C_{\mathbf{u}:\mathbf{r}} + \mathbf{d}) \cap C_{\mathbf{u}:\mathbf{r}\oplus\mathbf{u}':\mathbf{r}'}| = f$$

and

$$\sum_{\mathbf{u}:\mathbf{r}\in\mathcal{I}} |(C_{\mathbf{u}:\mathbf{r}} + \mathbf{d}) \cap C_{\mathbf{u}:\mathbf{r}}| = f - 1.$$

In the next section, the properties in Theorems 6 and 7 will be used to calculate the Hamming correlations of FHS sets derived from the k-fold cyclotomy.

3 Frequency-Hopping Sequence Sets of Length mN

3.1 Preliminaries to FHSs

For communication systems employing FHMA, it is an important problem to find FHSs or FHS sets with good Hamming correlation properties for a given length and a given frequency set size. For a survey of FHSs and their applications, we refer to [2,3,15]. We will begin with a brief review of FHSs for our presentation.

Let $\mathcal{F} = \{f_0, f_1, \ldots, f_{M-1}\}$ be a set of available frequencies. A sequence $X = \{X(t)\}_{t=0}^{N-1}$ is called a frequency-hopping sequence of length N over $\mathcal{F}$ if $X(t) \in \mathcal{F}$ for all $0 \le t \le N-1$. For two FHSs X and Y of length N over $\mathcal{F}$, the *periodic Hamming correlation* between X and Y is defined as

$$H_{X,Y}(\tau) = \sum_{t=0}^{N-1} h[X(t), Y(\langle t+\tau\rangle_N)], \quad 0 \le \tau \le N-1$$

where

$$h[x,y] = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{otherwise.} \end{cases}$$

If $X = Y$, $H_{X,Y}(\tau)$ is called the *Hamming autocorrelation* of X, denoted by $H_X(\tau)$. The *maximum out-of-phase Hamming autocorrelation* of X is defined as

$$H(X) = \max_{1 \le \tau \le N-1} \{H_X(\tau)\}.$$

Throughout the section, an FHS X of length N over $\mathcal{F}$ with $|\mathcal{F}| = M$ will be referred to as an (N, M, λ) FHS if $H(X) = \lambda$. The following lemma is well-known as the *Lempel-Greenberger bound*.

Lemma 8 ([16]). *For any FHS X of length N over $\mathcal{F}$ with $|\mathcal{F}| = M$,*

$$H(X) \ge \left\lceil \frac{(N-b)(N+b-M)}{M(N-1)} \right\rceil \tag{7}$$

where $b = \langle N \rangle_M$.

Let $\mathcal{S}$ be the set of all FHSs of length N over $\mathcal{F}$. For any two distinct FHSs X and Y in $\mathcal{S}$, let

$$H(X,Y) = \max_{0 \le \tau \le N-1} \{H_{X,Y}(\tau)\}.$$

For a subset $\mathcal{U}$ of $\mathcal{S}$, the *maximum out-of-phase Hamming autocorrelation* $H_{\mathrm{a}}(\mathcal{U})$ and the *maximum Hamming crosscorrelation* $H_{\mathrm{c}}(\mathcal{U})$ of $\mathcal{U}$ are defined as

$$H_{\mathrm{a}}(\mathcal{U}) = \max_{X \in \mathcal{U}} \{H(X)\},$$
$$H_{\mathrm{c}}(\mathcal{U}) = \max_{X,Y \in \mathcal{U},\, X \ne Y} \{H(X,Y)\},$$

respectively. The *maximum Hamming correlation* of $\mathcal{U}$ is also defined as

$$H(\mathcal{U}) = \max\{H_{\mathrm{a}}(\mathcal{U}), H_{\mathrm{c}}(\mathcal{U})\}.$$

When $H_{\mathrm{a}}(\mathcal{U}) = \lambda_{\mathrm{a}}$, $H_{\mathrm{c}}(\mathcal{U}) = \lambda_{\mathrm{c}}$, $|\mathcal{F}| = M$, and $|\mathcal{U}| = L$, we call $\mathcal{U}$ an $(N, M, \lambda_{\mathrm{a}}, \lambda_{\mathrm{c}}; L)$ FHS set. Peng and Fan established some bounds on the maximum out-of-phase Hamming autocorrelation and crosscorrelation of an FHS set in terms of frequency set size, length, and the number of FHSs [14]. The following lemma is known as a simplified version of the Peng-Fan bound.

Lemma 9 ([14]). *Let $\mathcal{U}$ be a set of L FHSs of length N over a frequency set with size M, and $I = \lfloor \frac{NL}{M} \rfloor$. Then we have*

$$H(\mathcal{U}) \ge \left\lceil \frac{(NL-M)N}{(NL-1)M} \right\rceil. \tag{8}$$

Let λ_L (resp. λ_P) be the right-hand side in (7) (resp. in (8)). From now on, we use the following definitions in this paper.

(a) An FHS X is said to be *optimal* (resp. *near-optimal*) if $H(X) = \lambda_L$ (resp. $H(X) = \lambda_L + 1$).
(b) An FHS set $\mathcal{U}$ will be referred to as an *optimal FHS set* (resp. *near-optimal FHS set*) if $H(\mathcal{U}) = \lambda_P$ (resp. $H(\mathcal{U}) = \lambda_P + 1$).

3.2 New Near-Optimal FHS Sets of Length mN

Interleaving techniques are employed to construct a sequence of length mN from m sequences of length N, which are not necessarily distinct for some positive integers m and N [17]. In [8], several new classes of optimal FHS sets constructed by interleaving techniques were presented. In particular, $(2p, M, 2f+1, 2f+1; M/2)$ optimal FHS sets were constructed for an odd prime $p = Mf + 1$ such that f is an odd integer, by combining an interleaving technique with the conventional cyclotomy.

For odd primes $p_1 < \cdots < p_k$, let f be a positive integer such that there exists an integer $M_i \geq 1$ satisfying $p_i = M_i f + 1$ for $1 \leq i \leq k$. Let $N = p_1 \cdots p_k$, $M = (N-1)/f$, and m a positive integer such that $2 \leq m \leq M_1$. Then any integer t with $0 \leq t \leq mN - 1$ can be uniquely represented as

$$t := (t_0, t_1, \ldots, t_k)$$

where $t_0 = \langle t \rangle_m$ and $t_i = \langle t \rangle_{p_i}$ for $1 \leq i \leq k$.

When $m = 2$, it is possible to construct (near-)optimal FHS sets of length $2N$ and frequency set size M by employing the k-fold cyclotomy as follows.

Construction $\mathcal{A}$: Let $p_1, \ldots, p_k$ be odd primes such that $p_1 < \cdots < p_k$ and $p_i = M_i f + 1$ with an odd integer f and a positive integer M_i for $1 \leq i \leq k$. Let $N = p_1 \cdots p_k$, $M = (N-1)/f$, and π a one-to-one mapping from $\mathcal{I}$ to $\mathbb{Z}_M$. Let $Y_h = \{Y_h(t)\}_{t=0}^{2N-1}$ be the FHS of length $2N$ over $\mathbb{Z}_M$ defined by

$$Y_h(t) = \begin{cases} \pi(\mathbf{1} : \mathbf{0}), & \text{if } t = 0 \\ \pi(\Lambda_1), & \text{if } t = N \\ \pi(\mathbf{u} : \mathbf{r} \oplus \mathbf{1} : \mathbf{h}), & \text{if } t_0 = 0 \text{ and } (t_1, \ldots, t_k) \in C_{\mathbf{u}:\mathbf{r}}, \\ & \text{or } t_0 = 1 \text{ and } (t_1, \ldots, t_k) \in C_{\mathbf{u}:\mathbf{r} \oplus \Gamma_M} \end{cases}$$

for $0 \leq h \leq \frac{M_1}{2} - 2$, and

$$Y_{-1}(t) = \begin{cases} \pi(\Lambda_1), & \text{if } t = 0 \\ \pi(\Lambda_2), & \text{if } t = N \\ \pi(\mathbf{u} : \mathbf{r} \oplus \mathbf{1} : (-1, \ldots, -1)), & \text{if } t_0 = 0 \text{ and } (t_1, \ldots, t_k) \in C_{\mathbf{u}:\mathbf{r}}, \\ & \text{or } t_0 = 1 \text{ and } (t_1, \ldots, t_k) \in C_{\mathbf{u}:\mathbf{r} \oplus \Gamma_M} \end{cases}$$

where $\Gamma_M = \mathbf{1} : \left(\frac{M_1}{2}, \ldots, \frac{M_k}{2}\right)$, $\Lambda_1 = \mathbf{1} : \left(\frac{M_1}{2} - 1, 0, \ldots, 0\right) \in \mathcal{I}$ and $\Lambda_2 = \mathbf{1} : (M_1 - 2, 0, \ldots, 0) \in \mathcal{I}$. The set $\mathcal{Y}_1$ is defined as

$$\mathcal{Y}_1 = \{Y_h \mid -1 \leq h \leq M_1/2 - 2\}.$$

Theorem 10. *When $M \geq 4$, the set $\mathcal{Y}_1$ in Construction $\mathcal{A}$ is a $(2N, M, 2f+1, 2f+1; M_1/2)$ FHS set whose FHSs are near-optimal. The set $\mathcal{Y}_1$ is optimal if $k = 1$ and near-optimal if $k \geq 2$.*

Proof. Let $\tau = (\tau_0, \ldots, \tau_k)$ where $\tau_0 = \langle \tau \rangle_2$ and $\tau_i = \langle \tau \rangle_{p_i}$ for $1 \leq i \leq k$. Denote the Hamming correlation between Y_{h_1} and Y_{h_2} by $H_{h_1,h_2}(\tau)$. Consider the case that $0 \leq h_1, h_2 \leq \frac{M_1}{2} - 2$. We have

$$H_{h_1,h_2}(\tau) = \sum_{t_0=0}^{1} \sum_{\langle t\rangle_N \in \mathbb{Z}_N \setminus \{0,\langle -\tau\rangle_N\}} h\left[Y_{h_1}(t_0,\ldots,t_k), Y_{h_2}(\langle t_0+\tau_0\rangle_2,\ldots,\langle t_k+\tau_k\rangle_{p_k})\right] + \Delta \tag{9}$$

where

$$\begin{aligned}\Delta = {} & h[\pi(\mathbf{1}:\mathbf{0}), Y_{h_2}(\tau)] + h[Y_{h_1}(-\tau), \pi(\mathbf{1}:\mathbf{0})] \\ & + h[\pi(\Lambda_1), Y_{h_2}(N+\tau)] + h[Y_{h_1}(N-\tau), \pi(\Lambda_1)]\end{aligned} \tag{10}$$

We divide our computation of $H_{h_1,h_2}(\tau)$ in (9) into four subcases and show that $H_{h_1,h_2}(\tau) \le 2f+1$ in each subcase.

Subcase i) $\langle\tau\rangle_N = 0$: It is easily checked that

$$H_{h_1,h_2}(0) = \begin{cases} 2N, & \text{if } h_1 = h_2 \\ 2, & \text{if } h_1 \neq h_2 \end{cases}$$

and

$$H_{h_1,h_2}(N) = 0$$

for any $0 \le h_1, h_2 \le M_1/2 - 2$.

Subcase ii) $\tau_0 = 0$ and $\tau_i \neq 0$ for all $1 \le i \le k$: Let $(\tau_1^{-1},\ldots,\tau_k^{-1}) \in C_{\mathbf{u}':\mathbf{r}'}$ for some $\mathbf{u}':\mathbf{r}' \in \mathcal{I}^*$. Then $H_{h_1,h_2}(\tau)$ in (9) can be represented as

$$\begin{aligned} H_{h_1,h_2}(\tau) &= 2\sum_{\mathbf{u}:\mathbf{r}\in\mathcal{I}} ((\mathbf{u}:\mathbf{r}\oplus\mathbf{1}:\mathbf{h}_1)\oplus\mathbf{u}':\mathbf{r}', (\mathbf{u}:\mathbf{r}\oplus\mathbf{1}:\mathbf{h}_2)\oplus\mathbf{u}':\mathbf{r}') + \Delta \\ &= 2\sum_{\mathbf{u}:\mathbf{r}\in\mathcal{I}} (\mathbf{u}:\mathbf{r}, \mathbf{u}:\mathbf{r}\oplus(\mathbf{1}:\mathbf{h}_2\oplus\overline{\mathbf{1}:\mathbf{h}_1})) + \Delta. \end{aligned}$$

By the k-fold diagonal sum in (e) of Theorem 6, we get

$$H_{h_1,h_2}(\tau) = \begin{cases} 2f-2+\Delta, & \text{if } h_1 = h_2 \\ 2f+\Delta, & \text{if } h_1 \neq h_2. \end{cases}$$

Moreover, (10) can be rewritten as

$$\begin{aligned} \Delta &= \left|\{(\tau_1,\ldots,\tau_k)\}\cap C_{\overline{\mathbf{1}:\mathbf{h}_2}}\right| + \left|\{(-\tau_1,\ldots,-\tau_k)\}\cap C_{\overline{\mathbf{1}:\mathbf{h}_1}}\right| \\ &\quad + \left|\{(\tau_1,\ldots,\tau_k)\}\cap C_{(\Lambda_1\oplus\overline{\mathbf{1}:\mathbf{h}_2})\oplus\Gamma_M}\right| + \left|\{(-\tau_1,\ldots,-\tau_k)\}\cap C_{(\Lambda_1\oplus\overline{\mathbf{1}:\mathbf{h}_1})\oplus\Gamma_M}\right| \\ &= \left|\{(\tau_1,\ldots,\tau_k)\}\cap C_{\overline{\mathbf{1}:\mathbf{h}_2}}\right| + \left|\{(\tau_1,\ldots,\tau_k)\}\cap C_{\overline{\mathbf{1}:\mathbf{h}_1}\oplus\Gamma_M}\right| \\ &\quad + \left|\{(\tau_1,\ldots,\tau_k)\}\cap C_{(\Lambda_1\oplus\overline{\mathbf{1}:\mathbf{h}_2})\oplus\Gamma_M}\right| + \left|\{(\tau_1,\ldots,\tau_k)\}\cap C_{\Lambda_1\oplus\overline{\mathbf{1}:\mathbf{h}_1}}\right| \end{aligned}$$

and so we have

$$\Delta = \begin{cases} 1, & \text{if } (\tau_1,\ldots,\tau_k) \in C_{\overline{\mathbf{1}:\mathbf{h}_2}}, C_{\overline{\mathbf{1}:\mathbf{h}_1}\oplus\Gamma_M}, C_{(\Lambda_1\oplus\overline{\mathbf{1}:\mathbf{h}_2})\oplus\Gamma_M}, \text{ or } C_{\Lambda_1\oplus\overline{\mathbf{1}:\mathbf{h}_1}} \\ 0, & \text{otherwise.} \end{cases}$$

Subcase iii) $\tau_0 = 1$ and $\tau_i \neq 0$ for all $1 \leq i \leq k$: In a similar way to Subcase ii), it is possible to prove that

$$H_{h_1,h_2}(\tau) \leq 2f + 1$$

for any $0 \leq h_1, h_2 \leq M_1/2 - 2$.

Subcase iv) $\langle \tau \rangle_N \neq 0$ and $\tau_i = 0$ for some i with $1 \leq i \leq k$: After reducing the problem into the l-fold case for an integer l with $1 \leq l < k$, it may be similarly proved that

$$H_{h_1,h_2}(\tau) \leq \begin{cases} 2f - 2, & \text{if } h_1 = h_2 \text{ and } \tau_0 = 0 \\ 2f, & \text{otherwise.} \end{cases}$$

In the remaining case that $h_1 = -1$ or $h_2 = -1$, it may be similarly proved that

$$H_{h_1,h_2}(\tau) \leq 2f + 1$$

for $0 \leq \tau \leq 2N - 1$ when $h_1 \neq h_2$, and for $0 < \tau \leq 2N - 1$ when $h_1 = h_2 = -1$. Summarizing the above results, we can conclude that $\mathcal{Y}_1$ is a $(2N, M, 2f+1, 2f+1; M_1/2)$ FHS set. Plugging the parameters of $\mathcal{Y}_1$ into (7) and (8), we get

$$\left\lceil \frac{(2N-2)(2N+2-M)}{M(2N-1)} \right\rceil = 2f$$

and

$$\left\lceil \frac{(2NM_1 - M)2N}{(2NM_1 - 1)M} \right\rceil = \begin{cases} 2f + 1, & \text{if } k = 1 \\ 2f, & \text{otherwise,} \end{cases}$$

respectively. Therefore, the optimality of $\mathcal{Y}_1$ can be easily checked. □

It is easily checked that Construction C1 in [8] corresponds to the $k = 1$ case in Construction $\mathcal{A}$.

Remark: In general, the existence of optimal FHSs (FHS sets) with respect to the Lempel-Greenberger bound (the Peng-Fan bound, respectively) is not guaranteed for any given length and any given frequency set size. For example, one can easily check that no $(6, 2, 3)$ optimal FHSs with respect to the Lempel-Greenberger bound exist. For these reasons, some FHSs which are near-optimal with respect to the Lempel-Greenberger bound are 'actually' optimal if there are no optimal FHSs with the same length and frequency set size. Therefore, it is also important to design near-optimal FHSs (FHS sets), when there are no known optimal FHSs (FHS sets, respectively) with the same length and frequency set size. Note that the parameters obtained by Construction $\mathcal{A}$ are not covered in the literature.

If we add another symbol which is not an element of $\mathbb{Z}_M$, it is possible to construct (near-)optimal FHS sets of length mN and frequency set size $M + 1$ for any integer m with $2 \leq m \leq M_1$ by employing the k-fold cyclotomy.

Construction $\mathcal{B}$: Let $p_1, \ldots, p_k$ be odd primes such that $p_1 < \cdots < p_k$ and $p_i = M_i f + 1$ with positive integers f and M_i for $1 \leq i \leq k$. Let $N = p_1 \cdots p_k$,

$M = (N-1)/f$, and π a one-to-one mapping from $\mathcal{I}$ to $\mathbb{Z}_M$. For an integer $2 \le m \le M_1$, let $L = \lfloor \frac{M_1}{m} \rfloor$. For $0 \le h \le L-1$, define the FHS $Y_h = \{Y_h(t)\}_{t=0}^{mN-1}$ of length mN over $\mathbb{Z}_M \cup \{\infty\}$ as

$$Y_h(t) = \begin{cases} \infty, & \text{if } \langle t \rangle_N = 0 \\ \pi(\mathbf{u} : \mathbf{r} \oplus \Lambda_{t_0,h}), & \text{if } (t_1, \ldots, t_k) \in C_{\mathbf{u}:\mathbf{r}} \end{cases}$$

where $\Lambda_{t_0,h} = \mathbf{1} : (t_0 L + h, \ldots, t_0 L + h) \in \mathcal{I}$. The set $\mathcal{Y}_2$ is defined as

$$\mathcal{Y}_2 = \{Y_h \,|\, 0 \le h \le L-1\}.$$

Theorem 11. *The set $\mathcal{Y}_2$ in Construction $\mathcal{B}$ is an $(mN, M+1, mf, mf; L)$ FHS set. When $f = 1$, $\mathcal{Y}_2$ is an optimal FHS set, whose FHSs are also optimal. When $2 \le f \le \frac{2M}{m} + 1$, $\mathcal{Y}_2$ is a near-optimal FHS set, whose FHSs are also near-optimal.*

Proof. Let $\tau = (\tau_0, \ldots, \tau_k)$ where $\tau_0 = \langle \tau \rangle_m$ and $\tau_i = \langle \tau \rangle_{p_i}$ for $1 \le i \le k$. Denote the Hamming correlation between Y_{h_1} and Y_{h_2} by $H_{h_1,h_2}(\tau)$.

Case i) $\langle \tau \rangle_N = 0$: It is easily checked that

$$H_{h_1,h_2}(\tau) = \begin{cases} mN, & \text{if } h_1 = h_2 \text{ and } \tau = 0 \\ m, & \text{otherwise.} \end{cases}$$

Case ii) $\langle \tau \rangle_N \neq 0$ and $\tau_i \neq 0$ for all $1 \le i \le k$: In a similar approach to the Proof of Theorem 10, we have

$$H_{h_1,h_2}(\tau) = m \sum_{\mathbf{u}:\mathbf{r} \in \mathcal{I}} (\mathbf{u} : \mathbf{r}, \mathbf{u} : \mathbf{r} \oplus \mathbf{1} : \mathbf{h}_3)_M$$

for some $\mathbf{1} : \mathbf{h}_3 \in \mathcal{I}^*$. Then, by the k-fold diagonal sum in (e) of Theorem 6, we get

$$H_{h_1,h_2}(\tau) = \begin{cases} mf - m, & \text{if } \mathbf{h}_3 = (0, \ldots, 0) \\ mf, & \text{otherwise.} \end{cases}$$

Case iii) $\langle \tau \rangle_N \neq 0$ and $\tau_i = 0$ for some i with $1 \le i \le k$: After reducing the problem into the l-fold case for an integer l with $1 \le l < k$, it may be similarly proved that

$$H_{h_1,h_2}(\tau) \le mf.$$

Summarizing the above results, we can conclude that $\mathcal{Y}_2$ is an $(mN, M+1, mf, mf; L)$ FHS set. Its optimality can be easily checked by plugging the parameters of $\mathcal{Y}_2$ into (7) and (8). □

4 Conclusion

For odd primes $p_1, \ldots, p_k$ such that $p_1 < \cdots < p_k$ and there exists an integer f with $p_i = M_i f + 1$, we presented new FHS sets of length mN by employing the k-fold cyclotomy, where $N = p_1 \cdots p_k$ and $2 \le m \le M_1$. When $m = 2$, we constructed $(2N, M, 2f+1, 2f+1; M_1/2)$ near-optimal FHS sets whose FHSs are also near-optimal. For an integer m with $2 \le m \le M_1$, we also gave $(mN, M+1, mf, mf; \lfloor M_1/m \rfloor)$ near-optimal FHS sets. The FHS sets constructed in this paper have new parameters not covered in the literature.

References

1. Specification of the Bluetooth Systems-Core. The Bluetooth Special Interest Group (SIG), http://www.bluetooth.com
2. Simon, M.K., Omura, J.K., Scholtz, R.A., Levitt, B.K.: Spread Spectrum Communications Handbook. McGraw-Hill Inc., New York (1994) (Revised Ed.)
3. Sarwate, D.V.: Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications. In: Wicker, S.B., Bharagava, V.K. (eds.) Reed-Solomon Codes and Their Applications. IEEE Press, Piscataway (1994)
4. Gauss, C.F.: Disquisitiones Arithmeticae (1801); English translation, Yale, New Haven (1966)
5. Chu, W., Colbourn, C.J.: Optimal frequency-hopping sequences via cyclotomy. IEEE Trans. Inf. Theory 51(3), 1139–1141 (2005)
6. Ding, C., Yin, J.: Sets of optimal frequency-hopping sequences. IEEE Trans. Inf. Theory 54(8), 3741–3745 (2008)
7. Han, Y.K., Yang, K.: On the Sidel'nikov sequences as frequency-hopping sequences. IEEE Trans. Inf. Theory 55(9), 4279–4285 (2009)
8. Chung, J.-H., Han, Y.K., Yang, K.: New classes of optimal frequency-hopping sequences by interleaving techniques. IEEE Trans. Inf. Theory 55(12), 5783–5791 (2009)
9. Chung, J.-H., Yang, K.: Optimal frequency-hopping sequences with new parameters. IEEE Trans. Inf. Theory 56(4), 1685–1693 (2010)
10. Storer, T.: Cylotomy and Difference Sets. Lectures in Advanced Mathematics. Markham, Chicago (1967)
11. Whiteman, A.L.: A family of difference sets. Illinois J. Math. 6, 107–121 (1962)
12. Ding, C., Helleseth, T.: New generalized cyclotomy and its applications. Finite Fields Their Appl. 4, 140–166 (1998)
13. Chung, J.-H., Yang, K.: k-fold cyclotomy and its application to frequency-hopping sequences (submitted for publication)
14. Peng, D., Fan, P.: Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences. IEEE Trans. Inf. Theory 50(9), 2149–2154 (2004)
15. Fan, P.Z., Darnell, M.: Sequence Design for Communications Applications. Research Studies Press (RSP). John Wiley & Sons, London (1996)
16. Lempel, A., Greenberger, H.: Families of sequences with optimal Hamming correlation properties. IEEE Trans. Inf. Theory 20(1), 90–94 (1974)
17. Gong, G.: Theory and applications of q-ary interleaved sequences. IEEE Trans. Inf. Theory 41(2), 400–411 (1995)

User-Irrepressible Sequences

Kenneth W. Shum, Yijin Zhang, and Wing Shing Wong

Department of Information Engineering,
the Chinese University of Hong Kong,
Shatin, Hong Kong
{wkshum,zyj007,wswong}@ie.cuhk.edu.hk

Abstract. Protocol sequences are binary and periodic sequences used in multiple-access scheme for collision channel without feedback. Each user reads out the bits from the assigned protocol sequence periodically, and sends a packet whenever the bit is equal to one. It is assumed that any two or more packets overlapping in time result in a collision, and the collided packets are unrecoverable. Due to the lack of feedback and cooperation, there are some relative delay offsets between protocol sequences. We consider protocol sequences with the property, called user-irrepressibility, that each user is guaranteed to send at least one packet in each sequence period without collision, no matter what the delay offsets are. The period length is hence a measure of delay; each user need to wait no more than a period time before a successful transmission can be made. Our objective is to construct user-irrepressible sequences with sequence period as short as possible. In this paper, we present a new construction for prime number of users. A lower bound on period which is applicable in general for any number of users is also derived.

Keywords: Protocol sequences, conflict-avoiding codes, collision channel without feedback.

1 Introduction

We consider packetized multiple-access transmission system in which time is divided into time slots, and assume slot synchronization. A user who wants to transmit a packet must send the packet within a time slot. If exactly one user transmits in a time slot, then the packet is received error-free. However, when two or more users send simultaneously in a time slot, we have a collision and the collided packets are assumed unrecoverable.

We assume that there is no communication among the transmitting nodes. The transmission scheme is thus fully distributed. Also, as argued in [5], information is transmitted via the content of the packets only, but not via the channel access times of the users. The decision of whether transmitting a packet or not in a time slot is independent of the data to be sent. Without loss of generality,

This work was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region under Project 417909.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 88–101, 2010.

the scheduling of packets is done by assigning each user a deterministic binary sequence, call protocol sequence. Each user reads out the bits from the assigned protocol sequence periodically, and sends a packet if and only if the value is equal to one. The users may start their communication at different times. Since we do not assume any feedback from the receiver and cooperation among the users, this incurs relative delay offsets between protocol sequences. We assume that the relative delay offsets of the protocol sequences are arbitrary but fixed throughout the transmission session.

Our design objective, called *user-irrepressibility* [11], is to guarantee in the worst case that each user is able to send at least one packet successfully to the sink node in each period. In other words, no mater what the relative delay offsets are, there is at least one successful packet for each user in each period. This can be re-phrased in terms of the sequence matrix as follow. Given M binary sequences of length L, we cyclically shift each of them and stack them together in an $M \times L$ matrix, one row for each sequence. The sequences are user-irrepressible if no matter what the cyclic shifts are, the resulting $M \times L$ matrix always contains an $M \times M$ identity matrix as a submatrix. The common period of a set of user-irrepressible sequences measures the maximum waiting time until a packet can be sent successfully. This bounded-delay requirement finds application in medical systems [7] and body sensor networks [13] for instance. Let $L_{\min}(M)$ be the smallest L such that a set of M user-irrepressible sequences of common period L exists. Previous work in [2] shows that $L_{\min}(M)$ is lower bounded by $1 + M(M+1)/2$.

The notion of user-irrepressibility is addressed in another context, under the name of *conflict-avoiding codes* (CAC) (see e.g. [4,6] and the references therein) with different perspective. In the study of CAC, there are T potential users, and at most M of them are active at the same time. Given the sequence period L, the objective in the construction of CAC is to maximize the number of potential users T, with the guarantee of at least one packet received successfully from each active user in a period time, provided that the number of active users is no more than M. In this paper, we consider the case where all users are active, and minimize the period for fixed number of users.

In this paper we assume slot synchronism. If frame synchronization, which is stronger than slot synchronization, is allowed, the problem has a trivial time-division multiple-access (TDMA) solution, namely, the sequence period is $L = M$ and the ith user sends a packet in the ith time slot. Collision can be totally avoided in this case. However, with slot synchronization, the relative delay offsets among sequences are nonzero and uncontrollable.

This paper is organized as follows. After setting up the notations in Section 2, we review some existing constructions of user-irrepressible sequences in Section 3. A new construction of user-irrepressible sequence is given in Section 4. A method for computing a lower bound for $L_{\min}(M)$ is presented in Section 5. The current status of our knowledge on $L_{\min}(M)$ is summarized at the end of this paper.

2 Notations and Preliminaries

We represent a periodic sequence with period L by a sequence of finite length L. We will use "period" and "length" interchangeably. The *Hamming weight* of a binary sequence $a(t)$, denoted by $w_H(a)$, is the number of 1's in a period. The *Hamming cross-correlation* between two sequences $a(t)$ and $b(t)$, denoted by $H_{ab}(\tau)$, is defined as

$$H_{ab}(\tau) := \sum_{t=0}^{L-1} a(t)b(t-\tau).$$

Let $\mathbb{Z}_L = \{0, 1, 2, \ldots, L-1\}$ denote the residues of integer modulo L. Given a binary sequence $s(t)$ of length L, we define the *characteristic set* of $s(t)$ by

$$\mathcal{I}_s := \{t \in \mathbb{Z}_L : s(t) = 1\}.$$

A cyclic shift of a sequence $s(t)$ by τ corresponds to a translation of $\mathcal{I}_s$ by τ in $\mathbb{Z}_L$. Given any subset $\mathcal{A}$ of $\mathbb{Z}_L$, we define the sum of $\mathcal{A}$ and an element x in $\mathbb{Z}_L$ by

$$\mathcal{A} + x := \{a + x \in \mathbb{Z}_L : a \in \mathcal{A}\}.$$

A cyclic shift of $s(t)$ by τ is thus represented by $\mathcal{I}_s + \tau$. The Hamming cross-correlation between two binary sequence s_1 and s_2, with delay offset τ, is equal to the cardinality of

$$\mathcal{I}_{s_1} \cap (\mathcal{I}_{s_2} + \tau).$$

Consider a collection of subsets $\mathscr{S} = \{\mathcal{I}_0, \mathcal{I}_1, \ldots, \mathcal{I}_{M-1}\}$ of $\mathbb{Z}_L$. This specifies a set of M binary sequences $\{s_0(t), s_1(t), \ldots, s_{M-1}(t)\}$ by letting the ith subset $\mathcal{I}_i$ in $\mathscr{S}$ be the characteristic set of $s_i(t)$. We say that $\mathcal{I}_i$ is *cyclically covered* by the other sets in $\mathscr{S}$ if we can find some integers τ_j, for $j \in \{1, 2, \ldots, M-1\} \setminus \{i\}$, such that

$$\mathcal{I}_i \subseteq \bigcup_{j \neq i} (\mathcal{I}_j + \tau_j)$$

The sequence $s_i(t)$ corresponding $\mathcal{I}_i$ is then said to be *blocked* by the other sequences. If there is a set in $\mathscr{S}$ which is cyclically covered by the others, or equivalently if there is a sequence which is blocked by the other sequences, we say that $\mathscr{S}$ is *user-repressible*. Otherwise, $\mathscr{S}$ is said to be *user-irrepressible* (UI). We use $\mathsf{UIS}(L, M)$ to denote a collection of M user-irrepressible subsets in $\mathbb{Z}_L$. We will abuse notation and use $\mathsf{UIS}(L, M)$ for the corresponding set of binary sequences as well.

UI sequences are related to another combinatorial structure called cover-free family [3]. A collection of sets $\mathscr{F}$ is called *r-cover-free* if $\mathcal{F}_0 \not\subset \mathcal{F}_1 \cup \mathcal{F}_2 \cup \ldots \cup \mathcal{F}_r$ for all $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_r \in \mathscr{F}$ ($\mathcal{F}_i \neq \mathcal{F}_j$ if $i \neq j$). A collection of M binary sequences is UI if for all possible choices of delay offsets τ_i, the translated characteristic sets $\mathcal{I}_i + \tau_i$, for $i = 0, 1, \ldots, M-1$, form an $(M-1)$-cover-free family.

As a "non-example", consider the following three sequences of length 7:

$$s_1(t) : 1110000$$
$$s_2(t) : 1010100$$
$$s_3(t) : 1001001$$

The first sequence $s_1(t)$ can be blocked by $s_2(t)$ and $s_3(t)$, because $\mathcal{I}_1 = \{0, 1, 2\}$ is contained in

$$\mathcal{I}_2 \cup (\mathcal{I}_3 + 1) = \{0, 1, 2, 4\}.$$

These three binary sequences are hence not UI.

A sequence set is said to be *constant-weight* if all sequences have the same Hamming weight. A constant-weight UI sequence set with Hamming weight w is denoted by $\mathsf{UIS}(L, M, w)$. Several existing constructions of constant-weight UI sequences are reviewed in the next section. A new construction of non-constant-weight UI sequences will be described in Section 4.

3 Known Constructions of UI Sequences

Shift-Invariant Sequences (SIS). Shift-invariant sequences are studied in [5] as an essential ingredient for achieving the capacity of the collision channel without feedback. This class of protocol sequences has the property that all Hamming cross-correlation functions of order two or higher are constant. From the construction of SIS, we obtain constant-weight $\mathsf{UIS}(2^M, M, 2^{M-1})$ for $M \geq 2$. For example, the following are three constant-weight UI sequences which are shift-invariant:

$$s_0(t) : 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0,$$
$$s_1(t) : 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0,$$
$$s_2(t) : 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0.$$

However, it is proved in [9] that the period of SIS increases exponentially as a function of the number of users. Shift-invariant sequences are of practical interests only when the small number of users is small.

Extended Prime Sequences (EPS). For prime p, a construction of constant-weight $\mathsf{UIS}(p(2p-1), p, p)$ is given in [12]. Let $[x \bmod p]$ denote the unique integer between 0 and $p-1$ such that

$$x = qp + [x \bmod p]$$

holds for some integer q. For $g = 1, 2, \ldots, p$, the gth extended prime sequence is defined by setting the characteristic set of the gth sequence to

$$\mathcal{I}_g = \{j(2p-1) + [gj \bmod p] : j = 0, 1, \ldots, p-1\}.$$

It can be shown that the Hamming cross-correlation between two distinct EPS is at most one. As the Hamming weight of each sequence is p, this implies that the extended prime sequences enjoy the UI property.

CRT Sequences. Given a positive integer M, let p be the smallest prime number which is larger than or equal to M. A constant-weight $\mathsf{UIS}(p(2M-1), M, M)$ can be constructed as follows. By Bertrand's postulate [1, Chapter 2], p can be chosen between M and $2M-2$, and hence p and $2M-1$ are relatively prime. We apply Chinese remainder theorem (CRT) and identify $\mathbb{Z}_{p(2M-1)}$ with the direct sum $\mathbb{Z}_p \oplus \mathbb{Z}_{2M-1}$; the bijection $\varphi : \mathbb{Z}_{p(2M-1)} \to \mathbb{Z}_p \oplus \mathbb{Z}_{2M-1}$ is given by

$$\varphi(x) := (x \bmod p, x \bmod 2M-1).$$

For $g = 1, 2, \ldots, p$, the gth sequence is defined by setting the corresponding characteristic set to

$$\mathcal{I}_g = \{t \in \mathbb{Z}_L : \varphi(t) = (jg \bmod p, j), j = 0, 1, \ldots, M-1\}.$$

It is shown in [10] that the Hamming cross-correlation between two distinct CRT sequences is at most one. This guarantees that the constructed sequences are UI.

4 A New Construction Based on CRT for Prime Number of Users

We present a variation of the CRT construction in this section. Even though the two constructions look similar, the proof of user-irrepressibility is very different. The new sequences are not constant-weight, and are shorter than the extended prime sequences with the same number of users.

Let p be an odd prime. Since p and $2p-2$ are relatively prime, by the Chinese remainder theorem, there is an isomorphism θ from $\mathbb{Z}_{p(2p-2)}$ to $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$, given by

$$\theta(t) := (t \bmod p, t \bmod 2p-2).$$

We will henceforth identify $\mathbb{Z}_{p(2p-2)}$ with $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. The new class of UI sequences is specified by the corresponding characteristic sets in $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. For $g = 0$, let

$$\mathcal{I}_0 = \{(i, 0) : i = 0, 1, \ldots, p-1\}, \tag{1}$$

and for $g = 1, \ldots, p-1$, let

$$\mathcal{I}_g = \{(gj \bmod p, j) : j = 0, 1, 2, \ldots, p\}. \tag{2}$$

This produces p sequences of length $p(2p-2)$. The first sequence is of weight p, and the remaining sequences are of weight $p+1$. We call this construction CRT_p, and distinguish it from the previous CRT construction by subscript "$_p$".

A cyclic shift of a sequence by τ corresponds to adding $\theta(\tau)$ to the corresponding characteristic set. We will use the notation

$$\mathcal{I}_g + (a, b) := \{(x, y) + (a, b) : (x, y) \in \mathcal{I}_g\},$$

with the addition carried out in $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. We note that the sets in (1) and (2) are arithmetic progressions in $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. For $(x, y) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$ and integers

$k_1 \leq k_2$, we will use $(x, y) \cdot [k_1, k_2]$ to represent an arithmetic progression with common difference (x, y),

$$\{(k_1 x, k_1 y), ((k_1 + 1)x, (k_1 + 1)y), \ldots, (k_2 x, k_2 y)\}.$$

In this notation, the characteristic sets in (1) and (2) are $(1, 0) \cdot [0, p - 1]$ and $(g, 1) \cdot [0, p]$.

Lemma 1. *For each* $(a, b) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$ *and* $h = 1, 2, \ldots, p-1$, $(1, 0) \cdot [0, p-1]$ *and* $(h, 1) \cdot [0, p] + (a, b)$ *contains at most one common element.*

Proof. If $(i, 0) = (hj + a, j + b)$, for some $i = 0, 1, \ldots, p - 1$ and $j = 0, 1, \ldots, p$, then by equating the second components, the value of j is uniquely determined by $j = -b \bmod 2p-2$. The value of i is then uniquely determined as well by equating the first components. This shows that if $(1, 0) \cdot [0, p]$ and $(h, 1) \cdot [0, p - 1] + (a, b)$ have nonempty intersection, the intersection contains exactly one element. □

Lemma 2. *For each* $(a, b) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$ *and distinct* g *and* h *in* $\{1, 2, \ldots, p-1\}$, $(g, 1) \cdot [0, p]$ *and* $(h, 1) \cdot [0, p] + (a, b)$ *contains at most two common elements.*

Proof. Suppose that there are two or more common elements in $(g, 1) \cdot [0, p]$ and $(h, 1) \cdot [0, p] + (a, b)$. Let A and B be two of them. We have

$$A = (gj_1, j_1) = (hj'_1 + a, j'_1 + b) \tag{3}$$
$$B = (gj_2, j_2) = (hj'_2 + a, j'_2 + b) \tag{4}$$

for some $j_1, j_2, j'_1, j'_2 \in \{0, 1, \ldots, p\}$, $j_1 \neq j_2$ and $j'_1 \neq j'_2$.

Let $\delta := j_2 - j_1$ and $\delta' := j'_2 - j'_1$. Both δ and δ' assume value in the following range

$$\{-p, -(p-1), \ldots, -2, -1\} \cup \{1, 2, \ldots, p-1, p\}. \tag{5}$$

By interchanging the values of j_1 and j_2 if necessary, we consider only $\delta \in \{1, 2, \ldots, p\}$ without loss of generality.

After subtracting (3) from (4) and equating the two components, we obtain the following system of modular equations

$$g\delta = h\delta' \bmod p, \tag{6}$$
$$\delta = \delta' \bmod 2p - 2. \tag{7}$$

For $\delta = 1, 2, \ldots, p-3$, (6) and (7) have no common solution. Indeed, the only δ' in the range of (5) which equals $\delta \bmod 2p - 2$ is $\delta' = \delta$, and from (6), we obtain $(g - h)\delta = 0 \bmod p$, which contradicts the assumption that $g \neq h$.

For $\delta = p - 2$, (6) and (7) also have no common solution. In this case, δ' is equal to either $p - 2$ and $-p$ by (7). The possibility of $\delta' = p - 2$ is forbidden because otherwise we would obtain the contradiction $g = h$ from (6). On the other hand, if $\delta' = -p$, we get $g(p - 2) = 0 \bmod p$ from (6), which implies that $g = 0 \bmod p$. Again, we arrive at a contradiction.

In the following, we consider the two remaining cases: $\delta = p$ and $\delta = p-1$.

(i) Suppose $\delta = p$. The value of δ' is equal to either p or $-(p-2)$ by (7). The latter is not feasible, because after substituting $\delta = p$ and $\delta' = -(p-2)$ into (6), we obtain

$$0 = -h(p-2) \bmod p,$$

which contradicts the assumption that h is nonzero. Hence, we must have $\delta' = \delta = p$. Since the range of j_1, j_2, j_1' and j_2' is $\{0, 1, \ldots, p\}$, we obtain $j_1 = j_1' = 0$, and $j_2 = j_2' = p$. By substituting $j_1 = j_1' = 0$ into (3), we thus get $a = b = 0$. This solution is tabulated in the first row of Table 1.

(ii) Suppose $\delta = p-1$. The values of δ' which satisfy (7) are $\pm(p-1)$. We cannot have $\delta' = p-1$, because it implies $g = h \bmod p$ by (6). The only choice of δ' is thus $\delta' = -(p-1)$. In this case, we have $\delta = -\delta'$ and $g = -h \bmod p$. Since $\delta = p-1$, the corresponding pairs of j_1 and j_2 are (a) $j_1 = 0$ and $j_2 = p-1$, and (b) $j_1 = 1$ and $j - 2 = p$. Likewise, since $\delta = -(p-1)$, the corresponding pairs of j_1' and j_2' are (a') $j_1' = p-1$ and $j_2' = 0$ and (b') $j_1' = p$ and $j_2' = 1$. The four different combinations are summarized in the last four rows of Table 1.

As h is between 1 and $p-1$, each pair of (a, b) in the last two columns of Table 1 are distinct. For fixed values of a and b, if $(gj, j) = (hj' + a, j' + b)$ has two solutions (j_1, j_1'), (j_2, j_2'), they must be associated with one of the rows in Table 1. Therefore, $(g, 1) \cdot [0, p]$ and $(h, 1) \cdot [0, p] + (a, b)$ contain exactly two common elements for precisely five different combinations of a and b listed in Table 1. This excludes the possibility of having three or more common elements. □

Table 1. Solutions to (3) and (4)

j_1	j_2	j_1'	j_2'	$a \bmod p$	$b \bmod 2p-2$
0	p	0	p	0	0
0	$p-1$	$p-1$	0	h	$p-1$
0	$p-1$	p	1	0	$p-2$
1	p	$p-1$	0	0	p
1	p	p	1	$-h$	$p-1$

Lemmas 1 and 2 show that the Hamming cross-correlation of two sequences from the CRT_p is either 0, 1 or 2. In fact, if $h = -g \bmod p$, the number of occurrences of 2 as a cross-correlation value is exactly five. For distinct h and g in $\{1, 2, \ldots, p-1\}$ such that $h \neq -g \bmod p$, only the first row in Table 1 is feasible, and the Hamming cross-correlation equals 2 when and only when the relative delay offset is zero.

Theorem 1. *For prime number p, the sequences from the CRT_p construction form a $\mathsf{UIS}(2p(p-1), p)$.*

Proof. Let $\mathcal{I}_i$, $i = 0, 1, \ldots, p-1$, be the characteristic set from the CRT_p construction, and τ_i be the relative delay offsets.

Consider the first sequence, which is represented by $\mathcal{I}_0$. By Lemma 1, $\mathcal{I}_0$ and $\mathcal{I}_h + \theta(\tau_h)$ have at most one common elements, for $h = 1, 2, \ldots, p-1$. Since $\mathcal{I}_0$ contains p elements and there are only $p-1$ other users, we can find an element in $\mathcal{I}_0$ which is not contained in $\bigcup_{h=1}^{p-1}(\mathcal{I}_h + \theta(\tau_h))$. Hence $\mathcal{I}_0$ cannot be cyclically covered no matter how the delay offsets are chosen.

Next, we show that for each $g \in \{1, 2, \ldots, p-1\}$, $\mathcal{I}_g$ cannot be cyclically covered by the others. Suppose without loss of generality that $\tau_g = 0$. Let $\bar{g}$ denote $-g \bmod p$. We have seen in the proof of Lemma 2 that $\mathcal{I}_{\bar{g}}$ is the only one whose translates can overlap $\mathcal{I}_g$ with intersection other than $(0,0)$ and $(0,p)$.

Let $\mathcal{J}$ denote $\mathcal{I}_g \cap (\mathcal{I}_{\bar{g}} + (\theta(\tau_{\bar{g}})))$. We consider two cases. (i) $|\mathcal{J}| = 0, 1$. Let

$$\mathscr{A} := \{h \in \{0, 1, \ldots, p-1\} \setminus \{g\} : \left|\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h))\right| = 2\},$$

and $\mathscr{B}$ be $\{0, 1, \ldots, p-1\} \setminus (\{g\} \cup \mathscr{A})$. In other words, $\mathscr{A}$ (resp. $\mathscr{B}$) corresponds to the set of sequences whose Hamming cross-correlation with s_g is equal to two (resp. one). By assumption, we have $\bar{g} \in \mathscr{B}$. For all $h \in \mathscr{A}$, we have

$$\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h)) = \{(0,0), (0,p)\}.$$

(the first row in Table 1). Then

$$\left|\mathcal{I}_g \cap \bigcup_{h \neq g} (\mathcal{I}_h + \theta(\tau_h))\right| \leq \left|\bigcup_{h \in \mathscr{A}} (\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h)))\right| + \left|\bigcup_{h \in \mathscr{B}} (\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h)))\right|.$$

If $\mathscr{A}$ is empty, then the first term on the right hand side is zero, and the second term is no more than $p-1$. If $\mathscr{A}$ is not empty, then the first term is equal to two, and the second term is no more than $p-2$. In any case, the sum on the right hand side does not exceed p. Since $|\mathcal{I}_g| = p+1$, we see that $\mathcal{I}_g$ is not contained in $\bigcup_{h \neq g}(\mathcal{I}_h + \theta(\tau_h))$.

(ii) $|\mathcal{J}| = 2$. In this case, $\mathcal{J}$ equals either $\{(0,0), ((p-1)g, p-1)\}$, or $\{(g,1), (0,p)\}$ (the last four rows in Table 1). For $h \notin \{g, \bar{g}\}$, we claim that

$$|(\mathcal{I}_g \setminus \mathcal{J}) \cap (\mathcal{I}_h + \theta(\tau_h))| \leq 1. \tag{8}$$

If $|\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h))| = 1$, then (8) follows immediately. Otherwise, if $\mathcal{I}_g$ and $\mathcal{I}_h + \theta(\tau_h)$ have two elements in common, then these two elements are $(0,0)$ and $(0,p)$ (the first row in Table 1). Either $(0,0)$ or $(0,p)$ is in common with $\mathcal{J}$. This implies

$$|(\mathcal{I}_g \setminus \mathcal{J}) \cap (\mathcal{I}_h + \theta(\tau_h))| = 1$$

and finishes the proof of the claim. Hence,

$$\left|\mathcal{I}_g \cap \bigcup_{h \neq g} (\mathcal{I}_h + \theta(\tau_h))\right| \leq |\mathcal{J}| + \left|\bigcup_{h \neq \{g, \bar{g}\}} (\mathcal{I}_g \setminus \mathcal{J}) \cap (\mathcal{I}_h + \theta(\tau_h))\right|.$$

As the second term on the right hand side is no more than $p-2$, we see that the sum is less than or equal to p. Since $|\mathcal{I}_g| = p+1$, this completes the proof that $\mathcal{I}_g$ cannot be cyclically covered. □

Example: Let $p = 7$. The CRT_p construction produces a set of seven UI sequences of period 84. The characteristic sets are:

$$\mathcal{I}_0 = \{0, 12, 24, 36, 48, 60, 72\}, \qquad \mathcal{I}_1 = \{0, 1, 2, 3, 4, 5, 6, 7\},$$
$$\mathcal{I}_2 = \{0, 7, 17, 27, 37, 54, 64, 74\}, \qquad \mathcal{I}_3 = \{0, 7, 18, 29, 40, 51, 62, 73\},$$
$$\mathcal{I}_4 = \{0, 7, 16, 25, 41, 50, 66, 75\}, \qquad \mathcal{I}_5 = \{0, 7, 15, 30, 38, 53, 61, 76\},$$
$$\mathcal{I}_6 = \{0, 7, 13, 26, 39, 52, 65, 78\}.$$

The period of UI sequences obtained by construction CRT_p is shorter than the period from EPS. The shortest known periods of UI sequences, for $M = 1, 2, \ldots, 12$, are shown in Table 2 in the next section.

Remark: We can generalize the construction in (2) by defining

$$\mathcal{I}_g := \{(gj \bmod p, fj \bmod q) : j = 0, 1, 2, \ldots, p\}$$

for some integer f which is relatively prime with q. It can be proved in a similar way that the resulting sequences are UI. The original construction is a special case with $f = 1$.

5 Lower Bound on Period

The property of user-irrepressibility can be interpreted as a two-person game. Player 1 writes down a set of M binary sequences of length L. Then Player 2 tries to adjust the delay offsets and block one of the sequences. If Player 2 succeeds in doing so, the binary sequences are not UI, otherwise, the Player 1 wins and the binary sequences are UI. In this section, we describe a greedy algorithm for Player 2, called *blocking algorithm*, and derive a sufficient condition under which Player 2 has a sure win, no matter what Player 1 writes down in the first place. Under this condition, one of the protocol sequence is blocked by the others, and hence the sequence set cannot be UI. This gives a lower bound on the period of UI sequences.

Blocking algorithm

Inputs: A set of M binary sequences of length L, $s_0(t)$, $s_1(t), \ldots, s_{M-1}(t)$.

(1) Re-label the sequences so that the Hamming weight of $s_0(t)$ is smallest among the M binary sequences. Set $k = 1$.

(2) Cyclically shift $s_k(t)$ so that the Hamming cross-correlation between $s_0(t)$ and $s_k(t)$ is maximal.

(3) Set the 1's in $s_0(t)$ which overlap with the shifted version of $s_k(t)$ to zero.

(4) If $k < M - 1$, increment k by one and go back to step (2).

If all of the 1's in $s_0(t)$ is removed after the termination of the blocking algorithm, then $s_0(t)$ is blocked and Player 2 wins.

Theorem 2. *Let $s_0(t), s_1(t), \ldots, s_{M-1}(t)$ be M binary sequences of length L. Suppose s_0 has the smallest Hamming weight, i.e., $w_H(s_0) = w$ and $w_H(s_i) \geq w$ for $i = 1, \ldots, M - 1$. Define an integer sequence $(r_k(w, L))_{k=0}^{\infty}$ recursively by*

$$r_0(w, L) := w \tag{9}$$

$$r_k(w, L) := r_{k-1}(w, L) - \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil, \quad \text{for } k \geq 1. \tag{10}$$

If $r_{M-1}(w, L) = 0$, then $s_0(t)$ is blocked by $s_1(t)$, $s_2(t), \ldots, s_{M-1}(t)$.

Proof. We will use the following fact: For two binary sequences $a(t)$ and $b(t)$ of period L and Hamming weight $w_H(a)$ and $w_H(b)$, we have

$$\sum_{\tau=0}^{L-1} H_{ab}(\tau) = w_H(a) w_H(b). \tag{11}$$

The proof of this fact is straightforward, and can be found in [8].

Let $x_0(t)$ be the sequence $s_0(t)$. We will recursively define $M-1$ sequences $x_1(t), x_2(t), \ldots, x_{M-1}(t)$, and prove by induction that $w_H(x_k) = r_k(w, L)$, for $k = 1, 2, \ldots, M-1$. The sequence $x_k(t)$ corresponds to what we get after step (3) in the blocking algorithm. Note that the Hamming weight of $x_0(t)$ is equal to $r_0(w, L) = w$. Because $w_H(x_0) = w$ and $w_H(s_1) \geq w$, from (11), we obtain

$$\frac{1}{L} \sum_{\tau=0}^{L-1} H_{x_0 s_1}(\tau) = \frac{w_H(x_0) w_H(s_1)}{L} \geq \frac{w^2}{L}.$$

The mean Hamming cross-correlation, averaged over all τ, is no less than w^2/L. We pick a delay offset for $s_1(t)$, say τ_1, so that $H_{x_0 s_1}(\tau_1) \geq \lceil w^2/L \rceil$, and define a binary sequence $x_1(t)$ by removing $\lceil w^2/L \rceil$ 1's from $x_0(t)$ which overlap with the 1's in the shifted version of $s_1(t)$. Here we slightly modify the blocking algorithm; in order to make the analysis more tractable, the number of 1's we take away from $x_0(t)$ is *exactly* $\lceil w^2/L \rceil$, instead of the maximal Hamming cross-correlation between $x_0(t)$ and $s_1(t)$. After the first step, we have $w_H(x_1) = w - \lceil w^2/L \rceil = r_1(w, L)$.

Given $x_{k-1}(t)$, we recursively define $x_k(t)$ in a similar fashion. In the kth step, we have

$$\frac{1}{L} \sum_{\tau=0}^{L-1} H_{x_{k-1} s_k}(\tau) = \frac{w_H(x_{k-1}) w_H(s_k)}{L} \geq \frac{r_{k-1}(w, L) \cdot w}{L}.$$

We can find a particular cyclic shift of $s_k(t)$ so that the Hamming cross-correlation between x_{k-1} and s_k is at least $\lceil \frac{w}{L} r_{k-1}(w, L) \rceil$. We remove exactly $\lceil \frac{w}{L} r_{k-1}(w, L) \rceil$ 1's in x_{k-1} which overlap with the shifted version of $s_k(t)$, and call the resulting sequence $x_k(t)$. Again, the total number of overlapping 1's may be more than $\lceil \frac{w}{L} r_{k-1}(w, L) \rceil$ but we only remove $\lceil \frac{w}{L} r_{k-1}(w, L) \rceil$ of them. After the kth step, we have $w_H(x_k) = r_k(w, L)$.

If $r_{M-1}(w, L)$ is zero, then there is no more 1 in $x_{M-1}(t)$. In this case, $s_0(t)$ is blocked by $s_1(t)$, $s_2(t), \ldots, s_{M-1}(t)$. □

We apply Theorem 2 several times, once for each $w \in \{1, 2, \ldots, L\}$. If $r_{M-1}(w, L)$ is zero for all $w = 1, 2, \ldots, L$, then for any M sequences of length L, the blocking algorithm can always succeed in blocking one of the sequences. We thus have the following necessary condition for the existence of UI sequences.

Theorem 3. *Let $r_k(w, L)$ be defined by (9) and (10). If $r_{M-1}(w, L) = 0$ for $w = 1, 2, \ldots, L$, and $L \leq L_0$, then $\mathsf{UIS}(L_0, M)$ does not exist, i.e., $L_{\min}(M)$ is strictly larger than L_0.*

As an example, we consider the case when $M = 3$. We tabulate $r_2(w, L)$ in the following table.

L	$r_2(1,L)$	$r_2(2,L)$	$r_2(3,L)$	$r_2(4,L)$	$r_2(5,L)$	$r_2(6,L)$	$r_2(7,L)$	$r_2(8,L)$
1	0							
2	0	0						
3	0	0	0					
⋮	⋮	⋮	⋮					
7	0	0	0	0	0	0	0	
8	0	0	0	1	0	0	0	0

The value of $r_2(w, L)$ is zero for all w when L is less than or equal to 7. The first non-zero entry occurs when $L = 8$ and $w = 4$, and $r_2(4, 8)$ is equal to one. By Theorem 3, we conclude that $L_{\min}(3) \geq 8$. In fact, a set of three UI sequences of length eight exists and is exhibited in Section 3. Therefore, $L_{\min}(3) = 8$. Furthermore, since $r_2(w, 8)$ is positive only when $w = 4$, the smallest Hamming weight in an $\mathsf{UIS}(8, 3)$ must be equal to four. The protocol sequences in the example in Section 3 indeed have Hamming weight equal to four.

We investigate the integer sequence $(r_k(w, L))_{k=0}^{\infty}$ defined in (9) and (10) in more details. We observe that for any fixed w and L, the value of $r_k(w, L)$ is monotonically decreasing as k increases, and stabilizes at 0 eventually. For instance, if $w \leq \sqrt{L}$, then $\lceil w r_k(w, L)/L \rceil = 1$ for $k = 0, 1, \ldots, w-1$. The integer sequence $(r_k(w, L))_{k=0}^{\infty}$ in this case is

$$w,\ w-1,\ w-2, \ldots, 3,\ 2,\ 1,\ 0,\ 0,\ \ldots.$$

Suppose that w is in the range $\sqrt{L} < w \leq \sqrt{2L}$. The decrease of Hamming weight after a step in the blocking algorithm is equal to two whenever

$$r_{k-1}(w, L) - r_k(w, L) = \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil = 2.$$

This happens when $1 < (w/L) \cdot r_{k-1}(w, L) \leq 2$. The integer sequence $(r_k(w, L))_{k=0}^{\infty}$ for $\sqrt{L} < w \leq \sqrt{2L}$ is

$$\underbrace{w,\ w-2,\ \ldots, n_1+2}_{n_2},\ \underbrace{n_1,\ n_1-1,\ \ldots,\ 1}_{n_1},\ 0, \ldots,$$

where n_1 and n_2 denote the number of terms with a step size of -1 and -2 respectively. We note that $n_1 + 2n_2 = w$.

In general, we have the following

Theorem 4. *Let $w \leq L$ be fixed integers, and α be $\lceil w^2/L \rceil$. Then*

$$r_{M-1}(w, L) > 0 \text{ implies } M \leq \frac{w}{\alpha} + \frac{L}{w} \sum_{i=2}^{\alpha} \frac{1}{i}.$$

Proof. In this proof, we simplify notation and write r_k instead of $r_k(w, L)$. For $i = 1, 2, \ldots, \alpha$, let n_i be number of integers r_k in $(r_k)_{k=0}^{\infty}$ such that $r_k - r_{k+1} = i$. The integers n_1, $n_2, \ldots, n_\alpha$ satisfy the relation

$$n_1 + 2n_2 + 3n_3 + \ldots + \alpha n_\alpha = w. \tag{12}$$

Now, consider the terms r_k in $(r_k)_{k=0}^{\infty}$ which satisfy $r_k - r_{k+1} = i$, i.e.,

$$r_k - r_{k+1} = \lceil wr_k/L \rceil = i.$$

We obtain from the last equality that $wr_k/L > i - 1$. Therefore, the r_k's which satisfy $r_k - r_{k+1} = i$ must lie in the range

$$(i-1)\frac{L}{w} < r_k \leq w - \sum_{j=i+1}^{\alpha} jn_j. \tag{13}$$

Furthermore, if r_{k_i} is the smallest r_k in $(r_k)_{j=0}^{\infty}$ such that $r_{k_i} - r_{k_i+1} = i$, then $r_{k_i-1} \leq (i-1)L/w < r_{k_i}$.

The range in (13) may be empty, in which case there is no r_k which satisfies $r_k - r_{k+1} = i$ and $n_i = 0$. If it is not empty, then

$$n_i \geq \frac{1}{i}\Big(\big(w - \sum_{j=i+1}^{\alpha} jn_j\big) - (i-1)\frac{L}{w}\Big),$$

since the difference between two adjacent r_k's in this range is precisely i. We simplify the above inequality to

$$(i-1)\frac{L}{w} + \sum_{j=i}^{\alpha} jn_j \geq w. \tag{14}$$

Inequality (14) is valid for $i = 1, 2, \ldots, \alpha$, and reduces to (12) when $i = 1$.

For $i = 2, 3, \ldots, \alpha$, divide both sides of (14) by $i(i-1)$, and add the resulting inequalities,

$$\sum_{i=2}^{\alpha} \frac{L}{iw} + \sum_{i=2}^{\alpha}\sum_{j=i}^{\alpha} \frac{jn_j}{i(i-1)} \geq \sum_{i=2}^{\alpha} \frac{w}{i(i-1)}. \tag{15}$$

After exchanging the order of the double summation, we can rewrite (15) as

$$\sum_{i=2}^{\alpha} \frac{L}{iw} + \sum_{j=2}^{\alpha} n_j(j-1) \geq w\Big(1 - \frac{1}{\alpha}\Big)$$

$$w - \sum_{j=2}^{\alpha} n_j(j-1) \leq \frac{w}{\alpha} + \frac{L}{w}\sum_{i=2}^{\alpha} \frac{1}{i}.$$

We replace w on the left hand side by $\sum_{j=1}^{\alpha} jn_j$, and obtain

$$\sum_{j=1}^{\alpha} n_j \leq \frac{w}{\alpha} + \frac{L}{w}\sum_{i=2}^{\alpha} \frac{1}{i}. \tag{16}$$

The theorem follows by noting that $M \leq \sum_{j=1}^{\alpha} n_j$. □

For positive integer n, let the nth harmonic number be denoted by $H_n := \sum_{i=1}^{n} 1/i$, and let $F : \mathbb{R}_+ \to \mathbb{R}_+$ be a function defined as

$$F(x) := \frac{x}{k} + \frac{H_k - 1}{x} \quad \text{for } \sqrt{k-1} < x \le \sqrt{k},\ k = 1, 2, 3, \ldots.$$

Although $F(x)$ is defined in a piece-wise manner, it can be shown that $F(x)$ is a continuous function, i.e., it is continuous at $x = \sqrt{k}$ for $k = 1, 2, 3, \ldots$

In terms of $F(x)$, Theorem 4 can be re-phrased as

$$r_{M-1}(w, L) > 0 \text{ implies } M \le \sqrt{L} F(w/\sqrt{L}).$$

Indeed, as $\alpha - 1 < w^2/L \le \alpha$, the right hand side of (16) can be written as

$$\sqrt{L}\Big(\frac{w}{\sqrt{L}\alpha} + \frac{\sqrt{L}}{w}\sum_{i=2}^{\alpha}\frac{1}{i}\Big) = \sqrt{L}\Big(\frac{w}{\sqrt{L}\alpha} + \frac{\sqrt{L}}{w}(H_\alpha - 1)\Big) = \sqrt{L} \cdot F(w/\sqrt{L}).$$

One can show by calculus that the function $F(x)$ attains global maximum at $x = \sqrt{2}$, with maximal value $F(\sqrt{2}) = 3/\sqrt{8}$. If a $\mathsf{UIS}(L, M)$ exists, then from Theorem 2 we know that $r_{M-1}(w, L)$ is positive for some w, and from Theorem 4, we have $M \le \sqrt{L} F(w/\sqrt{L}) \le \sqrt{L}(3/\sqrt{8})$. We have thus proved the following

Theorem 5. $L_{\min}(M) \ge \lceil 8M^2/9 \rceil$.

Theorem 5 improves upon the previous lower bound $1 + M(M-1)/2$ from [10].

The calculations as described in Theorem 3 have been automated by a computer program, and the resulting lower bounds on the period of UI sequences for $M = 2, 3, \ldots, 13$ are tabulated in the third column in Table 2. The value of $\lceil 8M^2/9 \rceil$ is shown in the second column. We can observe that the lower bounds obtained by Theorem 3 coincide with those by Theorem 5 very often. In fact, one can show by a more detailed analysis that the two lower bounds yield the same value when M is a multiple of 3. In the last column in Table 2, we list the shortest known period of UI sequences. The known periods in the first five entries come from the class of shift-invariant sequences. For seven or more users, CRT and CRT_p give the shortest known period.

Table 2. Lower bound on the minimum period of user-irrepressible sequences and periods of known user-irrepressible sequences. (It can be proved that there is no $\mathsf{UIS}(15, 4)$ by a separate argument and thus $L_{\min}(4) = 16$).

M	$\lceil 8M^2/9 \rceil$	$L_{\min}(M)$	Known period
2	4	4	4 (SIS)
3	8	8	8 (SIS)
4	15	≥ 15	16 (SIS)
5	23	≥ 24	32 (SIS)
6	32	≥ 32	64 (SIS)
7	44	≥ 44	84 (CRT_p)
8	57	≥ 60	165 (CRT)
9	72	≥ 72	187 (CRT)
10	89	≥ 90	209 (CRT)
11	108	≥ 108	220 (CRT_p)
12	128	≥ 128	299 (CRT)
13	151	≥ 152	312 (CRT_p)

6 Conclusion

A new construction of UI sequences when the number of users is a prime integer is devised. The sequence length of the new construction increases asymptotically like $2M^2$. Also, a lower bound of $8M^2/9$ is proved in this paper. Closing the gap between the upper and lower bound for $L_{\min}(M)$ is an interesting direction for future work.

References

1. Aigner, M., Ziegler, G.M.: Proofs from THE BOOK, 3rd edn. Springer, New York (2004)
2. Chen, C.S., Shum, K.W., Sung, C.W., Wong, W.S., Øien, G.E.: User unsuppressible protocol sequences for collision channel without feedback. In: Proc. IEEE Int. Symp. Inform. Theory and its Applications, Auckland, pp. 1213–1218 (December 2008)
3. Erdős, P., Frankl, P., Füredi, Z.: Family of finite sets in which no set is covered by the union of r others. Israel J. of Math. 51(1-2), 79–89 (1985)
4. Jimbo, M., Mishima, M., Janiszewski, S., Teymorian, A.Y., Tonchev, V.D.: On conflict-avoiding codes of length $n = 4m$ for three active users. IEEE Trans. Inform. Theory 53, 2732–2742 (2007)
5. Massey, J.L., Mathys, P.: The collision channel without feedback. IEEE Trans. Inform. Theory 31(2), 192–204 (1985)
6. Momihara, K., Müller, M., Satoh, J., Jimbo, M.: Constant weight conflict-avoiding codes. SIAM J. Discrete Math. 21(4), 959–979 (2007)
7. Roedig, U., Barroso, A., Sreenan, C.J.: f-MAC: A deterministic media access control protocol without time synchronization. In: Römer, K., Karl, H., Mattern, F. (eds.) EWSN 2006. LNCS, vol. 3868, pp. 276–291. Springer, Heidelberg (2006)
8. Sarwate, D.V., Pursley, M.B.: Crosscorrelation properties of pseudorandom and related sequences. Proc. IEEE 68(5), 593–619 (1980)
9. Shum, K.W., Chen, C.S., Sung, C.W., Wong, W.S.: Shift-invariant protocol sequences for the collision channel without feedback. IEEE Trans. Inform. Theory 55, 3312–3322 (2009)
10. Shum, K.W., Wong, W.S., Sung, C.W., Chen, C.S.: Design and construction of protocol sequences: Shift invariance and user irrepressibility. In: IEEE Int. Symp. Inform. Theory, Seoul, pp. 1368–1372 (June 2009)
11. Wong, W.S.: New protocol sequences for random access channels without feedback. IEEE Trans. Inform. Theory 53(6), 2060–2071 (2007)
12. Yang, G.C., Kwong, W.C.: Performance analysis of optical CDMA with prime codes. IEE Electron. Lett. 31(7), 569–570 (1995)
13. Yang, G.Z. (ed.): Body Sensor Networks. Springer, London (2006)

New Optimal Variable-Weight Optical Orthogonal Codes

Dianhua Wu*, Jiayun Cao, and Pingzhi Fan**

Keylab of Information Coding and Transmission,
Lab of Traffic Information Engineering and Control,
Southwest Jiaotong University,
Chengdu, 610031, China
dhwu@gxnu.edu.cn, p.fan@ieee.org

Abstract. Let W, L, and Q denote the sets $\{w_0, w_1, \ldots, w_p\}$, $\{\lambda_a^0, \lambda_a^1, \ldots, \lambda_a^p\}$ and $\{q_0, q_1, \ldots, q_p\}$, respectively. An (n, W, L, λ_c, Q) variable-weight optical orthogonal code C, or (n, W, L, λ_c, Q)-OOC, is a collection of binary n-tuples such that for each $0 \leq i \leq p$, there are exactly $q_i|C|$ codewords of weight w_i, L is related to periodic auto-correlation, and λ_c is related to periodic cross-correlation. The notation (n, W, λ, Q)-OOC is used to denote an (n, W, L, λ_c, Q)-OOC with the property that $\lambda_a^0 = \lambda_a^1 = \ldots = \lambda_a^p = \lambda_c = \lambda$. An (n, W, L, λ_c, Q)-OOCs was introduced by Yang for multimedia optical CDMA systems with multiple quality of service (QoS) requirements. A cyclic $(v, K, 1)$ difference family (cyclic (v, K, λ)-DF in short) is a family $\mathcal{F} = \{B_1, B_2, \ldots, B_t\}$ of t subsets of Z_v, the residue ring of integers modulo v, $K = \{|B_i| : 1 \leq i \leq t\}$, such that the differences in $\mathcal{F}$, $\Delta\mathcal{F} = \bigcup_{B \in \mathcal{F}} \Delta B$ cover each nonzero element of Z_v exactly λ times, where for each $B \in \mathcal{F}$, $\Delta B = \{x - y : x, y \in B, x \neq y\}$, and $|dev\ B_i| = v$, $1 \leq i \leq t$, $dev\ B_i = \{B_i + g : g \in Z_v\}$. A cyclic $(v, W, 1, Q)$-DF is defined to be a cyclic $(v, W, 1)$-DF with the property that the fraction of number of blocks of size w_i is q_i, $0 \leq i \leq p$. In this paper, constructions for cyclic $(v, \{4, 6, 7\}, 1, \{1/3, 1/3, 1/3\})$-DFs for primes $v \equiv 1 \pmod{84}$, $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DFs for primes $v \equiv 1 \pmod{u(u-1)+12}$, $u \equiv 0, 1 \pmod 3 > 4$ are presented. New optimal $(v, W, 1, Q)$-OOCs for $2 \leq |W| \leq 4$ are then obtained.

Keywords: cyclic difference family, difference family, optical orthogonal code, variable-weight OOC.

1 Introduction

Optical orthogonal codes (OOCs) were introduced by Salehi, as signature sequences to facilitate multiple access in optical fibre networks [1,2]. OOCs have

* The work was supported in part by NSFC (No. 10961006) and Guangxi Science Foundation (No. 0991089). Dianhua Wu is also with the Department of Mathematics, Guangxi Normal University, 541004, Guilin, China.

** The work was partially supported by NSFC (No. 60772087), the 863 High-Tech Program (No. 2009AA01Z238), the 111 project (No.111-2-14) and the Sino-Swedish Int. Cooperation Program (No.2008DFA12160).

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 102–112, 2010.

been found in a wide range of applications such as mobile radio, frequency-hopping spread-spectrum communications, radar, sonar, collision channel without feedback and neuromorphic network [3,7].

Most existing works on OOC's have assumed that all codewords have the same weight, see [8,23] for the examples. In general, the code size of OOCs depends upon the weights of codewords. The variable-weight OOCs can generate larger code size than that of constant-weight OOCs [24]. In 1996, Yang introduced a multimedia optical CDMA communication system employing variable-weight OOCs [25]. The multi-weight property of the OOCs enables the system to meet multiple QoS (Quality of Services) requirements. Variable-weight OOCs have attracted much attention recently [24,27].

Based on the notation of [25], throughout this paper, let W, L, and Q denote the sets $\{w_0, w_1, \ldots, w_p\}$, $\{\lambda_a^0, \lambda_a^1, \ldots, \lambda_a^p\}$ and $\{q_0, q_1, \ldots, q_p\}$, respectively as defined below.

An (n, W, L, λ_c, Q) variable-weight optical orthogonal code C, or (n, W, L, λ_c, Q)-OOC, is a collection of binary n-tuples such that the following three properties hold:

- *Weight Distribution:* Every n-tuple in C has a Hamming weight contained in the set W; furthermore, there are exactly $q_i|C|$ codewords of weight w_i, i.e., q_i indicates the fraction of codewords of weight w_i. It is clear that $\sum_{i=0}^{p} q_i = 1$.
- *Periodic Auto-correlation:* For any $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in C$ with Hamming weight $w_i \in W$, and any integer τ, $0 < \tau < n$,

$$\sum_{t=0}^{n-1} x_t x_{t\oplus\tau} \leq \lambda_a^i,$$

  where the summation is carried out by treating binary symbols as reals.
- *Periodic Cross-correlation:* Similarly, for $\mathbf{x} \neq \mathbf{y}$, $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in C$, $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in C$, and any integer τ,

$$\sum_{t=0}^{n-1} x_t y_{t\oplus\tau} \leq \lambda_c.$$

In [27], the notation (n, W, λ, Q)- OOC is used to denote an (n, W, L, λ_c, Q)-OOC with the property that $\lambda_a^0 = \lambda_a^1 = \ldots = \lambda_a^p = \lambda_c = \lambda$. The term variable-weight optical orthogonal code, or variable-weight OOC, is also used if there is no need to list the parameters.

For each $q_i \in Q$, without loss of generality, write $q_i = b_i/a_i$, where a_i, b_i are integers and $\gcd(a_i, b_i) = 1$, $0 \leq i \leq p$. Let $f(Q)$ be the least common multiple of $a_0, a_1, \ldots, a_p$, $f_i(Q) = f(Q)q_i$, then $q_i = f_i(Q)/f(Q)$, and $\sum_{i=0}^{p} f_i(Q) = f(Q)$. It is clear that $f_i(Q)$, $0 \leq i \leq p$, and w are integers. In the sequel, we use the notation $w = \sum_{i=0}^{p} f_i(Q)w_i(w_i - 1)$. We will also use the notation $a_i, b_i, f_i(Q)$, $0 \leq i \leq p$, and $f(Q)$ as defined above.

The work of Yang [25] contains lower and upper bounds on the size of variable-weight OOCs to judge the goodness of the constructions. Here we provide only an upper bound on the size of variable-weight OOCs given in [25].

Lemma 1. *Let* $\lambda_a^i \geq \lambda$, $0 \leq i \leq p$. *Then*

$$\Phi(v, W, L, \lambda, Q) \leq \left\lfloor \frac{(v-1)(v-2)\cdots(v-\lambda)}{\sum_{i=0}^{p} q_i w_i (w_i-1)(w_i-2)\cdots(w_i-\lambda)/(\lambda_a^i)} \right\rfloor,$$

where $\Phi(v, W, L, \lambda, Q)$=max$\{|C| : C$ *is a* (v, W, L, λ, Q)-OOC$\}$.

A (v, W, L, λ, Q)-OOC with cardinality $\Phi(v, W, L, \lambda, Q)$ is said to be *optimal*.

Let $\Phi(v, W, \lambda, Q)$=max$\{|C| : C$ is a (v, W, λ, Q)-OOC$\}$, the following result is clear from Lemma 1.

Lemma 2. $\Phi(v, W, \lambda, Q) \leq \left\lfloor \frac{\lambda(v-1)(v-2)\cdots(v-\lambda)}{\sum_{i=0}^{p} q_i w_i (w_i-1)(w_i-2)\cdots(w_i-\lambda)} \right\rfloor.$

Optimal optical orthogonal codes are closely related to some combinatorial configurations. For example, Yin [23] showed that an optimal $(v, k, 1)$-OOC, i. e. optical orthogonal codes with length v, and constant weight k for each codeword, is equivalent to an optimal cyclic packing CP$(k, 1; v)$. In this paper, we will use cyclic difference families to construct optimal variable-weight OOCs.

A (v, K, λ) *pairwise balanced design* (PBD) is a pair $(V, \mathcal{B})$, where V is a v-set whose elements are called *points* and $\mathcal{B}$ is a family of subsets of V (*blocks*) with sizes from K such that any 2-subset of V is contained in exactly λ blocks. A (v, K, λ)-PBD where $K = \{k\}$ is a singleton is a *balanced block design* and is denoted by (v, k, λ)-BIBD.

Suppose that $B = \{b_1, b_2, \ldots, b_k\}$ is a subset of Z_v, the residue ring of integers modulo v, define $\Delta B = \{x-y : x, y \in B, x \neq y\}$, $dev\ B = \{B+i : i \in Z_v\}$, where $B+i = \{b_1+i, b_2+i, \ldots, b_k+i\} \subseteq Z_v$. A cyclic $(v, K, 1)$ difference family (cyclic (v, K, λ)-DF in short) is a family $\mathcal{F} = \{B_1, B_2, \ldots, B_t\}$ of t subsets (*base blocks*) of Z_v, $K = \{|B_i| : 1 \leq i \leq t\}$, such that the differences in $\mathcal{F}$, $\Delta\mathcal{F} = \bigcup_{B \in \mathcal{F}} \Delta B$ cover each nonzero element of Z_v exactly λ times, and $|dev\ B_i| = v$, $1 \leq i \leq t$. If $K = \{k\}$, we will omit the braces. A cyclic $(v, W, 1, Q)$-DF is defined to be a cyclic $(v, W, 1)$-DF with the property that the fraction of number of blocks of size w_i is q_i, $0 \leq i \leq p$.

A number of constant-weight OOCs had been constructed from $(v, k, 1)$-DFs. There are some results on the existence of cyclic $(v, K, 1)$-DFs for $K = \{3, 4\}$ and $\{3, 6\}$ (see [28,30]).

Given a cyclic $(v, W, 1, Q)$-DF, one can construct a $(0, 1)$-sequence of length v, and weight w_i from a base block of size w_i whose nonzero bit positions are exactly indexed by the base block. The following result was stated in [27].

Lemma 3. *If there exists a cyclic* $(v, W, 1, Q)$*-DF, then there exists an optimal* $(v, W, 1, Q)$-OOC.

For a cyclic $(v, W, 1, Q)$-DF, $\mathcal{F}$, suppose that $|\mathcal{F}| = s$, then the number of blocks of size w_i is sb_i/a_i. Since $\gcd(a_i, b_i) = 1$, then $a_i|s$, $0 \le i \le p$, and hence $f(Q)|s$.

Lemma 4. *A necessary condition for the existence of a cyclic $(v, W, 1, Q)$-DF is $v \equiv 1 \pmod{w}$, where $w = \sum_{i=0}^{p} f_i(Q)w_i(w_i - 1)$.*

Proof. Suppose $\mathcal{F}$ is a cyclic $(v, W, 1, Q)$-DF, and $|\mathcal{F}| = s$, then

$$v - 1 = \sum_{i=0}^{p} \frac{sf(Q_i)}{f(Q)} w_i(w_i - 1) = w\frac{s}{f(Q)}.$$

Since $f(Q)|s$, then the conclusion is true. □

In [25], Yang gave an upper and lower bounds on the size of variable-weight OOCs. Some constructions for variable-weight OOCs were presented, some of them are optimal. In [24], Gu and Wu had constructed variable-weight OOCs by using pairwise balanced designs (PBDs) and packing designs with a partition. In [27], some optimal $(v, W, 1, Q)$-OOCs were obtained. To the authors knowledge, little is known for the existences of optimal $(v, W, 1, Q)$-OOCs for $W = \{4, 6\}$, $\{4, 7\}$, $\{3, 4, 6\}$, $\{3, 4, 7\}$ and $\{3, 4, 6, 7\}$.

In this paper, the following results are obtained.

Theorem 1. *For each prime $v = 42t + 1 \le 5000$, and $v > 43$, there exists a cyclic $(v, \{4, 6\}, 1, \{1/2, 1/2\})$-DF. There does not exist a cyclic $(43, \{4, 6\}, 1, \{1/2, 1/2\})$-DF.*

Theorem 2. *For each prime $v = 54t + 1 \le 5000$, and $v > 55$, there exists a cyclic $(v, \{4, 7\}, 1, \{1/2, 1/2\})$-DF.*

Theorem 3. *For each prime $v = 84t + 1 \le 5000$, and $v > 85$, there exists a cyclic $(v, \{4, 6, 7\}, 1, \{1/3, 1/3, 1/3\})$-DF.*

By using these cyclic difference families, new optimal $(v, W, 1, Q)$-OOCs for $2 \le |W| \le 4$ are obtained in the last section.

The following are some notations that will be used in this paper. Fix a prime $q \equiv 1 \pmod{n}$ and a primitive element $\theta \in GF(q)$, H^n will denote the multiplicative subgroup $\{\theta^{in} : 0 \le i \le \frac{q-1}{n} - 1\}$ of the nth powers modulo q, while C_j^n denote the coset of H^n in $\mathrm{GF}(q)^*(= H^1)$ represented by θ^j, i. e., $C_j^n = \theta^j C_0^n$, $0 \le j \le n-1$. A set of distinct representatives of cosets of $C_0^n (= H^n)$ is denoted by an SDRC.

For given sets A, B defined on $\mathrm{GF}(q)$, set $A \circ B = \{ab | a \in A, b \in B\}$.

2 Cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DFs for $u \equiv 0 \pmod 3$

Theorem 4. *Let $u = 3k \ge 6$ be a fixed positive integer, $v = (u(u-1)+12)t+1$ a prime, $e = \frac{k(3k-1)}{2} + 2$, θ a primitive element of $GF(v)$, ξ a primitive 3rd root of unity in $GF(v)$. Let $c_0 = 1$. If there exist elements c_i, $1 \le i \le k$, such that*

$S = \{c_i(\xi - 1) : 0 \le i \le k\} \bigcup \{c_h - c_l, c_h - c_l\xi, c_h - c_l\xi^2 : 0 \le l < h \le k-1\} \bigcup \{c_k\}$
forms an SDRC of H^e*, then there exists a cyclic* $(v, \{4, u\}, 1, \{1/2, 1/2\})$*-DF.*

Proof. Let $A_1 = \{1, \xi, \xi^2, c_1, c_1\xi, c_1\xi^2, \ldots, c_{k-1}, c_{k-1}\xi, c_{k-1}\xi^2\}$,
$A_2 = \{0, c_k, c_k\xi, c_k\xi^2\}$.

Since ξ is a primitive 3rd root of unity in GF(v), then $\xi^2 - 1 = \xi^2 - \xi^3 = -\xi^2(\xi - 1)$. It is not difficult to see that $\Delta A_1 \bigcup \Delta A_2 = (S \bigcup (-S)) \circ \{1, \xi, \xi^2\}$.

Let $\mathcal{F} = \{A_i\theta^{ej} : 1 \le j \le t, i = 1, 2\}$. If the conditions are satisfied, then it is not difficult to check that $\Delta\mathcal{F} = GF(v)^*$, and hence $\mathcal{F}$ forms a cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DF. This completes the proof. □

Remark 1. The similar method was used to construct $(v, k, 1)$-DFs for $k \in \{6, 7, 9\}$, and $(v, 9, 2)$-DFs (see [31]).
Applying Theorem 4 with $k = 2$, one can obtain the following result.

Corollary 1. *Let* $v = 42t+1$ *be a prime,* $e = 7$*,* θ *a primitive element of* $GF(v)$*,* ξ *a primitive* 3*rd root of unity in* $GF(v)$*. Let* $c_0 = 1$*. If there exist elements* c_i*,* $1 \le i \le 2$*, such that*
$S = \{c_i(\xi - 1) : 0 \le i \le 2\} \bigcup \{c_1 - 1, c_1 - \xi, c_1 - \xi^2\} \bigcup \{c_2\}$
forms an SDRC of H^7*, then there exists a cyclic* $(v, \{4, 6\}, 1, \{1/2, 1/2\})$*-DF.*

Example 1. A cyclic $(337, \{4, 6\}, 1, \{1/2, 1/2\})$-DF. Let $v = 337$, $\theta = 10$ a primitive element of GF(337), then $\xi = \theta^{112} = 128$, $\xi^2 = 208$. Let $c_1 = 33$, $c_2 = 15$, then c_1, c_2 satisfying the condition in Corollary 1,
$A_1 = \{1, 128, 208, c_1, 128c_1, 208c_1\} = \{1, 128, 208, 33, 180, 124\}$,
$A_2 = \{0, c_2, 128c_2, 208c_2\} = \{0, 15, 235, 87\}$
$\mathcal{F}_{337} = \{\theta^{7j}A_i : \ i = 1, 2, 1 \le j \le 8\}$
$= \{\{199, 197, 278, 164, 98, 75\}, \{172, 111, 54, 284, 293, 97\}, \{0, 250, 322, 102\}$
$\{191, 184, 299, 237, 6, 94\}, \{265, 220, 189, 320, 183, 171\}, \{0, 301, 110, 163\}$,
$\{163, 307, 204, 324, 21, 329\}, \{85, 96, 156, 109, 135, 93\}, \{0, 264, 92, 318\}$,
$\{65, 232, 40, 123, 242, 309\}, \{129, 336, 209, 213, 304, 157\}, \{0, 289, 259, 126\}$
$\{0, 221, 317, 136\}, \{0, 169, 64, 104\}, \{0, 268, 267, 139\}, \{0, 86, 224, 27\}\}$.
It is not difficult to check that $\mathcal{F}_{337}$ forms a cyclic $(337, \{4, 6\}, 1, \{1/2, 1/2\})$-DF.

Let $R = \{r : r \equiv 1 \pmod{42}$ is a prime, $43 \le r \le 5000\}$, $R_1 = \{43, 127, 211, 757, 883, 1597\}$. The following result is obtained.

Lemma 5. *For each* $v \in R \setminus R_1$*, there exists a cyclic* $(v, \{4, 6\}, 1, \{1/2, 1/2\})$*-DF.*

Proof. For each $v \in R \setminus R_1$, with the aid of a computer, one can find elements c_1, c_2 satisfying the conditions in Corollary 1. We list (v, θ, c_1, c_2) in Appendix A. This completes the proof. □

The following result was stated in [28].

Lemma 6. *Let* $k_1, k_2, \ldots, k_r$ *be positive integers such that* $\lambda(q-1) \equiv 0 \bmod m$*, where* $m = (1/2\lambda)\sum_{h=1}^{r} k_h(k_h - 1)$ *is also an integer. Let* $q \equiv 1 \pmod{m}$ *be an*

odd prime power, θ a primitive element of GF(q) and $A_h = \{a_{h,1}, a_{h,2}, \ldots, a_{h,k_h}\}$ be a k_h-subset of GF(q), $h = 1, \ldots, r$. Let

$$\mathcal{F} = (A_h \theta^{mi} | 1 \le h \le r, 0 \le i \le \frac{q-1}{2m}).$$

If the list $L = (a_{h,j} - a_{h,i} | 1 \le h \le r, 1 \le i < j \le k_h)$ is evenly distributed over H^m, then, $\mathcal{F}$is a $(q, K, \lambda, \{1/r, 1/r, \ldots, 1/r\})$-DF, where $K = \{k_1, k_2, \ldots, k_r\}$.

Applying Lemma 6 with $q = v$, $h = 2$, $k_1 = u$, $k_2 = 4$, $m = \frac{u(u-1)}{2} + 6$, we have $\lambda = 1$, the following result is obtained.

Lemma 7. *Suppose $v = (u(u-1)+12)t+1$ is a prime, $u \equiv 0,\ 1 \pmod 3 \ge 6$ is an integer, $m = \frac{u(u-1)}{2} + 6$, θ is a primitive element of GF(q). Let*

$A_v^{(1)} = \{x_1, x_2, \ldots, x_u\}$, $A_v^{(2)} = \{y_1, y_2, y_3, y_4\}$.

If $\{x_j - x_i : 1 \le i < j \le u\} \bigcup \{y_j - y_i : 1 \le i < j \le 4\}$ forms an SDRC of H^m, then there exists a cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DF.

Remark 2. To use Lemma 7 construct $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DFs for $u \equiv 0 \pmod 3$, one may assume $x_1 = 0, x_2 = 1$. In this case, one needs to find $u + 2$ elements, and compute $d = \frac{u(u-1)}{2} + 6$ differences. However, when Theorem 4 is used, one needs only to find $u/3$ elements, and compute $d/3$ differences. The case of $u \equiv 1 \pmod 3$ is similar. This fact shows the powerful of Theorem 4.

Lemma 8. *For each $v \in R_1 \setminus \{43\}$, there exists a cyclic $(v, \{4, 6\}, 1, \{1/2, 1/2\})$-DF.*

Proof. For each $v \in R_1 \setminus \{43\}$, with the aid of a computer, $A_v^{(i)}$, $i = 1, 2$ had been found, we list $A_v^{(i)}, \theta$, $i = 1, 2$ as follows. This completes the proof.

$A_{127}^{(1)} = \{0, 1, 3, 8, 29, 45\}$, $A_{127}^{(2)} = \{0, 4, 35, 58\}$, $\theta = 3$,
$A_{211}^{(1)} = \{0, 1, 4, 11, 35, 109\}$, $A_{211}^{(2)} = \{0, 8, 30, 129\}$, $\theta = 2$,
$A_{757}^{(1)} = \{0, 1, 5, 11, 25, 125\}$, $A_{757}^{(2)} = \{0, 16, 102, 221\}$, $\theta = 2$,
$A_{883}^{(1)} = \{0, 1, 3, 7, 18, 139\}$, $A_{883}^{(2)} = \{0, 13, 101, 264\}$, $\theta = 2$,
$A_{1597}^{(1)} = \{0, 1, 5, 11, 24, 156\}$, $A_{1597}^{(2)} = \{0, 14, 70, 748\}$, $\theta = 11$. □

We are now in a position to prove Theorem 1.

Proof of Theorem 1. For $q \ne 43$, the result comes from Lemma 5 and Lemma 8. For $q = 43$, by exhausted computer searching, there does not exist a cyclic $(43, \{4, 6\}, 1, \{1/2, 1/2\})$-DF. This completes the proof. □

3 Cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DFs for $u \equiv 1 \pmod 3$

Theorem 5. *Let $u = 3k+1 \ge 7$ be a fixed positive integer, $v = (u(u-1)+12)t+1$ a prime, $e = \frac{k(3k+1)}{2} + 2$, θ a primitive element of GF(v), ξ a primitive 3rd root of unity in GF(v). Let $c_0 = 1$. If there exist elements c_i, $1 \le i \le k$, such that*

$S = \{c_i(\xi - 1) : 0 \le i \le k\} \bigcup \{c_h - c_l, c_h - c_l\xi, c_h - c_l\xi^2 : 0 \le l < h \le k-1\} \bigcup \{c_i : 0 \le i \le k\}$

forms an SDRC of H^e, then there exists a cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DF.

Proof. Let $A_1 = \{0, 1, \xi, \xi^2, c_1, c_1\xi, c_1\xi^2, \ldots, c_{k-1}, c_{k-1}\xi, c_{k-1}\xi^2\}$,
$A_2 = \{0, c_k, c_k\xi, c_k\xi^2\}$.

Since ξ is a primitive 3rd root of unity in GF(v), then $\xi^2 - 1 = \xi^2 - \xi^3 = -\xi^2(\xi - 1)$. It is not difficult to see that $\Delta A_1 \bigcup \Delta A_2 = (S \bigcup (-S)) \circ \{1, \xi, \xi^2\}$.

Let $\mathcal{F} = \{A_i\theta^{ej} : 1 \le j \le t, i = 1, 2\}$. If the conditions are satisfied, then it is not difficult to check that $\Delta\mathcal{F} = GF(v)^*$, and hence $\mathcal{F}$ forms a cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DF. This completes the proof. □

Applying Theorem 5 with $k = 2$, one can obtain the following result.

Corollary 2. *Let $v = 54t+1$ be a prime, $e = 9$, θ a primitive element of GF(v), and ξ a primitive 3rd root of unity in GF(v). Let $c_0 = 1$. If there exist elements c_i, $1 \le i \le 2$, such that*

$S = \{c_i(\xi - 1) : 0 \le i \le 2\} \bigcup \{c_1 - 1, c_1 - \xi, c_1 - \xi^2\} \bigcup \{c_0, c_1, c_2\}$ forms an SDRC of H^9, then there exists a cyclic $(v, \{4, 7\}, 1, \{1/2, 1/2\})$-DF.

Example 2. A cyclic $(163, \{4, 7\}, 1, \{1/2, 1/2\})$-DF. Let $v = 163$, $\theta = 2$ be a primitive element of GF(163), then $\xi = \theta^{54} = 104$, $\xi^2 = 58$. Let $c_1 = 67$, $c_2 = 3$, then c_1, c_2 satisfying the condition in Corollary 2,

$$A_1 = \{0, 1, 104, 58, c_1, 104c_1, 58c_1\} = \{0, 1, 104, 58, 67, 122, 137\},$$
$$A_2 = \{0, c_2, 104c_2, 58c_2\} = \{0, 3, 149, 11\},$$
$$\mathcal{F}_{163} = \{\theta^{9j}A_i : \ i = 1, 2, 1 \le j \le 3\}$$
$$= \{\{0, 23, 110, 30, 74, 35, 54\}, \{0, 40, 85, 38, 72, 153, 101\}, \{0, 69, 4, 90\},$$
$$\{0, 105, 162, 59, 26, 96, 41\}, \{0, 120, 92, 114\}, \{0, 152, 160, 14\}\}.$$

It is not difficult to check that $\mathcal{F}_{163}$ forms a cyclic $(163, \{4, 7\}, 1, \{1/2, 1/2\})$-DF.

Let $T = \{v : v \equiv 1 \pmod{54}$ is a prime, $55 < v \le 5000\}$, $T_1 = \{109, 271, 1621, 2269, 3079, 3187\}$. The following result is obtained.

Lemma 9. *For each $v \in T \backslash T_1$, there exists a cyclic $(v, \{4, 7\}, 1, \{1/2, 1/2\})$-DF.*

Proof. For each $v \in T \setminus T_1$, with the aid of a computer, one can find elements c_1, c_2 satisfying conditions in Corollary 2. We list (v, θ, c_1, c_2) in Appendix B. This completes the proof. □

Lemma 10. *For each $v \in T_1$, there exists a cyclic $(v, \{4, 7\}, 1, \{1/2, 1/2\})$-DF.*

Proof. For each $v \in T_1$, with the aid of a computer, $A_v^{(i)}$, $i = 1, 2$ in Lemma 7 had been found, we list $A_v^{(i)}, \theta$, $i = 1, 2$ as follows. This completes the proof.

$A_{109}^{(1)} = \{0, 1, 4, 9, 16, 36, 58\}$, $A_{109}^{(2)} = \{0, 2, 26, 47\}$, $\theta = 6$,
$A_{271}^{(1)} = \{0, 1, 3, 7, 24, 50, 180\}$, $A_{271}^{(2)} = \{0, 9, 76, 202\}$, $\theta = 6$,
$A_{1621}^{(1)} = \{0, 1, 3, 8, 21, 46, 984\}$, $A_{1621}^{(2)} = \{0, 6, 221391\}$, $\theta = 2$,
$A_{2269}^{(1)} = \{0, 1, 5, 11, 25, 105, 552\}$, $A_{2269}^{(2)} = \{0, 16, 145, 1844\}$, $\theta = 2$,
$A_{3079}^{(1)} = \{0, 1, 5, 19, 40, 69, 295\}$, $A_{3079}^{(2)} = \{0, 8, 202, 707\}$, $\theta = 6$,
$A_{3187}^{(1)} = \{0, 1, 5, 11, 25, 64, 1140\}$, $A_{3187}^{(2)} = \{0, 22, 288, 2302\}$, $\theta = 2$. □

We are now in a position to prove Theorems 2.

Proof of Theorem 2. The result comes from Lemmas 9-10. □

4 Cyclic $(v, \{4, 6, 7\}, 1, \{1/3, 1/3, 1/3\})$-DFs

Theorem 6. *Let $v = 84t+1$ be a prime, $e = 14$, θ a primitive element of $GF(v)$, ξ a primitive 3rd root of unity in $GF(v)$. Let $c_0 = 1$. If there exist elements c_i, $1 \le i \le 4$, such that*

$S = \{c_i(\xi - 1) : 0 \le i \le 4\} \bigcup \{c_h - c_l, c_h - c_l\xi, c_h - c_l\xi^2 : 0 \le l < h \le 3\} \bigcup \{c_0, c_1, c_4\}$

forms an SDRC of H^e, then there exists a cyclic $(v, \{4, 6, 7\}, 1, \{1/3, 1/3, 1/3\})$-DF.

Proof. Let $A_1 = \{0, 1, \xi, \xi^2, c_1, c_1\xi, c_1\xi^2\}$, $A_2 = \{c_2, c_2\xi, c_2\xi^2, c_3, c_3\xi, c_3\xi^2\}$, $A_3 = \{0, c_4, c_4\xi, c_4\xi^2\}$.

Since ξ is a primitive 3rd root of unity in GF(v), then $\xi^2 - 1 = \xi^2 - \xi^3 = -\xi^2(\xi - 1)$. It is not difficult to see that $\bigcup_{i=1}^{3} \Delta A_i = (S \bigcup (-S)) \circ \{1, \xi, \xi^2\}$.

Let $\mathcal{F} = \{A_i\theta^{ej} : 1 \le j \le t, 1 \le i \le 3\}$. If the conditions are satisfied, then it is not difficult to check that $\Delta\mathcal{F} = GF(v)^*$, and hence $\mathcal{F}$ forms a cyclic $(v, \{4, 6, 7\}, 1, \{1/3, 1/3, 1/3\})$-DF. This completes the proof. □

We are now in a position to prove Theorem 3.

Proof of Theorem 3. For each prime $v \equiv 1 \pmod{84} \le 5000$ and $v > 85$, with the aid of a computer, elements $c_1, \ldots, c_4$ satisfying conditions in Theorem 6 had been found. We list $(v, \theta, c_1, c_2, c_3, c_4)$ in Appendix C. This completes the proof. □

5 New Optimal Variable OOCs

In [24], Gu and Wu had used Singer difference sets and PBDs to construct DFs. Given a cyclic $(v, K, 1)$-DF, breaking up some of the base blocks of size $k \in K$ by a $(k, H, 1)$-PBD, one can obtain the following result, which is a generalization of Gu and Wu in [24].

Lemma 11. *Suppose there exists a cyclic $(v, K, 1)$-DF. For $k \in K$, if there exists a $(k, H, 1)$-PBD, then there exists a cyclic $(v, K \bigcup H, 1)$-DF.*

Remark 3. Breaking up all base blocks of size $k \in K$ by a $(k, H, 1)$-PBD, one can obtain a cyclic $(v, (K \setminus \{k\}) \bigcup H, 1)$-DF. One can also breaking up base blocks of distinct block sizes to obtain cyclic difference families.

Let $G = Z_7$, $\mathcal{B} = \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}\}$. It is well known that $(G, \mathcal{B})$ is a $(7, 3, 1)$-BIBD.

For prime $v = 54t + 1 \le 5000$ and $v > 55$, the cyclic difference family in Theorem 2 has t blocks of size 4 and 7 each. For $1 \le s \le t$, breaking up s blocks of size 7 by a $(7, 3, 1)$-BIBD, one can obtain the following result.

Lemma 12. *For prime $v = 54t + 1 \le 5000$ and $v > 55$, there exists a cyclic $(v, \{3, 4\}, 1, \{7/8, 1/8\})$-DF. For each $1 \le s < t$, there exists a cyclic $(v, \{3, 4, 7\}, 1, \{\frac{7s}{2t+6s}, \frac{t}{2t+6s}, \frac{t-s}{2t+6s}\})$-DF.*

For prime $v = 84t+1 \leq 5000$ and $v > 85$, the cyclic difference family in Theorem 6 has t blocks of size 4, 6 and 7 each. For $1 \leq s \leq t$, breaking up s blocks of size 7 by a $(7, 3, 1)$-BIBD, one can obtain the following result.

Lemma 13. *For prime* $v = 84t + 1 \leq 5000$ *and* $v > 85$, *there exists a cyclic* $(v, \{3, 4, 6\}, 1, \{7/9, 1/9, 1/9\})$*-DF. For each* $1 \leq s < t$, *there exists a cyclic* $(v, \{3, 4, 6, 7\}, 1, \{\frac{7s}{3t+6s}, \frac{t}{3t+6s}, \frac{t}{3t+6s}, \frac{t-s}{3t+6s}\})$*-DF.*

From Theorems 1-3, Lemmas 12-13 and Lemma 3, the following results are obtained.

Theorem 7. *For each prime* $v = 42t + 1 \leq 5000$ *and* $v > 43$, *there exists an optimal* $(v, \{4, 6\}, 1, \{1/2, 1/2\})$-OOC. *There does not exist an optimal* $(43, \{4, 6\}, 1, \{1/2, 1/2\})$-OOC.

Theorem 8. *For each prime* $v = 54t + 1 \leq 5000$, $v > 55$, *the following optimal variable-weight* OOC *exists:*

(1) *a* $(v, \{4, 7\}, 1, \{1/2, 1/2\})$-OOCs*;*
(2) *a* $(v, \{3, 4\}, 1, \{7/8, 1/8\})$-OOCs*;*
(3) $(v, \{3, 4, 7\}, 1, \{\frac{7s}{2t+6s}, \frac{t}{2t+6s}, \frac{t-s}{2t+6s}\})$-OOCs *for each* $1 \leq s < t$.

Theorem 9. *For each prime* $v = 84t + 1 \leq 5000$, $v > 85$, *the following optimal variable-weight* OOCs *exists:*

(1) *a* $(v, \{4, 6, 7\}, 1, \{1/3, 1/3, 1/3\})$-OOCs*;*
(2) *a* $(v, \{3, 4, 6\}, 1, \{7/9, 1/9, 1/9\})$-OOCs*;*
(3) $(v, \{3, 4, 6, 7\}, 1, \{\frac{7s}{3t+6s}, \frac{t}{3t+6s}, \frac{t}{3t+6s}, \frac{t-s}{3t+6s}\})$-OOCs *for each* $1 \leq s < t$.

Remark 4. One can use Corollary 1 and Corollary 2 to construct cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DFs for $u = 6, 7$ and primes $v \equiv 1 \pmod{u(u-1)+12} > 5000$. One can also use Theorem 4 and Theorem 5 to construct cyclic $(v, \{4, u\}, 1, \{1/2, 1/2\})$-DFs for $u \equiv 0, 1 \pmod 3 > 7$ and primes $v \equiv 1 \pmod{u(u-1)+12}$, for example $u \in \{9, 10, 12, 13, 15\}$. By breaking up some of the blocks by PBD, new cyclic difference families are obtained, and new optimal variable-weight OOCs are constructed. Note that a $(9, 3, 1)$-BIBD, a $(10, \{3, 4\}, 1)$-PBD, a $(12, \{3, 4\}, 1)$-PBD, a $(13, 3, 1)$-BIBD, a $(13, \{4, 7\}, 1)$-PBD, a $(15, \{3, 5\}, 1)$-PBD, a $(15, \{3, 4\}, 1)$-PBD exist.

References

1. Salehi, J.A.: Code division multiple access techniques in optical fiber networks-Part I Fundamental Principles. IEEE Trans. Commun. 37, 824–833 (1989)
2. Salehi, J.A., Brackett, C.A.: Code division multiple access techniques in optical fiber networks-Part II Systems performance analysis. IEEE Trans. Commun. 37, 834–842 (1989)
3. Chung, F.R.K., Salehi, J.A., Wei, V.K.: Optical orthogonal codes: Design, analysis and applications. IEEE Trans. Inform. Theory 35, 595–604 (1989)

4. Golomb, S.W.: Digital communication with space application. Penisula, Los Altos (1982)
5. Massey, J.L., Mathys, P.: The collision channel without feedback. IEEE Trans. Inform. Theory 31, 192–204 (1985)
6. Salehi, J.A.: Emerging optical code-division multiple-access communications systems. IEEE Network 3, 31–39 (1989)
7. Vecchi, M.P., Salehi, J.A.: Neuromorphic networks based on sparse optical orthogonal codes. In: Neural Information Processing Systems-Natural and Synthetic, pp. 814–823. Amer. Inst. Phys, New York (1988)
8. Abel, R., Buratti, M.: Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes. J. Combin. Theory 106, 59–75 (2004)
9. Bitan, S., Etzion, T.: Constructions for optimal constant weight cyclically permutable codes and difference families. IEEE Trans. Inform. Theory 41, 77–87 (1995)
10. Buratti, M.: Cyclic designs with block size 4 and related optimal optical orthogonal codes. Des. Codes Cryptogr. 26, 111–125 (2002)
11. Chang, Y., Fuji-Hara, R., Miao, Y.: Combinatorial constructions of optimal optical orthogonal codes with weight 4. IEEE Trans. Inform. Theory 49, 1283–1292 (2003)
12. Chang, Y., Ji, L.: Optimal $(4up, 5, 1)$ optical orthogonal codes. J. Combin. Des. 12, 346–361 (2004)
13. Chang, Y., Miao, Y.: Constructions for optimal optical orthogonal codes. Discrete Math. 261, 127–139 (2003)
14. Chen, K., Ge, G., Zhu, L.: Starters and related codes. J. Statist. Plann. Inference 86, 379–395 (2000)
15. Chu, W., Colbourn, C.J.: Recursive constructions for optimal $(n, 4, 2)$-OOCs. J. Combin. Des. 12, 333–345 (2004)
16. Chu, W., Golomb, S.W.: A new recursive construction for optical orthogonal codes. IEEE Trans. Inform. Theory 49, 3072–3076 (2003)
17. Chung, H., Kumar, P.V.: Optical orthogonal codes-new bounds and an optimal construction. IEEE Trans. Inform. Theory 36, 866–873 (1990)
18. Fuji-Hara, R., Miao, Y.: Optical orthogonal codes: Their bounds and new optimal constructions. IEEE Trans. Inform. Theory 46, 2396–2406 (2000)
19. Fuji-Hara, R., Miao, Y., Yin, J.: Optimal $(9v, 4, 1)$ optical orthogonal codes. SIAM J. Discrete Math. 14, 256–266 (2001)
20. Ge, G., Yin, J.: Constructions for optimal $(v, 4, 1)$ optical orthogonal codes. IEEE Trans. Inform. Theory 47, 2998–3004 (2001)
21. Ma, S., Chang, Y.: A new class of optimal optical orthogonal codes with weight five. IEEE Trans. Inform. Theory 50, 1848–1850 (2004)
22. Ma, S., Chang, Y.: Constructions of optimal optical orthogonal codes with weight five. J. Combin. Des. 13, 54–69 (2005)
23. Yin, J.: Some combinatorial constructions for optical orthogonal codes. Discrete Math. 185, 201–219 (1998)
24. Gu, F.R., Wu, J.: Construction and performance analysis of variable-weight optical orthogonal codes for asynchronous optical CDMA systems. J. Lightw. Technol. 23, 740–748 (2005)
25. Yang, G.C.: Variable-weight optical orthogonal codes for CDMA networks with multiple performance requirements. IEEE Trans. Commun. 44, 47–55 (1996)
26. Yang, G.C.: Variable weight optical orthogonal codes for CDMA networks with multiple performance requirements. In: GLOBECOM 1993, vol. 1, pp. 488–492. IEEE, Los Alamitos (1993)

27. Wu, D., Fan, P., Li, H., Parampalli, U.: Optimal variable-weight optical orthogonal codes via cyclic difference families. In: 2009 IEEE International Symposium on Information Theory, ISIT 2009, June 28-July 3, pp. 448–452. IEEE, Los Alamitos (2009)
28. Buratti, M.: Pairwise balanced designs from finite fields. Discrete Math. 208/209, 103–117 (1999)
29. Wu, D., Chen, Z., Cheng, M.: A note on the existence of balanced $(q, \{3, 4\}, 1)$ difference families. The Australasian J. Combin. 41, 171–174 (2008)
30. Wu, D., Cheng, M., Chen, Z., Luo, H.: The existence of balanced $(v, \{3, 6\}, 1)$ difference families. Science in China (Ser. F) (to appear)
31. Abel, R., Buratti, M.: Differnce families. In: Colbourn, C.J., Dinitz, J.H. (eds.) The CRC Handbook of Combinatorial Designs, 2nd edn., pp. 392–410. Chapman and Hall/CRC, Boca Raton (2006)

Appendix A

$(v, \theta, c_1, c_2) \in \{(337, 10, 33, 15), (379, 257, 12), (421, 2, 9, 2), (463, 3, 2, 9), (547, 2, 88, 3), (631, 3, 7, 19), (673, 5, 3, 5), (967, 5, 12, 7), (1009, 11, 9, 32), (1051, 7, 44, 4), (1093, 5, 44, 14), (1303, 6, 20, 9), (1429, 6, 8, 4), (1471, 6, 30, 2), (1723, 3, 23, 3), (1933, 5, 11, 6), (2017, 5, 6, 2), (2143, 3, 50, 5), (2269, 2, 30, 8), (2311, 3, 16, 2), (2437, 2, 32, 34), (2521, 17, 2, 12), (2647, 3, 3, 8), (2689, 19, 33, 3),(2731, 3, 14, 9), (2857, 11, 31, 27), (3067, 2, 38, 2), (3109, 6, 42, 3), (3319, 6, 11, 7), (3361, 22, 28, 3), (3529, 17, 19, 2), (3571, 2, 77, 31), (3613, 2, 23, 2), (3697, 5, 9, 3), (3739, 7, 29, 3), (3823, 3, 11, 3), (3907, 2, 16, 4), (4159, 3, 16, 2), (4201, 11, 19, 8), (4243, 2, 21, 10), (4327, 3, 8, 2), (4621, 2, 8, 4), (4663, 3, 20, 3), (4789, 2, 39, 6), (4831, 3, 9, 4), (4957, 2, 24, 3), (4999, 3, 53, 3)\}$.

Appendix B

$(v, \theta, c_1, c_2) \in \{(163, 2, 67, 3), (379, 2, 27, 3), (433, 5, 32, 2), (487, 3, 135, 3), (541, 2, 148, 6), (757, 2, 126, 7), (811, 3, 5, 9), (919, 7, 147, 14), (1297, 10, 20, 2), (1459, 3, 38, 4), (1567, 3, 17, 23), (1783, 10, 56, 4), (1999, 3, 57, 4), (2053, 2, 43, 4), (2161, 23, 58, 15), (2377, 5, 98, 8), (2539, 2, 262, 6), (2593, 7, 50, 43), (2647, 3, 191, 15), (2917, 5, 102, 3), (2971, 10, 179, 15), (3457, 7, 29, 9), (3511, 7, 44, 3), (3673, 5, 43, 2), (3727, 3, 8, 13), (3889, 11, 224, 5), (3943, 3, 35, 43), (4051, 10, 35, 5), (4159, 3, 170, 3), (4483, 2, 45, 6), (4591, 11, 25, 11), (4861, 11, 4, 2), (4969, 11, 82, 6)\}$.

Appendix C

$(v, \theta, c_1, c_2, c_3, c_4) \in \{(337, 10, 11, 38, 9, 18), (421, 2, 3, 68, 4, 52), (673, 5, 11, 298, 6, 9), (757, 2, 8, 94, 5, 7), (1009, 11, 16, 67, 4, 32), (1093, 5, 4, 383, 5, 28), (1429, 6, 10, 82, 3, 14), (1597, 11, 5, 105, 7, 10), (1933, 5, 2, 417, 8, 10), (2017, 5, 2, 14, 3, 6), (2269, 2, 2, 645, 6, 3), (2437, 2, 2, 53, 3, 8), (2521, 17, 11, 238, 16, 2), (2689, 19, 16, 1559, 17, 3), (2857, 11, 13, 681, 10, 3), (3109, 6, 2, 115, 7, 13), (3361, 22, 2, 36, 3, 4), (3529, 17, 2, 287, 4, 31), (3613, 2, 3, 139, 8, 5), (3697, 5, 3, 243, 4, 67), (4201, 11, 2, 129, 3, 4), (4621, 2, 2, 142, 4, 14), (4789, 2, 2, 477, 6, 17), (4957, 2, 2, 811, 7, 16)\}$.

Recent Results on Recursive Nonlinear Pseudorandom Number Generators
(Invited Paper)

Arne Winterhof

Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz, Austria
arne.winterhof@oeaw.ac.at

Dedicated to Joachim von zur Gathen on the occasion of his 60th birthday

Abstract. This survey article collects recent results on recursive nonlinear pseudorandom number generators and sketches some important proof techniques. We mention upper bounds on additive character sums which imply uniform distribution results. Moreover, we present lower bounds on the linear complexity profile and closely related lattice tests and thus results on the suitability in cryptography. Finally, we give bounds on multiplicative character sums from which one can derive results on the distribution of powers and primitive elements.

1 Introduction

Let p be a prime, r a positive integer, $q = p^r$ and denote by $\mathbb{F}_q$ the finite field of q elements. Given a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $d \geq 2$, we define the *recursive nonlinear pseudorandom number generator* (μ_n) of elements of $\mathbb{F}_q$ by the recurrence relation

$$\mu_{n+1} = f(\mu_n), \qquad n = 0, 1, \ldots, \tag{1}$$

with some *initial value* $\mu_0 \in \mathbb{F}_q$. This sequence is eventually periodic with some period $T \leq q$. We assume that the sequence (μ_n) is purely periodic.

In this survey we mention recent results on different features of these sequences in view of different applications. We study additive and multiplicative character sums as well as linear complexity and lattice tests in view of possible applications for quasi-Monte Carlo methods, cryptography or algorithmic number theory.

In [40,43,52,66], a method has been presented to study the additive character sums

$$S_{\mathbf{a},N}(f) = \sum_{n=0}^{N-1} \chi\left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+j}\right), \quad 1 \leq N \leq T,$$

and thus the distribution of such sequences for arbitrary polynomials $f(X)$ where χ is a nontrivial additive character of $\mathbb{F}_q$ and $\mathbf{a} = (\alpha_0, \ldots, \alpha_{s-1}) \in \mathbb{F}_q^s \setminus \mathbf{0}$, see

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 113–124, 2010.

also the recent surveys [37,44,47,63,66]. More precisely, under some necessary restrictions, say $\gcd(d,p)=1$, we can prove:

$$S_{\mathbf{a},N}(f) \ll N\left(\log\frac{2q}{N}\right)^{1/2}(\log d)^{1/2}/(\log q)^{1/2}, \quad 1\le N\le T, \tag{2}$$

where $A \ll B$ is equivalent to the assertion that the inequality $|A|\le cB$ holds for some constant $c>0$ depending only on s. We present the proof of (2) in Section 2. (Note that the general results of [40,52,66] deal only with the case $r=1$.)

Unfortunately, the general bound (2) is only nontrivial if $d=q^{o(1)}$. However, in several special cases one can obtain much stronger bounds. We give an overview of such known special cases in Section 3.

We derive from the sequence (μ_n) defined by (1) a nonlinear method for pseudorandom number generation defined as follows. Let $\{\beta_1,\ldots,\beta_r\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and identify $\mathbb{F}_p$ with the set of integers $\{0,1,\ldots,p-1\}$. If

$$\mu_n = u_{n,1}\beta_1+\ldots+u_{n,r}\beta_r, \quad \text{with } u_{n,i}\in\mathbb{F}_p,$$

then we derive *digital nonlinear pseudorandom numbers* in the unit interval $[0,1)$ by putting

$$y_n=\sum_{j=1}^{r} u_{n,j}p^{-j}.$$

For positive integers N and s the *discrepancy* $D_N^{(s)}$ of $\mathbf{y}_0,\ldots,\mathbf{y}_{N-1}\in[0,1)^s$ is

$$D_N^{(s)}(P)=D_N^{(s)}(\mathbf{y}_0,\ldots,\mathbf{y}_{N-1})=\sup_J\left|\frac{A_N(J)}{N}-V(J)\right|,$$

where the supremum is taken over all sub-intervals $J\subseteq[0,1)^s$, $A_N(J)$ is the number of points $\mathbf{y}_0,\ldots,\mathbf{y}_{N-1}$ in J and $V(J)$ is the volume of J. The discrepancy is a measure for the deviation from uniform distribution and thus suitability for quasi-Monte Carlo methods. Suitable general discrepancy bounds reduce the discrepancy of the points $\mathbf{y}_n=(y_n,y_{n+1},\ldots,y_{n+s-1})$, $n=0,\ldots,N-1$, of consecutive digital nonlinear pseudorandom numbers to the additive character sums mentioned above, see for example the bound of [36, Theorem 3.12]. For $r=1$ we mention the *Erdős-Turán-Koksma inequality*, see [11, Theorem 1.21]:

$$D_N^{(s)}(\mathbf{y}_0,\ldots,\mathbf{y}_{N-1})\ll\frac{1}{H}+\frac{1}{N}\sum_{0<\max_{0\le i<s}\alpha_i\le H}\frac{1}{\prod_{i=0}^{s-1}\max\{|\alpha_i|,1\}}|S_{\mathbf{a},N}(f)|$$

for any $H\ge1$, where the implied constant depends only on s.

For $N\ge1$ and a sequence (μ_n) over $\mathbb{F}_q$, its *Nth linear complexity* $L(\mu_n,N)$ over $\mathbb{F}_q$ is the smallest integer L such that there exist $\alpha_0,\ldots,\alpha_{L-1}\in\mathbb{F}_q$ such that

$$\mu_{n+L}=\alpha_{L-1}\mu_{n+L-1}+\ldots+\alpha_0\mu_n \quad \text{for } 0\le n<N-L, \tag{3}$$

with the conventions that $L(\mu_n, N) = 0$ if $\mu_0 = \cdots = \mu_{N-1} = 0$ and $L(\mu_n, N) = N$ if $\mu_0 = \cdots = \mu_{N-2} = 0$ but $\mu_{N-1} \neq 0$. Its *linear complexity* is $L(\mu_n) = \sup_{N \geq 1} L(\mu_n, N)$. Note that for a T-periodic sequence we have $L(\mu_n) \leq T$. The linear complexity is a measure for the unpredictability and thus suitability in cryptography. For recent surveys on linear complexity and related measures see [38,68].

For the sequence (μ_n) defined in (1) we know the general lower bound

$$L(\mu_n, N) \geq \frac{\min\{\log(N - \log N/\log d), \log T\}}{\log d}, \quad N \geq 1, \tag{4}$$

of [28, Theorem 4]. We give the short proof of (4) in Section 4. Specially tailored results for some special cases have been proved and are also mentioned in Section 4.

Whereas linear complexity comes from cryptography, a closely related concept called *lattice test* has its origin in the area of quasi-Monte Carlo methods. We mention recent results on this area in Section 6.

Besides studying additive character sums, bounds on *multiplicative character sums* are of interest in view of results on the distribution of powers and primitive elements in a finite field. We mention the recent results in this area in Section 5.

2 Proof of the General Additive Character Sum Bound

In this section, we prove the bound (2) using the method of bounding character sums introduced in [40,43] and refined in [52,66].

Proof. We can assume $N \geq 2q^{1/2}$. We first prove that, for any integer $r \geq 1$ and $\mathbf{0} \neq \mathbf{a} \in \mathbb{F}_q^s$, we have

$$S_{\mathbf{a},N} \ll Nr^{1/2}(q/N)^{1/(2r)}(\min\{\log q, rq^{1/(11r)}\})^{-1/2} \tag{5}$$

for $2q^{1/2} \leq N \leq T$. Since otherwise (5) is trivial, we may assume $r < \log q$.

It is obvious that for any integer $k \geq 0$ we have

$$\left| S_{\mathbf{a},N}(f) - \sum_{n=0}^{N-1} \chi\left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+j+k}\right)\right| \leq 2k.$$

Therefore, for any integer $K \geq 1$,

$$K|S_{\mathbf{a},N}(f)| \leq W + K(K-1), \tag{6}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi\left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+j+k}\right)\right|.$$

We consider the sequence of polynomials $f_k(X) \in \mathbb{F}_q[X]$ defined by

$$f_0(X) = X, \quad f_k(X) = f(f_{k-1}(X)), \quad k \geq 1. \tag{7}$$

By the Hölder inequality, using $\mu_{n+k} = f_k(\mu_n)$ and putting

$$F_k(X) = \sum_{j=0}^{s-1} \alpha_j f_{k+j}(X),$$

we obtain

$$W^{2r} \le N^{2r-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi(F_k(\mu_n)) \right|^{2r} \le N^{2r-1} \sum_{x \in \mathbb{F}_q} \left| \sum_{k=0}^{K-1} \chi(F_k(x)) \right|^{2r}$$
$$\le N^{2r-1} \sum_{k_1,\ldots,k_{2r}=0}^{K-1} \left| \sum_{x \in \mathbb{F}_q} \chi(F_{k_1,\ldots,k_{2r}}(x)) \right|,$$

where $F_{k_1,\ldots,k_{2r}}(X) = F_{k_1}(X) + \ldots + F_{k_r}(X) - F_{k_{r+1}}(X) - \ldots - F_{k_{2r}}(X)$. If $\{k_1, \ldots, k_r\} = \{k_{r+1}, \ldots, k_{2r}\}$ as multisets, then $F_{k_1,\ldots,k_{2r}}(X)$ is constant and the inner sum is trivially equal to q. There are at most $r!K^r \le r^r K^r$ such sums. Otherwise note that the degree of $F_{k_1,\ldots,k_{2r}}$ is not divisible by p since $\gcd(d, p) = 1$ and we can apply Weil's bound (see e.g. [33, Chapter 5]) to the inner sum using $\deg(F_{k_1,\ldots,k_{2r}}) \le d^{K+s-2}$, to get the upper bound $d^{K+s-2}q^{1/2}$ for at most K^{2r} sums. Hence,

$$W^{2r} \le r^r K^r N^{2r-1} q + d^{K+s-2} K^{2r} N^{2r-1} q^{1/2}. \tag{8}$$

Choose

$$K = \min \left\{ \left\lceil 0.4 \frac{\log q}{\log d} \right\rceil, \left\lfloor r q^{1/(11r)} \right\rfloor \right\}$$

Then it is easy to see that the first term on the right-hand side of (8) dominates the second one in terms of the order of magnitude in q, and we get (5) from (6) and (8) after simple calculations.

Finally, we choose

$$r = \lfloor \log(q/N) \rfloor + 1$$

and the theorem follows after simple calculations from (5). □

3 Improvements for Some Special Nonlinear Generators

In two special cases, nonlinear generators with small *p-weight degree* [30] and *inversive generators* [27,39,41,43] the method in the proof of (2) leads to stronger bounds. For other special classes of polynomials, namely for *monomials* and *Dickson polynomials*, an alternative approach, producing much stronger bounds has been proposed in [2,18,19,21]. Related results for sequences produced by *Rédei functions* are obtained in [29]. Moreover, we mention that certain multivariate polynomial systems with slow degree growth introduced in [57] admit stronger additive character sum bounds than in the general case of higher order nonlinear recurrences [25,26,56].

For a nonnegative integer n, we define its *p-weight* (or *p-adic digit sum*) as the sum of the coefficients in its p-adic expansion:

$$\sigma_p\left(\sum_{i=0}^{l} n_i p^i\right) = \sum_{i=0}^{l} n_i, \text{ if } 0 \le n_i < p.$$

Let $0 \le e_1 < e_2 < \cdots < e_l$ be integers and $f(X) = \sum_{i=1}^{l} \gamma_i X^{e_i} \in \mathbb{F}_q[X]$ be a nonzero polynomial over a finite field $\mathbb{F}_q$, with $\gamma_i \ne 0$, $i = 1, \ldots, l$. We define its *p-weight degree* as

$$w_p(f) = \max\{\sigma_p(e_i) \mid 1 \le i \le l\}.$$

Therefore, $w_p(f) \le \deg(f)$. The main result of [30] is the following complement of (2) in the case that

$$f(X) = \alpha X^d + \tilde{f}(X) \in \mathbb{F}_q[X] \quad \text{with} \quad \alpha \ne 0, \quad w_p(\tilde{f}) < \sigma_p(d), \quad d \ge 2, \tag{9}$$

and

$$\gcd\left(d, \frac{q-1}{p-1}\right) \le \sigma_p(d)^r. \tag{10}$$

If the sequence (μ_n) given by (1) with a polynomial $f(X) \in \mathbb{F}_q[X]$ of the form (9), and satisfying (10) is purely periodic with period T, then

$$S_{\mathbf{a},N}(f) \ll N\left(\log \frac{2q}{N}\right)^{1/2} (\log w)^{1/2}/(\log p)^{1/2}, \quad 1 \le N \le T, \quad \mathbf{a} \ne \mathbf{0},$$

where $w = \sigma_p(d) > 1$ is the p-weight degree of $f(X)$ and the implied constant depends only on s. This result is proved in [30] and improves (2) for polynomials satisfying (9) and (10) if and only if $w^r < \deg(f)$.

The *inversive generator* (y_n) defined by

$$y_{n+1} = a y_n^{q-2} + b = \begin{cases} a y_n^{-1} + b & \text{if } y_n \ne 0, \\ b & \text{otherwise,} \end{cases} \quad n \ge 0, \tag{11}$$

with $a, b, y_0 \in \mathbb{F}_q$, $a \ne 0$, admits an additive character sum bound of order of magnitude $N^{1/2} q^{1/4}$.

Now we give the definitions of three more nice nonlinear pseudorandom number generators but refer to the original literature mentioned above for the corresponding bounds on additive character sums.

The *power generator* (p_n) is defined as

$$p_{n+1} = p_n^e, \quad n \ge 0,$$

with some integer $e \ge 2$ and initial value $0 \ne p_0 \in \mathbb{F}_p$. Additive character sums of the power generator were obtained in [2,18,19].

The family of *Dickson polynomials* $D_e(X, a) \in \mathbb{F}_p[X]$ is defined by the following recurrence relation

$$D_e(X, a) = X D_{e-1}(X, a) - a D_{e-2}(X, a), \quad e = 2, 3, \ldots,$$

with initial values $D_0(X,a)=2$, $D_1(X,a)=X$, where $a\in\mathbb{F}_p$. It is easy to see that $D_e(X,0)=X^e$, $e\ge 2$, which corresponds to the case of the power generator. Additive character sums of nonlinear generators with Dickson polynomials $D_e(X,1)$ were investigated in [21].

Another class of nonlinear congruential pseudorandom number generators, where $f(X)$ is a Rédei function, was analyzed in [29]. Suppose that

$$r(X)=X^2-\alpha X-\beta\in\mathbb{F}_p[X]$$

is an irreducible quadratic polynomial with the two different roots ξ and $\zeta=\xi^p$ in $\mathbb{F}_{p^2}$. We consider the polynomials $g_e(X)$ and $h_e(X)\in\mathbb{F}_p[X]$, which are uniquely defined by the equation

$$(X+\xi)^e=g_e(X)+h_e(X)\xi.$$

The *Rédei function* $f_e(X)$ of degree e is then given by

$$f_e(X)=\frac{g_e(X)}{h_e(X)}.$$

As any mapping over $\mathbb{F}_p$, the Rédei permutation can be uniquely represented by a polynomial of degree at most $p-1$ and therefore generators with Rédei functions belong to the class of nonlinear pseudorandom number generators (1).

We can regard sequences over $\mathbb{F}_{p^r}$ as r-dimensional vector sequences over $\mathbb{F}_p$ and define nonlinear vector sequences by $\mathbf{u}_{n+1}=(F_1(\mathbf{u}_n),\ldots,F_r(\mathbf{u}_n))$, $n\ge 0$, with multivariate polynomials $F_1,\ldots,F_r$ over $\mathbb{F}_p$ and some initial vector $\mathbf{u}_0$. In general, as in the case $r=1$, we can expect only an exponential degree growth of the iterations and thus bounds only as moderate as (2), see [56]. However, systems of multivariate polynomials with slow degree growth were introduced in [57] and further analyzed in [54,55,57,58] and give much better bounds on additive character sums. The multidimensional case brings in new (and favorable) effects which are impossible in the univariate case. We recall the construction of [57] of multivariate polynomial systems with slow degree growth. Let $F_i\in\mathbb{F}_p[X_1,\ldots,X_r]$, $i=1,\ldots,r$, be defined in the following way:

$$\begin{aligned}
F_1(X_1,\ldots,X_r) &= X_1G_1(X_2,\ldots,X_r)+H_1(X_2,\ldots,X_r),\\
F_2(X_1,\ldots,X_r) &= X_2G_2(X_3,\ldots,X_r)+H_2(X_3,\ldots,X_r),\\
&\ldots\\
F_{r-1}(X_1,\ldots,X_r) &= X_{r-1}G_{r-1}(X_r)+H_{r-1}(X_r),\\
F_r(X_1,\ldots,X_r) &= g_rX_r+h_r,
\end{aligned}$$

where $g_r,h_r\in\mathbb{F}_p$, $g_r\ne 0$, $G_i,H_i\in\mathbb{F}_p[X_{i+1},\ldots,X_r]$, $i=0,\ldots,r-1$. If either the G_i are constant, see [55], or under certain restrictions on the relative degrees of G_i and H_i, see [54,57,58], much better additive character sum bounds can be obtained than in the general case.

Exponential sums of nonlinear generators over residue class rings have also been studied. See [14,15,16,17] for general nonlinear generators, [42,48,51] for inversive generators, and [12,13] for the power generator.

Most of the results mentioned above are only nontrivial if the period T of the nonlinear generator is sufficiently long. However, little is known about it except for the inversive generator [5,6], the power generator [31], and Dickson permutation polynomials [32].

Some bounds on the average over all initial values are given in [45,64].

4 Linear Complexity Bounds

In this section first we prove the bound (4).

Proof. If the first N sequences elements $\mu_0, \ldots, \mu_{N-1}$ satisfy a linear recurrence (3) of length L we immediately see that the polynomial

$$F(X) = f_L(X) - \alpha_{L-1} f_{L-1}(X) - \ldots - \alpha_0 f_0(X)$$

of degree d^L has at least $\min\{N - L, T\}$ zeros and the result follows, where $f_0(X), \ldots, f_L(X)$ are defined by (7). □

Specially tailored results have been proved for the inversive generator [28], power generator [24,62], Dickson generator [1] and Rédei generator [35]. The linear complexities of nonlinear pseudorandom number generators of higher order and with multivariate polynomial systems have been analyzed in [65] and [59].

In [30] we proved the following improvement in a slightly more general form. If the sequence (μ_n) given by (1) with a polynomial $f(X) \in \mathbb{F}_q[X]$ of the form (9) satisfying

$$\gcd\left(d, \frac{q-1}{p-1}\right) \le \sigma_p(d)^{r/2},$$

with p-weight degree $w = \sigma_p(d) > 1$, is purely periodic with period T, then for $N \ge 2p^{r-1} \log p / \log w$,

$$L(\mu_n, N) \ge \frac{\log(\min\{N, T\}/p^{r-1}) - 1}{\log w}, \quad N \ge 2.$$

Note that this result is only an improvement of the result of [28] if $w_p(f) < \deg(f)^{1/r}$.

The inversive generator has linear complexity profile

$$L(y_n, N) \ge \min\left\{\frac{N-1}{3}, \frac{T-1}{2}\right\}, \quad N \ge 2.$$

The power generator satisfies

$$L(p_n, N) \ge \min\left\{\frac{N^2}{4(p-1)}, \frac{T^2}{p-1}\right\}, \quad N \ge 2.$$

Similar bounds for generators with Dickson polynomials with $a = 1$ or with Rédei functions were given in [1] and [35].

The linear complexity of vector sequences defined with the polynomial systems of [57] was analyzed in [59].

5 Multiplicative Character Sums and Distribution of Powers and Primitive Elements

The methods for estimating additive character sums can very often be adapted for estimating multiplicative character sums

$$S_\chi(N) = \sum_{n=0}^{N-1} \chi(\mu_n), \quad 1 \le N \le T,$$

as well. For arbitrary nonlinear generators see [50]. Improvements for inversive, Dickson and Rédei generators were obtained in [46,22,23]. Multiplicative character sums of nonlinear generators defined with the polynomial systems of [57] were estimated in [60]. Estimates on character sums with inversive and nonlinear recurring sequences on average over all initial values were given in [3].

Nontrivial estimates on $S_\chi(N)$ imply asymptotic formulas for the number of sth powers among $\mu_0, \mu_1, \ldots, \mu_{N-1}$ using standard arguments and primitive elements using Vinogradov's formula (see [33, Exercise 5.14]).

6 Lattice Tests

The following lattice test was introduced in [53]. Let (μ_n), $n = 0, 1, \ldots$, be a T-periodic sequence over $\mathbb{F}_q$. For given integers $s \ge 1$, $0 \le d_0 < d_1 < \ldots < d_{s-1} < T$, and $N \ge 2$, we say that (μ_n) passes the *s-dimensional N-lattice test with lags $d_0, \ldots, d_{s-1}$* if the vectors $\{\boldsymbol{u}_n - \boldsymbol{u}_0 : 0 \le n \le N-1\}$ span $\mathbb{F}_q^s$, where

$$\boldsymbol{u}_n = (\mu_{n+d_0}, \mu_{n+d_1}, \ldots, \mu_{n+d_{s-1}}), \quad 0 \le n \le N-1.$$

In the case $d_i = i$ for $0 \le i < s$, this test coincides essentially with the lattice test introduced in [9] and further analyzed in [7,8,9,10,20,67]. The latter lattice test is closely related to the concept of the linear complexity profile, see [9,10,49]. If additionally $N \ge T$, this special lattice test was proposed by Marsaglia [34].

The close relationship between the lattice test and linear recurrence relation is illustrated in the sequel.

We assume that the sequence elements $\mu_0, \ldots, \mu_{N-1}$ do not pass the s-dimensional N-lattice test for some lags $0 \le d_0 < d_1 < \ldots < d_{s-1} < p^2$. Let V be the subspace of $\mathbb{F}_q^s$ spanned by all $\boldsymbol{u}_n - \boldsymbol{u}_0$ for $0 \le n \le N-1$. Denote by $V^\perp = \{\boldsymbol{u} \in \mathbb{F}_q^s : \boldsymbol{u} \cdot \boldsymbol{v} = 0 \text{ for all } \boldsymbol{v} \in V\}$ the *orthogonal space* of V, where $\cdot$ denotes the usual inner product. Then $\dim(V) < s$ and $\dim(V^\perp) \ge 1$. Take $\boldsymbol{0} \ne \boldsymbol{\alpha} \in V^\perp$, then

$$\boldsymbol{\alpha} \cdot (\boldsymbol{u}_n - \boldsymbol{u}_0) = 0 \quad \text{for } 0 \le n \le N-1.$$

We denote $\delta = \boldsymbol{\alpha} \cdot \boldsymbol{u}_n = \boldsymbol{\alpha} \cdot \boldsymbol{u}_0$ for $0 \le n \le N-1$. If $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{s-1})$, then we get

$$\sum_{i=0}^{s-1} \alpha_i \mu_{n+d_i} \equiv \delta \pmod{p} \quad \text{for } 0 \le n \le N-1,$$

and we have derived an inhomogeneous linear recurrence. If d_{s-1} is small, the same methods as for estimating the linear complexity profile apply. However, for arbitrary lags little is known [53]. The only good bounds known are for a modification of the inversive generator introduced in [39] and further analyzed in [53]. However, for several *explicit* nonlinear pseudorandom number generators good results on the lattice test with arbitrary lags are known [61,4].

Acknowledgment

The author wishes to thank the organizers of SETA2010 for inviting him and his co-authors (and close friends) for the joyful joint works, in particular Gottlieb Pirsic and Igor Shparlinski for many useful comments.

References

1. Aly, H., Winterhof, A.: On the linear complexity profile of nonlinear congruential pseudorandom number generators with Dickson polynomials. Des. Codes Cryptogr. 39, 155–162 (2006)
2. Bourgain, J.: Mordell's exponential sum estimate revisited. J. Amer. Math. Soc. 18, 477–499 (2005)
3. Çeşmelioğlu, A., Winterhof, A.: On the average distribution of power residues and primitive elements in inversive and nonlinear recurring sequences. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 60–70. Springer, Heidelberg (2008)
4. Chen, Z., Ostafe, A., Winterhof, A.: Structure of pseudorandom numbers derived from Fermat quotients. In: Hasan, M.A., Helleseth, T. (eds.) WAIFI 2010. LNCS, vol. 6087, pp. 73–85. Springer, Heidelberg (2010)
5. Chou, W.-S.: The period lengths of inversive congruential recursions. Acta Arith. 73, 325–341 (1995)
6. Chou, W.-S.: The period lengths of inversive pseudorandom vector generations. Finite Fields Appl. 1, 126–132 (1995)
7. Dorfer, G.: Lattice profile and linear complexity profile of pseudorandom number sequences. In: Mullen, G.L., Poli, A., Stichtenoth, H. (eds.) Fq7 2003. LNCS, vol. 2948, pp. 69–78. Springer, Heidelberg (2004)
8. Dorfer, G., Meidl, W., Winterhof, A.: Counting functions and expected values for the lattice profile at n. Finite Fields Appl. 10, 636–652 (2004)
9. Dorfer, G., Winterhof, A.: Lattice structure and linear complexity profile of nonlinear pseudorandom number generators. Appl. Algebra Engrg. Comm. Comput. 13, 499–508 (2003)
10. Dorfer, G., Winterhof, A.: Lattice structure of nonlinear pseudorandom number generators in parts of the period. In: Niederreiter, H. (ed.) Monte Carlo and Quasi-Monte Carlo Methods 2002, pp. 199–211. Springer, Berlin (2004)
11. Drmota, M., Tichy, R.F.: Sequences, discrepancies and applications. LNM, vol. 1651. Springer, Berlin (1997)
12. El-Mahassni, E.D.: On the distribution of the power generator modulo a prime power for parts of the period. Bol. Soc. Mat. Mexicana 13(3), 7–13 (2007)
13. El-Mahassni, E.D.: On the distribution of the power generator over a residue ring for parts of the period. Rev. Mat. Complut. 21, 319–325 (2008)

14. El-Mahassni, E.D.: Exponential sums for nonlinear recurring sequences in residue rings. Albanian J. Math. (to appear)
15. El-Mahassni, E.D., Gomez, D.: On the distribution of nonlinear congruential pseudorandom numbers of higher orders in residue rings. In: Bras-Amorós, M., Høholdt, T. (eds.) AAECC-18. LNCS, vol. 5527, pp. 195–203. Springer, Heidelberg (2009)
16. El-Mahassni, E.D., Shparlinski, I.E., Winterhof, A.: Distribution of nonlinear congruential pseudorandom numbers modulo almost squarefree integers. Monatsh. Math. 148, 297–307 (2006)
17. El-Mahassni, E.D., Winterhof, A.: On the distribution of nonlinear congruential pseudorandom numbers in residue rings. Int. J. Number Theory 2, 163–168 (2006)
18. Friedlander, J.B., Hansen, J., Shparlinski, I.E.: Character sums with exponential functions. Mathematika 47, 75–85 (2000)
19. Friedlander, J.B., Shparlinski, I.E.: On the distribution of the power generator. Math. Comp. 70, 1575–1589 (2001)
20. Fu, F.W., Niederreiter, H.: On the counting function of the lattice profile of periodic sequences. J. Complexity 23, 423–435 (2007)
21. Gomez-Perez, D., Gutierrez, J., Shparlinski, I.E.: Exponential sums with Dickson polynomials. Finite Fields Appl. 12, 16–25 (2006)
22. Gomez, D., Winterhof, A.: Character sums for sequences of iterations of Dickson polynomials. Finite fields and applications. Contemp. Math. 461, 147–151 (2008)
23. Gomez, D., Winterhof, A.: Multiplicative character sums of recurring sequences with Redéi functions. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 175–181. Springer, Heidelberg (2008)
24. Griffin, F., Shparlinski, I.E.: On the linear complexity profile of the power generator. IEEE Trans. Inform. Theory 46, 2159–2162 (2000)
25. Griffin, F., Niederreiter, H., Shparlinski, I.E.: On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders. In: Fossorier, M.P.C., Imai, H., Lin, S., Poli, A. (eds.) AAECC 1999. LNCS, vol. 1719, pp. 87–93. Springer, Heidelberg (1999)
26. Gutierrez, J., Gomez-Perez, D.: Iterations of multivariate polynomials and discrepancy of pseudorandom numbers. In: Bozta, S., Sphparlinski, I. (eds.) AAECC 2001. LNCS, vol. 2227, pp. 192–199. Springer, Heidelberg (2001)
27. Gutierrez, J., Niederreiter, H., Shparlinski, I.E.: On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period. Monatsh. Math. 129, 31–36 (2000)
28. Gutierrez, J., Shparlinski, I.E., Winterhof, A.: On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators. IEEE Trans. Inform. Theory 49, 60–64 (2003)
29. Gutierrez, J., Winterhof, A.: Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions. Finite Fields Appl. 14, 410–416 (2008)
30. Ibeas, A., Winterhof, A.: Exponential sums and linear complexity of nonlinear pseudorandom number generators with polynomials of small p-weight degree. Unif. Distrib. Theory 5, 79–93 (2010)
31. Kurlberg, P., Pomerance, C.: On the periods of the linear congruential and power generators. Acta Arith. 119, 149–169 (2005)
32. Lidl, R., Mullen, G.L.: Cycle structure of Dickson permutation polynomials. Math. J. Okayama Univ. 33, 1–11 (1991)
33. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications, Revision of the 1986 first edition. Cambridge University Press, Cambridge (1994)

34. Marsaglia, G.: The structure of linear congruential sequences. In: Zaremba, S.K. (ed.) Applications of Number Theory to Numerical Analysis, pp. 249–285. Academic Press, New York (1972)
35. Meidl, W., Winterhof, A.: On the linear complexity profile of nonlinear congruential pseudorandom number generators with Rédei functions. Finite Fields Appl. 13, 628–634 (2007)
36. Niederreiter, H.: Random number generation and quasi-Monte Carlo methods. In: CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 63. Society for Industrial and Applied Mathematics (SIAM), Philadelphia (1992)
37. Niederreiter, H.: Design and analysis of nonlinear pseudorandom number generators. In: Monte Carlo Simulation, pp. 3–9. A.A. Balkema Publishers (2001)
38. Niederreiter, H.: Linear complexity and related complexity measures for sequences. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 1–17. Springer, Heidelberg (2003)
39. Niederreiter, H., Rivat, J.: On the correlation of pseudorandom numbers generated by inversive methods. Monatsh. Math. 153, 251–264 (2008)
40. Niederreiter, H., Shparlinski, I.E.: On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. Finite Fields Appl. 5, 246–253 (1999)
41. Niederreiter, H., Shparlinski, I.E.: On the distribution of pseudorandom numbers and vectors generated by inversive methods. Appl. Algebra Engrg. Comm. Comput. 10, 189–202 (2000)
42. Niederreiter, H., Shparlinski, I.E.: Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. Acta Arith. 92, 89–98 (2000)
43. Niederreiter, H., Shparlinski, I.E.: On the distribution of inversive congruential pseudorandom numbers in parts of the period. Math. Comp. 70, 1569–1574 (2001)
44. Niederreiter, H., Shparlinski, I.E.: Recent advances in the theory of nonlinear pseudorandom number generators. In: Monte Carlo and quasi-Monte Carlo methods, 2000 (Hong Kong), pp. 86–102. Springer, Berlin (2002)
45. Niederreiter, H., Shparlinski, I.E.: On the average distribution of inversive pseudorandom numbers. Finite Fields Appl. 8, 491–503 (2002)
46. Niederreiter, H., Shparlinski, I.E.: On the distribution of power residues and primitive elements in some nonlinear recurring sequences. Bull. London Math. Soc. 35, 522–528 (2003)
47. Niederreiter, H., Shparlinski, I.E.: Dynamical systems generated by rational functions. In: Fossorier, M.P.C., Høholdt, T., Poli, A. (eds.) AAECC 2003. LNCS, vol. 2643, pp. 6–17. Springer, Heidelberg (2003)
48. Niederreiter, H., Winterhof, A.: On the distribution of compound inversive congruential pseudorandom numbers. Monatsh. Math. 132, 35–48 (2001)
49. Niederreiter, H., Winterhof, A.: Lattice structure and linear complexity of nonlinear pseudorandom numbers. Appl. Algebra Engrg. Comm. Comput. 13, 319–326 (2002)
50. Niederreiter, H., Winterhof, A.: Multiplicative character sums for nonlinear recurring sequences. Acta Arith. 111, 299–305 (2004)
51. Niederreiter, H., Winterhof, A.: Exponential sums and the distribution of inversive congruential pseudorandom numbers with power of two modulus. Int. J. Number Theory 1, 431–438 (2005)
52. Niederreiter, H., Winterhof, A.: Exponential sums for nonlinear recurring sequences. Finite Fields Appl. 14, 59–64 (2008)
53. Niederreiter, H., Winterhof, A.: On the structure of inversive pseudorandom number generators. In: Boztaş, S., Lu, H.-F(F.) (eds.) AAECC 2007. LNCS, vol. 4851, pp. 208–216. Springer, Heidelberg (2007)

54. Ostafe, A.: Multivariate permutation polynomial systems and pseudorandom number generators. Finite Fields Appl. 16, 144–154 (2010)
55. Ostafe, A.: Pseudorandom vector sequences derived from triangular polynomial systems with constant multipliers. In: Anwar Hasan, M. (ed.) WAIFI 2010. LNCS, vol. 6087, pp. 62–72. Springer, Heidelberg (2010)
56. Ostafe, A., Pelican, E., Shparlinski, I.E.: On pseudorandom numbers from multivariate polynomial systems. Finite Fields Appl. (to appear)
57. Ostafe, A., Shparlinski, I.E.: On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators. Math. Comp. 79, 501–511 (2010)
58. Ostafe, A., Shparlinski, I.E.: Pseudorandom numbers and hash functions from iterations of multivariate polynomials. Cryptography and Communications 2, 49–67 (2010)
59. Ostafe, A., Shparlinski, I.E., Winterhof, A.: On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences. Adv. Math. Commun. 4, 369–379 (2010)
60. Ostafe, A., Shparlinski, I.E., Winterhof, A.: Multiplicative character sums of a class of nonlinear recurrence vector sequences (preprint)
61. Pirsic, G., Winterhof, A.: On the structure of digital explicit nonlinear and inversive pseudorandom number generators. J. Complexity 26, 43–50 (2010)
62. Shparlinski, I.E.: On the linear complexity of the power generator. Des. Codes Cryptogr. 23, 5–10 (2001)
63. Shparlinski, I.E.: On some dynamical systems in finite fields and residue rings. Discrete Contin. Dyn. Syst. 17, 901–917 (2007)
64. Shparlinski, I.E.: On the average distribution of pseudorandom numbers generated by nonlinear permutations. Math. Comp. (to appear)
65. Topuzoğlu, A., Winterhof, A.: On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders. Appl. Algebra Engrg. Comm. Comput. 16, 219–228 (2005)
66. Topuzoğlu, A., Winterhof, A.: Pseudorandom sequences. In: Topics in Geometry, Coding Theory and Cryptography. Algebr. Appl., vol. 6, pp. 135–166. Springer, Dordrecht (2007)
67. Wang, L.-P., Niederreiter, H.: Successive minima profile, lattice profile, and joint linear complexity profile of pseudorandom multisequences. J. Complexity 24, 144–153 (2008)
68. Winterhof, A.: Linear complexity and related complexity measures. In: Selected Topics in Information and Coding Theory, pp. 3–40. World Scientific, Singapore (2010)

A General Approach to Construction and Determination of the Linear Complexity of Sequences Based on Cosets

Ayça Çeşmelioğlu and Wilfried Meidl

Faculty of Engineering and Natural Sciences,
Sabancı University, Tuzla, 34956, İstanbul, Turkey

Abstract. We give a general approach to N-periodic sequences over a finite field $\mathbb{F}_q$ constructed via a subgroup D of the group of invertible elements modulo N. Well known examples are Legendre sequences or the two-prime generator. For some generalizations of sequences considered in the literature and for some new examples of sequence constructions we determine the linear complexity.

1 Introduction

A sequence $S = s_0, s_1, \ldots$ with terms in a finite field $\mathbb{F}_d$ with d elements is said to be N-*periodic* if $s_i = s_{i+N}$ for all $i \geq 0$. The *linear complexity* $L(S)$ of an N-periodic sequence S over $\mathbb{F}_d$ is the smallest nonnegative integer L for which there exist coefficients $c_1, c_2, \ldots, c_L$ in $\mathbb{F}_d$ such that S satisfies the linear recurrence relation $s_i + c_1 s_{i-1} + \cdots + c_L s_{i-L} = 0$ for all $i \geq L$. If d and N are relatively prime and θ is a primitive Nth root of unity in some extension field of $\mathbb{F}_d$, and $S(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$ then

$$L(S) = N - |\{a \ : \ S(\theta^a) = 0, 0 \leq a \leq N-1\}|. \tag{1}$$

The linear complexity is considered as a primary quality measure for periodic sequences and plays an important role in applications of sequences in cryptography and communication (see for instance [13] and the references therein).

In this paper we point to a general approach to N-periodic sequences over a finite field $\mathbb{F}_d$ defined via a subgroup D of the group $\mathbb{Z}_N^*$ of the invertible elements modulo N. Well-known basic examples are the Legendre sequences and its generalizations and the two-prime generator. We describe a uniform approach to obtain results on the linear complexity for such sequence constructions that comprise also the known proofs [3,4,5,6,7] for the above mentioned examples. We apply this approach to some further examples of sequences and determine their linear complexity. The first example can be seen as a natural generalization of earlier constructions, the further examples are different, some - otherwise than the sequences mentioned above - are based on subgroups D of $\mathbb{Z}_N^*$ for which the factor group $\mathbb{Z}_N^*/D$ is not cyclic.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 125–138, 2010.

2 A General Construction of Sequences Based on Cosets

Let N be an odd integer, Δ be a divisor of $\varphi(N)$, where φ denotes Euler's totient function, and let $D = D_0$ be a subgroup of index Δ of $\mathbb{Z}_N^*$, the group of invertible elements modulo N. Denote the elements of the factor group $G = \mathbb{Z}_N^*/D_0$ by $\{D_0, D_1, \ldots, D_{\Delta-1}\}$. Naturally this defines a partition of $\mathbb{Z}_N^*$, regarding to which we will write $n \in D_j$ if $nD_0 = D_j$ for an integer $n \in \mathbb{Z}_N^*$. An N-periodic sequence $S = s_0, s_1, \ldots$ over a finite field $\mathbb{F}_d$ satisfying

$$s_n = \xi_j \text{ whenever } n \bmod N \in D_j$$

is then called a *coset sequence*. We remark that the sequence terms s_n for $\gcd(n, N) \neq 1$ have to be defined separately.

In order to obtain (almost) balanced sequences over $\mathbb{F}_d$ one may prefer to consider subgroups D_0 of index d and to assign every field element $\xi_j \in \mathbb{F}_d$ to precisely one coset D_j.

If the period $N = p$ is prime and Δ is a divisor of $p - 1$, then the (only) subgroup D_0 of index Δ of $\mathbb{Z}_N^*$ is the set of Δth powers

$$D_0 = \{g^{\Delta s} \ : \ s = 0, 1, \ldots, (p-1)/\Delta - 1\} \tag{2}$$

for a primitive element g modulo p. The cosets $D_j = g^j D_0$, $0 \leq j \leq \Delta - 1$, are then called the *cyclotomic classes* of order Δ. Trivially the factor group $\mathbb{Z}_N^*/D_0$ is then cyclic.

Some well-known examples of coset sequences are the following:

Legendre sequences and its generalizations: To describe this class of sequences in its most general form we have to fix an ordering of the elements of the finite field $\mathbb{F}_d$, $d = r^t$ for a prime r. Given a basis $\{\beta_0, \beta_1, \ldots, \beta_{t-1}\}$ of $\mathbb{F}_{r^t}$ over $\mathbb{F}_r$ we fix an ordering of the elements of $\mathbb{F}_{r^t}$ by

$$\xi_j = j_0\beta_0 + j_1\beta_1 + \cdots + j_{t-1}\beta_{t-1} \tag{3}$$

if $(j_0, j_1, \ldots, j_{t-1})_r$ is the r-ary representation of the integer j. If $t = 1$ this reduces to the conventional ordering $0, 1, \ldots, r-1$ of the prime field $\mathbb{F}_r$ (with $\beta_0 = 1$).

Let $N = p$ be a prime, $\Delta = d = r^t$ a prime power divisor of $p - 1$ and D_0 be the group of the dth powers modulo p. The *generalized Legendre sequence* is then the N-periodic sequence over $\mathbb{F}_d$ defined by

$$s_n = \xi_j \text{ if } n \bmod p \in D_j, \quad \text{and} \quad s_n = 0 \text{ if } n \equiv 0 \bmod p. \tag{4}$$

For $d = 2$ the sequence (4) is known as the classical Legendre sequence, its linear complexity is determined in [5]. In [6] and [4] the linear complexity of (4) is presented for d prime and for $d = r^t$, r prime and $\gcd(t, r) = 1$.

Hall's sextic residue sequence: Let $N = p$ be prime congruent 1 modulo 6, $D_0, \ldots, D_5$ be the cyclotomic classes of order 6 defined as in (2). The N periodic binary coset sequence given by

$$s_n = \begin{cases} 1 & : \quad n \bmod N \in D_0 \cup D_1 \cup D_3, \\ 0 & : \quad \text{otherwise} \end{cases}$$

is called *Hall's sextic residue sequence* (see [10] for its linear complexity).

Two-prime generator: For two odd primes p and q let D_0 be the subgroup of index 2 of $\mathbb{Z}_{pq}^*$ consisting of the elements which are either squares or nonsquares modulo both primes p and q. Denoting the two elements of the corresponding factor group by D_0 and D_1, the *two-prime generator* is the binary pq-periodic sequence given by $s_{n+pq} = s_n$ and for $0 \le n < pq$

$$s_n = j \text{ if } n \in D_j, \ s_n = 0 \text{ if } n \in Q \cup \{0\} \text{ and } s_n = 1 \text{ if } n \in P,$$

where here and in the following $P = p\mathbb{Z}_q^* = \{p, 2p, \ldots, (q-1)p\}$ and $Q = q\mathbb{Z}_p^* = \{q, 2q, \ldots, (p-1)q\}$. The linear complexity of the two-prime generator has been determined in [7] for $\gcd(p-1, q-1) = 2$. In [9] the generalization to arbitrary prime fields has been analysed.

In [1,15] the subgroup D of $\mathbb{Z}_{pq}^*$ which consists of all elements which are a square modulo q has been used to define a pq-periodic binary sequence. As pointed out in [12] where a generalization to arbitrary prime fields was considered, these sequences essentially are only concatenations of p Legendre sequences of period q. Similar constructions leading to binary sequences of period q^m and $2q^m$ with much similarity to concatenated Legendre sequences of period q have been considered recently in [14,16].

3 Basic Results

In what follows N will always be an odd integer, d a prime power divisor of $\varphi(N)$, D_0 a subgroup of $\mathbb{Z}_N^*$ of index d, and $D_0, D_1, \ldots, D_{d-1}$ denote the cosets of D_0. If $\mathbb{Z}_N^*/D_0$ is cyclic, which always applies when d is prime, then we can suppose that $D_i D_j = D_{i+j \bmod d}$.

Let S be a coset sequence of period N over $\mathbb{F}_d$ with $s_n = \xi_j$ if $n \in D_j$. (At this position ξ_j does not necessarily refer to the ordering in (3).) The polynomial $S(x)$ corresponding to S can then be written as $S(x) = U(x) + T(x)$ with

$$U(x) = \sum_{n \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*} s_n x^n \ \text{ and } \ T(x) = \sum_{j=0}^{d-1} \xi_j f_j(x) \ \text{ where } \ f_j(x) = \sum_{i \in D_j} x^i. \qquad (5)$$

We collect some simple basic properties which partly had been shown in the literature for different concrete examples of coset sequences (see e.g. [4,5,6,7]). In what follows we suppose that $d = r^t$, r prime, $\gcd(N, r) = 1$, and we let θ be a primitive Nth root of unity over $\mathbb{F}_d$.

Lemma 1
(i) *If* $a, \bar{a} \in D_i$ *for some* $0 \le i \le d-1$ *then* $T(\theta^{\bar{a}}) = T(\theta^a)$.
(ii) *For all* $0 \le a \le N-1$ *we have* $f_j(\theta^a) \in \mathbb{F}_{r^d}$, $0 \le j \le d-1$. *If* $d \in D_0$ *then* $f_j(\theta^a) \in \mathbb{F}_d$, $0 \le j \le d-1$, *and* $T(\theta^a) \in \mathbb{F}_d$ *for all* $0 \le a \le N-1$. *If also* $r \in D_0$ *then* $f_j(\theta^a) \in \mathbb{F}_r$, $0 \le j \le d-1$, *for all* $0 \le a \le N-1$.
(iii) *If* $a \in D_k$ *then* $T(\theta^a) = \sum_{j=0}^{d-1} \xi_{j \ominus k} f_j(\theta)$ *where* $j \ominus k = l$ *if* $D_j = D_k D_l$ *in* $\mathbb{Z}_N^*/D_0$.
(iv) $\sum_{j=0}^{d-1} f_j(\theta) = \mu(N)$, *where* μ *denotes the Möbius function.*

Proof. (i),(ii) are straightforward, we also may refer to [4].
(iii) $T(\theta^a) = \sum_{j=0}^{d-1} \xi_j \sum_{i \in D_j} \theta^{ai} = \sum_{j=0}^{d-1} \xi_j \sum_{i \in aD_j} \theta^i = \sum_{j=0}^{d-1} \xi_j f_{j \oplus k}(\theta) = \sum_{j=0}^{d-1} \xi_{j \ominus k} f_j(\theta)$.
(iv) Observe that $\sum_{j=0}^{d-1} f_j(\theta) = \sum_{k \in \mathbb{Z}_N^*} \theta^k$ is the negative of the coefficient of $x^{\varphi(N)-1}$ in the Nth cyclotomic polynomial $\mathcal{Q}_N$. With $\mathcal{Q}_N = \prod_{c|N} (x^{N/c} - 1)^{\mu(c)}$ (see [11, Theorem 3.27]) we obtain

$$\mathcal{Q}_N = \frac{(x^{a_1} - 1) \cdots (x^{a_1} - 1)}{(x^{b_1} - 1) \cdots (x^{b_s} - 1)} = (x^A - x^{A-a_1} + \cdots \pm 1) \ : \ (x^B - x^{B-b_1} + \cdots \pm 1),$$

where a_i, b_j run through the divisors c of N for which N/c is squarefree, we choose a_1 and b_1 to be the minimum of the a_i and b_j, respectively, and put $A = a_1 + \cdots + a_r$ and $B = b_1 + \cdots + b_s$. As obvious, $A - B = \varphi(N)$. Performing the division we then get

$$\mathcal{Q}_N = x^{\varphi(N)} \pm x^{\varphi(N) - \min(a_1, b_1)} \pm \cdots + 1,$$

where the coefficient of $x^{\varphi(N)-\min(a_1,b_1)}$ is "1" if $a_1 > b_1$ and "-1" if $a_1 < b_1$. As $\mu(N) = 0$ implies $\min(a_1, b_1) > 1$, the coefficient of $x^{\varphi(N)-1}$ in $\mathcal{Q}_N$ is zero in this case. If $\mu(N) = 1$ then $\min(a_1, b_1) = a_1 = 1$, if $\mu(N) = -1$ then $\min(a_1, b_1) = b_1 = 1$, which completes the proof. □

As generally known the possible values for the linear complexity of an N-periodic sequence over $\mathbb{F}_d$ depend on the degrees of the polynomials in the canonical factorization of $x^N - 1$ over $\mathbb{F}_d$. The following proposition indicates that for many classes of coset sequences the order of the coset D_j which contains d in the factor group $\mathbb{Z}_N^*/D_0$ decides on the possible values for the linear complexity.

Proposition 1. *Let* D_0 *be a subgroup of* $\mathbb{Z}_N^*$, $G = \mathbb{Z}_N^*/D_0$, $d \in D_j$ *and let* $B = \langle D_j \rangle$ *be the subgroup of* G *generated by* D_j. *For a corresponding coset sequence over* $\mathbb{F}_d$ *let* $T(x)$ *be defined as in* (5). *If* $T(\theta^a) = 0$ *for* $a \in D_k$ *then* $T(\theta^b) = 0$ *for all* $b \in BD_k$.

Proof. Let s be the order of d modulo N, then the minimal polynomial of θ^a over $\mathbb{F}_d$ is given by $m(x) = \prod_{l=0}^{s-1} (x - \theta^{ad^l})$. Consequently if $T(\theta^a) = 0$ then $T(\theta^{ad^l}) = 0$ for $0 \le l \le s-1$. Since $B = \langle D_j \rangle = \{D_0, dD_0 = D_j, \ldots, d^{s-1}D_0\}$ (depending on the order of D_j in G elements in this set repeat), with Lemma 1(i) we have $T(\theta^b) = 0$ for all $b \in BD_k$. □

Remark 1. If $U(\theta^a) = c \in \mathbb{F}_d$ is constant for all $a \in \mathbb{Z}_N^*$ then Lemma 1(i) and consequently Proposition 1 also holds for $S(x)$.

If $\mathbb{Z}_N^*/D_0$ is cyclic (as in the sequence constructions in the literature , see [1,4,5,6,7,12,15]) then we can naturally employ the ordering defined as in (3) to define a coset sequence. Following the objective of the paper to give a general approach to N-periodic sequences constructed via subgroups D_0 of $\mathbb{Z}_N^*$ we consider further classes of factor groups that are not cyclic. We concentrate hereby on factor groups whose order is a prime power.

For an odd integer N and a prime r let D_0 be a subgroup of $\mathbb{Z}_N^*$ such that $\mathbb{Z}_N^*/D_0$ is isomorphic to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$ (with the componentwise addition) for some positive integers t_i, $1 \le i \le w$. The cardinality of $\mathbb{Z}_N^*/D_0$ is then $d = r^t$ with $t = t_1 + t_2 + \ldots + t_w$, and we can easily define an N-periodic coset sequence over $\mathbb{F}_d$ which is close to be balanced.

Example. Let $N = pq$ for two odd primes p and q, let $D_0^{(p)}$ and $D_0^{(q)}$ denote the set of squares modulo p and q, and consider

$$D_0 = \{j \mid 1 \le j \le pq-1, j \bmod p \in D_0^{(p)}, j \bmod q \in D_0^{(q)}\},$$

As obvious D_0 is a subgroup of $\mathbb{Z}_{pq}^*$ with $\mathbb{Z}_{pq}^*/D_0$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

For the definition of a sequence we again employ the ordering (3) of the elements of $\mathbb{F}_{r^t}$. In order to assign the elements of $\mathbb{F}_{r^t}$ to the r^t cosets of D_0 we also need an ordering of the elements of $\mathbb{Z}_N^*/D_0$. We put $\rho_0 = 0, \rho_1 = t_1, \rho_2 = t_1+t_2, \ldots, \rho_w = \sum_{i=1}^w t_i = t$, and let Ψ be the isomorphism from $\mathbb{Z}_N^*/D_0$ to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$. For $0 \le j \le r^t - 1$ we then denote the coset D of D_0 by D_j for which

$$\Psi(D) = (J_1, J_2, \ldots, J_w) \text{ with } J_1 + J_2 r^{\rho_1} + J_3 r^{\rho_2} + \cdots + J_w r^{\rho_{w-1}} = j. \qquad (6)$$

Based on the orderings (3), (6), N-periodic coset sequences over $\mathbb{F}_{r^t}$ with

$$s_n = \xi_j \text{ if } n \in D_j$$

can be defined. We remark that $D_k D_l = D_{k \oplus l}$ when we define

$$k \oplus l = h \text{ if } k = \sum_{i=1}^w K_i r^{\rho_i}, l = \sum_{i=1}^w L_i r^{\rho_i} \text{ and } h = \sum_{i=1}^w (K_i + L_i \bmod r^{t_i}) r^{\rho_i}, \quad (7)$$

according to the operation in $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$.

The following Lemma generalizes [4, Lemma 10] shown for the generalized Legendre sequence (4).

Lemma 2. *Let N be squarefree, D_0 a subgroup of $\mathbb{Z}_N^*$, $d = r^t$ a prime power with $\gcd(r,t) = 1$, and let*

1. *$\mathbb{Z}_N^*/D_0$ be a cyclic group of order d, or*
2. *$\mathbb{Z}_N^*/D_0$ be isomorphic to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$ with $t_1 + \cdots + t_w = t$.*

Consider a coset sequence over $\mathbb{F}_d$ satisfying $s_n = \xi_j$ if $n \in D_j$, where ξ_j refers to the ordering (3) of the elements of $\mathbb{F}_d$, the cosets D_j are naturally ordered in case 1 and ordered as in (6) in case 2. Then $T(\theta^{a'}) \neq T(\theta^a)$ if $a' \not\equiv a \bmod D_0$.

Proof. For this proof we denote by $k \oplus l$ the addition modulo d in case 1 and the addition (7) in case 2. Let $a \in D_k$ and $a' \in D_{k'}$, let $k \ominus k' = \delta$ and suppose that $0 \le v \le t-1$ is the smallest index in the r-ary representation of the integer $\delta = \sum_{i=0}^{t-1} \delta_i r^i$ of δ with $\delta_v \neq 0$. (We remark that in case 2 if $k = \sum_{i=1}^{w} K_i r^{\rho_i}$, $k' = \sum_{i=1}^{w} K'_i r^{\rho_i}$ and $\rho_{c-1} \le v < \rho_c$, then $K'_i = K_i$, $1 \le i < c$, but $K'_c \neq K_c$.)

Let $\xi_l = \sum_{i=0}^{t-1} l_i \beta_i$ and $\xi_{l\oplus\delta} = \sum_{i=0}^{t-1} l'_i \beta_i$. Then using the ordering of the elements of $\mathbb{F}_{r^t}$ and the property of v we get $l + \delta \equiv l \oplus \delta \equiv \sum_{i=0}^{v} l_i r^i + \delta_v r^v \bmod r^{v+1}$, thus $l'_i = l_i$ for $0 \le i \le v-1$ and $l'_v \equiv l_v + \delta_v \bmod r$.

For $0 \le j \le d-1$ we set $\xi_{j\ominus k} = \sum_{i=0}^{t-1} j_i \beta_i$ and $\xi_{j\ominus k'} = \sum_{i=0}^{t-1} j'_i \beta_i$. With Lemma 1(iii) we then obtain

$$T(\theta^{a'}) - T(\theta^a) = \sum_{j=0}^{d-1} (\xi_{j\ominus k'} - \xi_{j\ominus k}) f_j(\theta) = \sum_{j=0}^{d-1} (\xi_{j\ominus k\oplus\delta)} - \xi_{j\ominus k}) f_j(\theta)$$

$$= \sum_{j=0}^{d-1} \left(\delta_v \beta_v + \sum_{i=v+1}^{t-1} (j'_i - j_i)\beta_i \right) f_j(\theta)$$

$$= \delta_v \beta_v \sum_{j=0}^{d-1} f_j(\theta) + \sum_{j=0}^{d-1} \sum_{i=v+1}^{t-1} (j'_i - j_i)\beta_i f_j(\theta) = \mu(N)\delta_v \beta_v + \sum_{i=v+1}^{t-1} \beta_i \sum_{j=0}^{d-1} (j'_i - j_i) f_j(\theta)$$

$$= \mu(N)\delta_v \beta_v + \sum_{i=v+1}^{t-1} \Lambda_i \beta_i. \tag{8}$$

Since N is squarefree, (8) is a nontrivial linear combination of β_i, $0 \le i \le t-1$, and by Lemma 1(ii) its coefficients are in $\mathbb{F}_{r^d}$. As $\gcd(t, r) = 1$ the basis $\{\beta_0, \ldots, \beta_{t-1}\}$ of $\mathbb{F}_{r^t}$ over $\mathbb{F}_r$ is also a basis of $\mathbb{F}_{r^{td}}$ over $\mathbb{F}_{r^d}$, thus (8) is not 0. □

Corollary 1. *Let D_0 be a subgroup of prime power index $d = r^t$ of $\mathbb{Z}_N^*$, let $\mathbb{Z}_N^*/D_0$ be cyclic or isomorphic to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$. Let S be a coset sequence with $s_n = \xi_j$ if $n \in D_j$ for the ordering (3) of the elements in $\mathbb{F}_d$, the obvious ordering of $\mathbb{Z}_N^*/D_0$ in the cyclic case, else for the ordering defined in (6). If $d \in D_0$ then $T(\theta^a) = 0$ for $\varphi(N)/d$ values of $a \in \mathbb{Z}_N^*$. If $d \notin D_0$ then $T(\theta^a) \neq 0$ for all $a \in \mathbb{Z}_N^*$.*

Proof. By Lemma 2, $T(\theta^a) \neq T(\theta^{a'})$ if $a \not\equiv a' \bmod D_0$. If $d \in D_0$ then by Lemma 1(ii), $T(\theta^a) \in \mathbb{F}_d$ for all $a \in \mathbb{Z}_N^*$, thus for exactly one integer j, $0 \le j \le d-1$, we have $T(\theta^a) = 0$ if $a \in D_j$. If $d \in D_j \neq D_0$ then the order of D_j in $\mathbb{Z}_N^*/D_0$ is greater than 1, and with Proposition 1, $T(\theta^a) = 0$ for $a \in D_k$ implies that $T(\theta^b) = 0$ for all $b \in \langle D_j \rangle D_K$ which contradicts Lemma 2. □

We remark that Corollary 1 also holds for $S(x)$ if $U(\theta^a) = c \in \mathbb{F}_d$ for all $a \in \mathbb{Z}_N^*$.

4 Examples of Sequence Constructions

Let $N = pq$ for two odd primes p and q. As easily seen $aP = P$ if $a \in \mathbb{Z}_{pq}^*$ or $a \in P$ (where the calculation is performed modulo N), which will be used several times in the following.

On the basis of the previous section we firstly consider two constructions of pq-periodic sequences over an arbitrary finite field $\mathbb{F}_d$.

Construction 1: Let $d = r^t$ be a power of the prime r dividing $\gcd(p-1, q-1)$, then we can consider the cyclotomic classes (2) of order d, $D_j^{(p)}$ and $D_j^{(q)}$, $0 \le j \le d-1$, for both primes p, q, respectively. We define a subgroup D_0 by

$$D_0 = \{n \ : \ n \bmod p \in D_k^{(p)} \text{ and } n \bmod q \in D_l^{(q)} \\ \text{for some } k, l \text{ with } k + l \equiv 0 \bmod d\}. \tag{9}$$

For simplicity we will write $n \in D_k^{(p)} \sqcap D_l^{(q)}$ if $n \bmod p \in D_k^{(p)}$ and $n \bmod q \in D_l^{(q)}$. As obvious, the factor group $\mathbb{Z}_N^*/D_0$ is cyclic, its elements D_j, $0 \le j \le d-1$, are given by

$$D_j = \bigcup_{k+l \equiv j \bmod d} (D_k^{(p)} \sqcap D_l^{(q)}). \tag{10}$$

Note that $D_i D_j = D_{i+j \bmod d}$.

For $d = 2$, this construction reduces to the classical two-prime generator, thus we may call this construction the *generalized two-prime generator*. For d being an odd prime the generalized two-prime generator was analysed in [9].

Construction 2: Let $d = r^t$ be a power of the prime r, let t_1, t_2 be integers such that $t_1 + t_2 = t$, and let p and q be primes such that $d_1 = r^{t_1}$ divides $p-1$ and $d_2 = r^{t_2}$ divides $q-1$. (To keep the contribution of p and q to the behaviour of the sequence equal, one may prefer to choose d_1, d_2 close to each other, if possible $d_1 = r^{\lfloor t/2 \rfloor}$, $d_2 = r^{\lceil t/2 \rceil}$.) We consider the cyclotomic classes of order d_1 modulo p and order d_2 modulo q, and choose D_0 as

$$D_0 = \{n \mid 1 \le n \le pq-1, n \in D_0^{(p)} \sqcap D_0^{(q)}\}, \tag{11}$$

which is a subgroup of $\mathbb{Z}_{pq}^*$. The index of D_0 is $d = r^t$ and $\mathbb{Z}_{pq}^*/D_0$ is isomorphic to $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$. We then can employ the ordering (6) for the cosets of D_0.

For both subgroups, (9) and (11), we can utilize the ordering (3) of the elements of $\mathbb{F}_d$ and define a pq-periodic sequence $S = s_0, s_1, \ldots$ over $\mathbb{F}_d$ by

$$s_n = \begin{cases} \xi_j & : \quad n \in D_j, \\ 0 & : \quad n \in Q \cup \{0\}, \\ 1 & : \quad n \in P. \end{cases} \tag{12}$$

4.1 The Case $\gcd(r, t) = 1$

In the next theorem we determine the linear complexity of sequences obtained by both, Construction 1 and Construction 2. In order to be able to apply Lemma 2 and the subsequent Corollary 1 we need the condition $\gcd(r, t) = 1$.

Theorem 1. *For two odd primes p and q, and a power $d = r^t$ of the prime r with $\gcd(r, t) = 1$ let*

1. *d divide* $\gcd(p-1,q-1)$*, suppose* $d \neq 2$ *and let* D_0 *be the subgroup* (9) *of* $\mathbb{Z}_{pq}^*$*, or*
2. $d_1 = r^{t_1}$ *divide* $p-1$*,* $d_2 = r^{t_2}$ *divide* $q-1$ *for two positive integers* t_1, t_2 *with* $t = t_1 + t_2$*, suppose that* $r > 2$ *or* $t_i \geq 2$*,* $i = 1, 2$*, and let* D_0 *be the subgroup* (11) *of* $\mathbb{Z}_{pq}^*$*.*

Then the linear complexity L *of the sequence* (12) *is given by*

$$L = \begin{cases} pq - p - \frac{(p-1)(q-1)}{d} & : \quad d \in D_0 \\ pq - p & : \quad d \notin D_0. \end{cases}$$

Proof. Following (1) we have to determine the number of integers a, $0 \leq a \leq pq-1$ for which $S(\theta^a) = U(\theta^a) + T(\theta^a) = 0$ where $U(x), T(x)$ are defined as in (5), and θ is a primitive pqth root of unity in an extension field of $\mathbb{F}_d$.

We first observe that with $aP = P$ if $a \in \mathbb{Z}_{pq}^*$, we obtain $U(\theta^a) = \sum_{n \in P} \theta^{an} = \sum_{n \in P} \theta^n = U(\theta) = -1$. As a consequence, by Corollary 1 and the remark thereafter we have $S(\theta^a) \neq 0$ for all $a \in \mathbb{Z}_{pq}^*$ if $d \notin D_0$, and if $d \in D_0$ then $S(\theta^a) = 0$ for exactly $(p-1)(q-1)/d$ values for $a \in \mathbb{Z}_{pq}^*$. Hence it suffices to evaluate $S(\theta^a)$ for $a \in \mathbb{Z}_{pq} \setminus \mathbb{Z}_{pq}^*$.

First of all we see that

$$S(1) = \sum_{n \in P} 1 + \sum_{j=0}^{d-1} \xi_j \sum_{i \in D_j} 1 = (q-1) + \frac{(p-1)(q-1)}{d} \sum_{j=0}^{d-1} \xi_j = 0.$$

We finish the proof showing that $S(\theta^a) = -1$ if $a \in P$ and $S(\theta^a) = 0$ if $a \in Q$. With $aP = P$ if $a \in P$ we obtain $U(\theta^a) = -1$ as above, and $a \in Q$ implies $U(\theta^a) = \sum_{n \in P} \theta^{an} = \sum_{n \in P} 1 = q - 1 = 0$. Consequently it remains to be shown that $T(\theta^a) = \sum_{j=0}^{d-1} \xi_j f_j(\theta^a) = 0$ if $a \in P \cup Q$, where we have to distinguish between the two constructions.

Construction 1. Suppose that $b \in \mathbb{Z}_q^*$ is an element of $D_l^{(q)}$ and let $0 \leq k \leq d-1$ be the unique integer with $k + l \equiv j \bmod d$. By the Chinese remainder theorem for each of the $(p-1)/d$ elements c_i of $D_k^{(p)}$ there exists a unique integer n, $1 \leq n \leq pq-1$, with $n \equiv c_i \bmod p$, $n \equiv b \bmod q$, and by definition $n \in D_j$. Therefore if $a \in P$, then aD_j (modulo pq) runs $(p-1)/d$ times through $P = p\mathbb{Z}_q^*$. Consequently

$$f_j(\theta^a) = \sum_{i \in D_j} \theta^{ai} = \frac{p-1}{d} \sum_{n \in P} \theta^n = -\frac{p-1}{d},$$

hence $a \in P$ implies

$$T(\theta^a) = \sum_{j=0}^{d-1} \xi_j f_j(\theta^a) = -\frac{p-1}{d} \sum_{j=0}^{d-1} \xi_j. \tag{13}$$

For $a \in Q$ we similarly obtain $T(\theta^a) = -\frac{q-1}{d} \sum_{j=0}^{d-1} \xi_j$. With the assumption $d \neq 2$, the sum $\sum_{j=0}^{d-1} \xi_j$ of the elements of $\mathbb{F}_d$ vanishes, thus $T(\theta^a) = 0$ for $a \in P \cup Q$.

Construction 2. Let $j = r^{t_1}k+\ell$ with $k = 0, 1, \cdots, r^{t_2}-1$ and $\ell = 0, 1, \cdots, r^{t_1}-1$, then

$$D_j = \{n \mid 1 \le n \le pq-1, n \in D_l^{(p)} \sqcap D_k^{(q)}\}$$

by definition. Consequently if the set D_j is reduced modulo p every element of $D_l^{(p)}$ is taken on precisely $(q-1)/r^{t_2}$ times and vice versa in D_j reduced modulo q every element of $D_k^{(q)}$ appears $(p-1)/r^{t_1}$ times. For $a \in P$ we therefore get

$$f_j(\theta^a) = \sum_{i \in D_j} \theta^{ai} = \frac{p-1}{r^{t_1}} \sum_{i \in pD_k^{(q)}} \theta^i$$

and subsequently

$$T(\theta^a) = \sum_{k=0}^{r^{t_2}-1} \sum_{\ell=0}^{r^{t_1}-1} \frac{p-1}{r^{t_1}} \sum_{i \in pD_k^{(q)}} \theta^i \xi_{r^{t_1}k+\ell} \tag{14}$$

$$= \frac{p-1}{r^{t_1}} \sum_{k=0}^{r^{t_2}-1} \sum_{i \in pD_k^{(q)}} \theta^i \sum_{\ell=0}^{r^{t_1}-1} \xi_{r^{t_1}k+\ell}.$$

Since $\xi_{r^{t_1}k+\ell} = \xi_{r^{t_1}k} + \xi_\ell$ for all $k \in \{0, 1, \cdots, r^{t_2}-1\}, \ell \in \{0, 1, \cdots, r^{t_1}-1\}$, we can write

$$\sum_{\ell=0}^{r^{t_1}-1} \xi_{r^{t_1}k+\ell} = \sum_{\ell=0}^{r^{t_1}-1} \xi_{r^{t_1}k} + \xi_\ell = \sum_{\ell=0}^{r^{t_1}-1} \xi_\ell = 0, \tag{15}$$

where in the last step we used $r \neq 2$ or $r = 2$ and $t_1 > 1$. Hence $T(\theta^a) = 0$ for all $a \in P$.

For $a \in Q$ we obtain $T(\theta^a) = 0$ similarly if $r \neq 2$ or $r = 2$ and $t_2 > 1$. □

Remark 2. For $d = 2$ equation (13) yields $T(\theta^a) = (p-1)/2$ if $a \in P$ and similarly one then gets $T(\theta^a) = (q-1)/2$ if $a \in Q$. This leads to the formula presented in [7] for the linear complexity of the binary two-prime generator.

We observe that for Construction 2, in Theorem 1 we had to suppose that $r > 2$ or $t_i \ge 2$, $i = 1, 2$, which was used to show equation (15). However, to obtain a sequence over $\mathbb{F}_8$ with Construction 2 we have to choose $t_1 = 1$ (and $t_2 = 2$). Consequently sequences over $\mathbb{F}_8$ for Construction 2 are not covered by Theorem 1, thus have to be dealt with separately. This is accomplished in the next theorem. As basis of $\mathbb{F}_8$ over $\mathbb{F}_2$ we may choose the polynomial basis $\{1, \beta, \beta^2\}$, where β can be taken as a root of $x^3 + x + 1$.

Theorem 2. *The linear complexity of the sequence over $\mathbb{F}_8$ obtained by Construction 2 with $t_1 = 1, t_2 = 2$ and the polynomial basis $\{1, \beta, \beta^2\}$ of $\mathbb{F}_8$ over $\mathbb{F}_2$ is given by*

$$L(S) = \begin{cases} pq - p - \frac{(p-1)(q-1)}{8} & : \quad p \equiv 1 \mod 4,\ 2 \in D_0, \\ pq - p - q + 1 - \frac{(p-1)(q-1)}{8} & : \quad p \equiv 3 \mod 4,\ 2 \in D_0, \\ pq - p & : \quad p \equiv 1 \mod 4,\ 2 \notin D_0, \\ pq - p - q + 1 & : \quad p \equiv 3 \mod 4,\ 2 \notin D_0. \end{cases}$$

Proof. Since $r = 2$ and $t_1 = 1$ equation (15) now attains the value 1. Thus for equation (14) we obtain

$$T(\theta^a) = \frac{p-1}{2} \sum_{k=0}^{2^{t_2}-1} \sum_{i \in pD_k^{(q)}} \theta^i = \frac{p-1}{2} \sum_{i \in P} \theta^i = \frac{p-1}{2}.$$

As we had $U(\theta^a) = -1$ if $a \in P$ we therefore get $S(\theta^a) = (p+1)/2$ for all $a \in P$. With the observation that $8 \in D_0$ if and only if $2 \in D_0$, we obtain the assertion of the theorem. □

Remark 3. By definition of D_0 we have $2 \in D_0$ if and only if 2 is a quadratic residue modulo p and a quartic residue modulo q, or equivalently $p \equiv \pm 1 \bmod 8$ and $q \equiv -1 \bmod 8$ or $q \equiv 1 \bmod 8$ and $q = x^2 + 64y^2$ for some integers x, y. Thus one may write the statement of Theorem 2 entirely in terms of p and q.

4.2 Quaternary Sequences

If $\gcd(r, t) \neq 1$ then Lemma 2 cannot be applied and the values of $S(\theta^a)$ for $a \in \mathbb{Z}_{pq}^*$ have to be determined individually. We present the results for the linear complexity of sequences defined via the subgroups (9) and (11) for the important case $d = 4$. As we will see, for the subgroup (9) the linear complexity does not rely on a predefined ordering of the elements of $\mathbb{F}_4$, whereas for the subgroup (11) it does.

Theorem 3. *Let $\eta_0, \eta_1, \eta_2, \eta_3$ be the elements of $\mathbb{F}_4$, let D_j be defined as in (10) for two primes $p \equiv q \equiv 1 \bmod 4$ and $d = 4$, and let S be the pq-periodic sequence over $\mathbb{F}_4$ defined by*

$$s_n = \begin{cases} \eta_j & : \quad n \in D_j, \\ 0 & : \quad n \in Q \cup \{0\}, \\ 1 & : \quad n \in P. \end{cases}$$

The linear complexity $L(S)$ of S is then

$$L(S) = \begin{cases} pq - p - \frac{(p-1)(q-1)}{4} & : \quad p \equiv q \equiv 1 \bmod 8 \text{ or } p \equiv q \equiv 5 \bmod 8, \\ pq - p & : \quad p \equiv 1 \bmod 8, q \equiv 5 \bmod 8 \text{ or} \\ & \quad\ \ p \equiv 5 \bmod 8, q \equiv 1 \bmod 8. \end{cases}$$

Proof. With Lemma 1(i) and $aP = P$ for $a \in \mathbb{Z}_{pq}^*$ we have $S(\theta^a) = S(\theta)$ for all $a \in D_0$. Defining $U(x), T(x)$ as in equation (5) we observe that again $U(\theta^a) = U(\theta) = 1$ if $a \in \mathbb{Z}_{pq}^* \cup P$ and $U(\theta^a) = 0$ if $a \in Q$. We hence restrict ourselves to the determination of $T(\theta^a)$. From $\mathbb{Z}_{pq}^*/D_0$ being cyclic we get for $a \in D_1$

$$\begin{aligned} T(\theta^a) &= \sum_{j=0}^{3} \eta_j f_j(\theta^a) = \eta_3 f_0(\theta) + \eta_0 f_1(\theta) + \eta_1 f_2(\theta) + \eta_2 f_3(\theta) \\ &= T(\theta) + (\eta_0 + \eta_3) f_0(\theta) + (\eta_0 + \eta_1) f_1(\theta) + (\eta_1 + \eta_2) f_2(\theta) + (\eta_2 + \eta_3) f_3(\theta) \\ &= T(\theta) + (\eta_0 + \eta_3)(f_0(\theta) + f_2(\theta)) + (\eta_0 + \eta_1)(f_1(\theta) + f_3(\theta)), \end{aligned}$$

since $\sum_{j=0}^{3} \eta_j = 0$. With Lemma 1(iv) we then obtain

$$T(\theta^a) = T(\theta) + \eta_0 + \eta_1 + (\eta_1 + \eta_3)(f_0(\theta) + f_2(\theta)).$$

With similar arguments one gets $T(\theta^a) = T(\theta) + \eta_0 + \eta_2$ if $a \in D_2$, and $T(\theta^a) = T(\theta) + \eta_0 + \eta_3 + (\eta_1 + \eta_3)(f_0(\theta) + f_2(\theta))$ if $a \in D_3$.
$T(\theta^a) = 0$ if $a \in P \cup Q$, thus $S(\theta^a) = 1$ if $a \in P$ and $S(\theta^a) = 0$ if $a \in Q$, follows with the proof of Theorem 1 for the general case. We distinguish two cases.

First suppose that $2 \in D_0 \cup D_2$, or equivalently $p \equiv q \bmod 8$, then $4 \in D_0$ and thus $S(\theta) \in \mathbb{F}_4$. Furthermore observe that $2 \in D_0 \cup D_2$ also implies $f_0(\theta) + f_2(\theta) \in \mathbb{F}_2$. As easily seen we then have $S(\theta^a) \neq S(\theta^{a'})$ if $a \not\equiv a' \bmod D_0$ and we obtain the proclaimed value for the linear complexity with the usual conclusion.

Secondly suppose that $2 \in D_1 \cup D_3$, hence $4 \in D_2$. Then $S(\theta)^4 = S(\theta^4) = S(\theta) + \eta_0 + \eta_2 \neq S(\theta)$, and consequently $S(\theta) \notin \mathbb{F}_4$. On the other hand again $4 \in D_2$ implies $f_0(\theta) + f_2(\theta) \in \mathbb{F}_4$ and thus $S(\theta^a) \notin \mathbb{F}_4$ for all $a \in \mathbb{Z}_{pq}^*$, which yields the proclaimed linear complexity. □

Theorem 4. *Let $\eta_0, \eta_1, \eta_2, \eta_3$ be the elements of $\mathbb{F}_4$ and for two odd primes p, q let $D_0^{(p)}$ and $D_1^{(p)}$ ($D_0^{(q)}$, $D_1^{(q)}$) be the set of squares and nonsquares modulo p (modulo q), respectively. Let S be the pq-periodic sequence over $\mathbb{F}_4$ defined by*

$$s_n = \begin{cases} \eta_{l+2k} & : \ n \in D_l^{(p)} \sqcap D_k^{(q)}, \\ 0 & : \ n \in Q \cup \{0\}, \\ 1 & : \ n \in P. \end{cases}$$

The linear complexity of S is then

$$L(S) = \begin{cases} pq - 1 - \frac{(p-1)(q-1)}{4} & : \ q \equiv 3 \bmod 4 \text{ and } p \equiv 1 \bmod 4 \text{ or} \\ & \quad p \equiv 3 \bmod 4, \eta_2 \neq \eta_0 + 1, \\ pq - p - \frac{(p-1)(q-1)}{4} & : \ q \equiv 1 \bmod 4 \text{ and } p \equiv 1 \bmod 4 \text{ or} \\ & \quad p \equiv 3 \bmod 4, \eta_2 \neq \eta_0 + 1, \\ pq - q - \frac{(p-1)(q-1)}{4} & : \ q \equiv 3 \bmod 4, p \equiv 3 \bmod 4, \eta_2 = \eta_0 + 1, \\ pq - p - q + 1 - \frac{(p-1)(q-1)}{4} & : \ q \equiv 1 \bmod 4, p \equiv 3 \bmod 4, \eta_2 = \eta_0 + 1. \end{cases}$$

Proof. With Lemma 1(i) and $aP = P$ for $a \in \mathbb{Z}_{pq}^*$ we have $S(\theta^a) = S(\theta)$ for all $a \in D_0$. From $\mathbb{Z}_{pq}^*/D_0 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, for $a \in D_1$ we obtain

$$\begin{aligned} S(\theta^a) &= \sum_{n \in P} \theta^n + \eta_0 f_1(\theta) + \eta_1 f_0(\theta) + \eta_2 f_3(\theta) + \eta_3 f_2(\theta) = S(\theta) + \eta_0(f_0(\theta) + f_1(\theta)) \\ &\quad + \eta_1(f_0(\theta) + f_1(\theta)) + \eta_2(f_2(\theta) + f_3(\theta)) + \eta_3(f_2(\theta) + f_3(\theta)) \\ &= S(\theta) + (\eta_0 + \eta_1)(f_0(\theta) + f_1(\theta)) + (\eta_2 + \eta_3)(f_2(\theta) + f_3(\theta)) \\ &= S(\theta) + (\eta_0 + \eta_1) \sum_{j=0}^{3} f_j(\theta) = S(\theta) + \eta_0 + \eta_1. \end{aligned}$$

Similarly we get $S(\theta^a) = S(\theta) + \eta_0 + \eta_2$ for $a \in D_2$ and $S(\theta^a) = S(\theta) + \eta_0 + \eta_3$ for $a \in D_3$. Hence $S(\theta^a) \neq S(\theta^{a'})$ if $a \not\equiv a' \bmod D_0$. Since $4 \in D_0$ and $U(x)$

is as in the proof of Theorem 3, with Lemma 1(ii) we have $S(\theta^a) \in \mathbb{F}_4$ when $a \in D_j, j = 0, 1, 2, 3$.

Employing that the sets D_0 and D_2 (D_1 and D_3) reduced modulo q are equal for $a \in P$ we get

$$\begin{aligned} S(\theta^a) &= \sum_{n\in P} \theta^n + (\eta_0+\eta_2) \sum_{n\in D_0} \theta^{an} + (\eta_1+\eta_3) \sum_{n\in D_1} \theta^{an} \\ &= 1 + (\eta_0+\eta_2) \sum_{n\in D_0\cup D_1} \theta^{an} = 1 + (\eta_0+\eta_2)\frac{p-1}{2} \sum_{n\in P} \theta^n \\ &= 1 + (\eta_0+\eta_2)\frac{p-1}{2}. \end{aligned}$$

In the penultimate step we used that the set $D_0 \cup D_1$ reduced modulo q contains all elements of $\mathbb{Z}_q^*$ and each element is taken on $(p-1)/2$ times.

In an analog way we obtain $S(\theta^a) = (\eta_0+\eta_1)\frac{q-1}{2}$ if $a \in Q$. The simple observation that $S(1) = 0$ completes the proof. □

We complete this section pointing out that the generalized two-prime generator (Construction 1) has favourable autocorrelation properties when d is prime (or likewise if one defines the sequence as a d-ary sequence for an arbitrary module d in an analog way, as autocorrelation is then also defined). For $d = 2$ this was shown in [8], an alternative proof using characters was presented in [2]. The methods of [2] can be applied to the case of arbitrary modules d. As far as we are aware, autocorrelation results for arbitrary modules d have not been presented, thus we give the result but omit the proof. In the following we put $\varepsilon_d = e^{2\pi\sqrt{-1}/d}$, and $\chi^{(p)}$ ($\chi^{(q)}$) shall denote the multiplicative character of order d of $\mathbb{F}_p$ ($\mathbb{F}_q$) given by $\chi^{(p)}(g^k) = \varepsilon_d^k$ if g is a primitive element of $\mathbb{F}_p$ ($\mathbb{F}_q$).

Theorem 5. *The autocorrelation of the generalized two-prime generator S with prime d is given by*

$$A(S,t) = \begin{cases} p-q+1 & : \quad t \in q\mathbb{Z}_p^*, \\ \varepsilon_d + \overline{\varepsilon_d} + q - p - 1 & : \quad t \in p\mathbb{Z}_q^*, \\ 1 + (1-\overline{\varepsilon}\chi^{(p)}(-t)\chi^{(q)}(-t)) & : \quad t \in \mathbb{Z}_{pq}^*. \\ \quad +(1-\varepsilon\overline{\chi^{(p)}}(t)\overline{\chi^{(q)}}(t)) & \end{cases}$$

5 Final Remarks

We consider N-periodic sequences over finite fields that are constant on the cosets of a subgroup of $\mathbb{Z}_N^*$, which can be seen as a general approach to classes of N-periodic sequences that contain well known constructions as the Legendre sequences and the two-prime generator. With this general approach one may construct and analyse various classes of sequences. We give examples of pq-periodic sequences over arbitrary finite fields and determine their linear complexity. Similar constructions can be considered and analysed (using tools from Section 2) for other (squarefree) periods. One may use subgroups D of $\mathbb{Z}_N^*$ with index not

a prime power as in the following example: For an odd prime p and a prime $q \equiv 1 \bmod 3$ we consider the cyclotomic classes of order 2 and 3, respectively, and the subgroup $D_0 = D_0^{(q)} \sqcap D_0^{(p)}$ of index 6. We define a corresponding ternary sequence S by $s_n = l + 2k \bmod 3$ if $n \in D_l^{(p)} \sqcap D_k^{(q)}$, $s_n = 0$ if $n \in Q \cup \{0\}$ and $s_n = 1$ if $n \in P$. With the above used techniques and using Proposition 1 one obtains that $L(S) = pq - p - (p-1)(q-1)/3$ if $p \equiv \pm 1 \bmod 12$ and $q = 3a^2 + b^2$ with $9|a$ or $9|(a \pm b)$, if $q = 3a^2 + b^2$ with $9 \not| a$ and $9 \not| (a \pm b)$ then $L(S) = pq - p$. This pq-periodic ternary sequence is certainly different from the ternary version of the two-prime generator and the ternary sequence constructed as in [12]. An analysis of the autocorrelation of such coset sequences, which differently to the sequences in [1,12,14,15,16] are not similar to a concatenation of Legendre sequences, may be worthwhile. There, an adaptation of the method in [8] with an adequate generalization of cyclotomic numbers seems promising. In this connection it may also be of interest to use the above considered factor group of $\mathbb{Z}_{pq}^*$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ to define quaternary sequences.

References

1. Bai, E., Liu, X., Xiao, G.: Linear complexity of new generalized cyclotomic sequences of order two of length pq. IEEE Trans. Inform. Theory 51, 1849–1853 (2005)
2. Brandstätter, N., Winterhof, A.: Some notes on the two-prime generator of order 2. IEEE Trans. Inform. Theory 51, 3654–3657 (2005)
3. Cusick, T.W., Ding, C., Renvall, A.: Stream Ciphers and Number Theory. North-Holland Publishing Co., Amsterdam (1998)
4. Dai, Z., Yang, J., Gong, G., Wang, P.: On the linear complexity of generalized Legendre sequences. In: Sequences and their Applications, 145–153 (2001); Discrete Math. Theor. Comput. Sci. (Lond.). Springer, London (2002)
5. Ding, C., Helleseth, T., Shan, W.: On the linear complexity of Legendre sequences. IEEE Trans. Inform. Theory 44, 1276–1278 (1998)
6. Ding, C., Helleseth, T.: On cyclotomic generator of order r. Inform. Process. Letters 66, 21–25 (1998)
7. Ding, C.: Linear complexity of generalized cyclotomic binary sequences of order 2. Finite Fields Appl. 3, 159–174 (1997)
8. Ding, C.: Autocorrelation values of generalized cyclotomic sequences of order two. IEEE Trans. Inform. Theory 44, 1699–1702 (1998)
9. Green, D., Garcia-Perera, L.: The linear complexity of related prime sequences. Proc. R. Soc. Lond. A 460, 487–498 (2004)
10. Kim, J.-H., Song, H.-Y.: On the linear complexity of Hall's sextic residue sequences. IEEE Trans. Inform. Theory 47, 2094–2096 (2001)
11. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and their Applications. Cambridge University Press, Cambridge (1986)
12. Meidl, W.: Remarks on a cyclotomic sequence. Designs, Codes and Cryptography 51, 33–43 (2009)

13. Niederreiter, H.: Linear complexity and related complexity measures for sequences. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 1–17. Springer, Heidelberg (2003)
14. Yan, T., Li, S., Xiao, G.: On the linear complexity of generalized cyclotomic sequences with the period p^m. Appl. Math. Lett. 21, 187–193 (2008)
15. Yan, T., Chen, Z., Xiao, G.: Linear complexity of Ding generalized cyclotomic sequences. Journal of Shanghai University (English Edition) 11, 22–26 (2007)
16. Zhang, J., Zhao, C.A., Ma, X.: Linear complexity of generalized cyclotomic sequences with length $2p^m$. AAECC 21, 93–108 (2010)

On the Autocorrelation and the Linear Complexity of q-Ary Prime n-Square Sequences*

Fang Liu, Daiyuan Peng, Xiaohu Tang, and Xianhua Niu

Key Laboratory of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, Sichuan, 610031, P.R. China
hmimy5416@163.com, dypeng@swjtu.edu.cn, xhutang@ieee.org, rurustef1212@gmail.com

Abstract. Cryptographically strong sequences should have long periods, large linear complexity, low correlation, and balance properties. In this paper, we determine the autocorrelation of the q-ary prime n-square sequences with length p^n, where p is an odd prime, n is a positive integer and q is a divisor of $p-1$. When q is a prime, we also determine the linear complexity of the prime n-square sequences over the prime field F_q. It is shown that these sequences have good linear complexity and balance properties, but don't have desirable autocorrelation properties.

Keywords: Generalized cyclotomy, prime n-square sequence, autocorrelation, linear complexity, balance.

1 Introduction

For cryptographic applications, pseudo-random sequences are required to have the property of unpredictability. Balance and linear complexity are two main components that indicate this feature. The linear complexity of a sequence is defined as the length of the shortest linear feedback shift register (LFSR) that can generate the sequence. By the Berlekamp-Massey algorithm [1], for a sequence $s^\infty = (s(0), s(1), \cdots)$ with the least period N, if the linear complexity $L(s^\infty)$ of s^∞ is larger than $N/2$, then s^∞ is considered good with respect to its linear complexity. It has been reported that certain cyclotomic sequences possess good linear complexity [2,3,5,6,7,8,9,10,11].

A generalized cyclotomy with respect to $p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ was introduced by Ding and Helleseth [4] in 1998, where $p_1, p_2, \cdots, p_t$ are distinct odd primes and $e_1, e_2, \cdots, e_t$ are positive integers, which includes classical cyclotomy [13] as a special case. Since the generalized cyclotomy in [4] is different from that defined by Whiteman [14], we call it DH generalized cyclotomy in this paper. Some DH generalized cyclotomic sequences have good linear complexity [7,8,9,10,11]. In 2007, Yan *et al.* [7] computed the linear complexity and autocorrelation of the

* This work was supported by the National Science Foundation of China (Grant No. 60872015 and 60772086).

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 139–150, 2010.

binary DH generalized cyclotomic sequences of order 2 with respect to p^2, where p is an odd prime. Meanwhile, in 2007, Kim *et al.* [9] computed the linear complexity and autocorrelation of the binary DH generalized cyclotomic sequences of order 2 with respect to p^3. Recently, Kim *et al.* [10] computed the linear complexity of the binary DH generalized cyclotomic sequences of order 2 with respect to p^n for any positive integer n, which are called prime n-square sequences of order 2.

In this paper, we determine the autocorrelation of the q-ary prime n-square sequences of period p^n, where q is a divisor of $p-1$. When q is a prime, we determine the linear complexity of the prime n-square sequences over the prime field F_q. The results of this paper show that these sequences have good linear complexity.

2 q-Ary Prime n-Square Sequences

For any positive integer N, Z_N^* denotes the set of all invertible elements of the residue class ring Z_N. Let H be a subset of Z_N and let a be an element of Z_N. Define

$$H + a = \{h + a : h \in H\}, \qquad a \cdot H = \{a \cdot h : h \in H\}.$$

where " $+$ " and " $\cdot$ " denote the integer addition modulo N and integer multiplication modulo N, respectively.

Let p be an odd prime and g be a primitive root of $Z_{p^2}^*$. Then it is known that g is also a primitive root of $Z_{p^n}^*$ for $n \geq 1$ [1]. Let q be a divisor of $p-1$. Define $D_0^{(q,p^k)} = \langle g^q \rangle (\bmod\ p^k)$, the cyclic group generated by g^q modulo p^k and $D_i^{(q,p^k)} = g^i D_0^{(q,p^k)} (\bmod\ p^k)$ for $1 \leq i \leq q-1$. Obviously, $Z_{p^n}^* = \bigcup_{i=0}^{q-1} D_i^{(q,p^n)}$. Denote $pZ_{p^{k-1}} = \{0, p, \cdots, p(p^{k-1}-1)\}$, then $Z_{p^k} = Z_{p^k}^* \cup pZ_{p^{k-1}}$. It is easy to verify that [4]

$$Z_{p^n} = \Big(\bigcup_{k=1}^{n} p^{n-k} D_0^{(q,p^k)}\Big) \bigcup \Big(\bigcup_{k=1}^{n} p^{n-k} D_1^{(q,p^k)}\Big) \bigcup \cdots \bigcup \Big(\bigcup_{k=1}^{n} p^{n-k} D_{q-1}^{(q,p^k)}\Big) \bigcup \{0\}.$$

Lemma 1. *If* $a \in D_i^{(q,p^k)}$, *then* $aD_j^{(q,p^k)} = D_{i+j(\bmod q)}^{(q,p^k)} (\bmod\ p^k)$, *where* $0 \leq i, j \leq q-1$ *and* $1 \leq k \leq n$.

Proof. The proof is obvious. □

Lemma 2. *Given an integer* b, *then* $D_i^{(q,p^k)} + bp = D_i^{(q,p^k)} (\bmod\ p^k)$ *for* $0 \leq i \leq q-1$ *and* $1 \leq k \leq n$.

Proof. Note that every element of $D_i^{(q,p^k)} + bp$ is not a multiple of p and is relatively prime to p^k for each i , i.e., $D_i^{(q,p^k)} + bp \in Z_{p^k}^*$.

Suppose that $(D_i^{(q,p^k)} + bp) \cap D_j^{(q,p^k)} \neq \emptyset$ for $0 \leq i \neq j \leq q-1$. Then, there exist two integers s, t such that $g^{qs+i} + bp = g^{qt+j} \pmod{p^k}$, i.e.,

$$g^{qs+i} \equiv g^{qt+j} \pmod{p}.$$

This implies $g^{q(s-t)+i-j} \equiv 1 (\mathrm{mod}\ p)$, which contradicts the fact that the order of g modulo p is $p-1=qf$, a multiple of q.

That is, $D_i^{(q,p^k)} + bp \in Z_{p^k}^* \setminus \{\cup_{j \neq i} D_j^{(q,p^k)}\} = D_i^{(q,p^k)}$. Hence, $D_i^{(q,p^k)} + bp = D_i^{(q,p^k)}$ immediately follows from $|D_i^{(q,p^k)} + bp| = |D_i^{(q,p^k)}|$. □

Define

$$C_i = \left(\bigcup_{k=1}^{n} p^{n-k} D_i^{(q,p^k)} \right) \text{ for } 0 \leq i \leq q-2,$$

$$C_{q-1} = \left(\bigcup_{k=1}^{n} p^{n-k} D_{q-1}^{(q,p^k)} \right) \bigcup \{0\}.$$

Obviously, $C_i \cap C_j = \emptyset$ for $i \neq j$ and $\bigcup_{i=0}^{q-1} C_i = Z_{p^n}$.

The q-ary prime n-square sequence $\mathbf{s} = \{s(0), s(1), \cdots, s(p^n-1)\}$ of period p^n is defined as follows,

$$s(t) = i, \text{ if } (t \bmod p^n) \in C_i. \tag{1}$$

Note that the sequence $\mathbf{s}$ has the least period $N = p^n$, in which there are $(p^n-1)/q$ i's for each $0 \leq i \leq q-2$ and $(p^n-1)/q+1$ $q-1$'s. Therefore, it is balanced.

3 The Autocorrelation of the q-Ary Prime n-Square Sequences

The periodic autocorrelation function $R_{\mathbf{s}}(\tau)$ of a q-ary sequence $\mathbf{s}$ with period N is defined by

$$R_{\mathbf{s}}(\tau) = \sum_{t=0}^{N-1} w^{s(t)-s(t+\tau)}, \tag{2}$$

where w is a complex primitive qth root of unity.

The following definition and lemmas are very useful to calculate the autocorrelation of $\mathbf{s}$.

Definition 1 ([12]). *Let $p = qf+1$ be an odd prime and g be a primitive root modulo p. A sequence $\mathbf{u} = \{u(0), u(1), \cdots, u(p-1)\}$ of length p, defined by*

$$u(t) = \begin{cases} 0, \text{ if } (t \bmod p) = 0 \\ j, \text{ if } (t \bmod p) \in C'_j, \end{cases} \tag{3}$$

is called a q-ary power residue sequence, where $C'_0 = \langle g^q \rangle \ (\mathrm{mod}\ p)$, the cyclic group generalized by g^q modulo p, and $C'_j = g^j C'_0$ for $0 \leq j \leq q-1$.

Lemma 3 ([12]). *The autocorrelation of the q-ary power residue sequence $\mathbf{u}$ of period $p = qf+1$ is as follows,*

1). If f is even,

$$R_{\mathbf{u}}(\tau) = \begin{cases} p, & \text{if } \tau = 0 \\ -1 + w^k + w^{-k}, & \text{if } \tau \in C'_k, \end{cases} \tag{4}$$

2). If f is odd,

$$R_{\mathbf{u}}(\tau) = \begin{cases} p, & \text{if } \tau = 0 \\ -1 + w^{-k} - w^k, & \text{if } \tau \in C'_k. \end{cases} \tag{5}$$

Lemma 4. *Let $p = qf+1$ be an odd prime. If f is even, $-1(\bmod\ p^k) \in D_0^{(q,p^k)}$. If f is odd, $-1(\bmod\ p^k) \in D_{\frac{q}{2}}^{(q,p^k)}$ for $k = 1, 2, \cdots, n$.*

Proof. It can be proved in the same way as [10]. □

Theorem 1. *Let $p = qf + 1$ be an odd prime. The autocorrelation of the q-ary prime n-square sequence $\mathbf{s}$ defined in (1) of period p^n is as follows,*

1). If f is even,

$$R_{\mathbf{s}}(\tau) = \begin{cases} p^n, & \text{if } \tau = 0 \\ w^{-1-a} + w^{a+1} + p^n - p^k - p^{k-1}, & \text{if } \tau \in p^{n-k} D_a^{(q,p^k)}; \end{cases} \tag{6}$$

2). If f is odd,

$$R_{\mathbf{s}}(\tau) = \begin{cases} p^n, & \text{if } \tau = 0 \\ w^{-1-a} - w^{a+1} + p^n - p^k - p^{k-1}, & \text{if } \tau \in p^{n-k} D_a^{(q,p^k)}, \end{cases} \tag{7}$$

where $0 \le a \le q-1$ and $1 \le k \le n$.

Proof. For the case $\tau \equiv 0(\bmod\ p^n)$,

$$R_{\mathbf{s}}(0) = \sum_{t=0}^{p^n-1} w^0 = p^n.$$

When $\tau \in p^{n-k} D_a^{(q,p^k)}$ for $0 \le a \le q-1$ and $1 \le k \le n$, we have

$$\begin{aligned} R_{\mathbf{s}}(\tau) &= \sum_{t=0}^{p^n-1} w^{s(t)-s(t+\tau)} \\ &= w^{q-1-a} + \sum_{r=0}^{q-1} \sum_{t \in D_r^{(q,p^n)}} w^{s(t)-s(t+\tau)} + \sum_{r=0}^{q-1} \sum_{t \in pD_r^{(q,p^{n-1})}} w^{s(t)-s(t+\tau)} + \cdots \\ &\quad + \sum_{r=0}^{q-1} \sum_{t \in p^{n-1} D_r^{(q,p)}} w^{s(t)-s(t+\tau)}, \end{aligned}$$

where we use $s(0) = q-1$ and $s(\tau) = a$. Let $\tau = p^{n-k}b$, where $b \in D_a^{(q,p^k)}$. Note that $p^{n-j}D_r^{(q,p^j)} + p^{n-k}b = p^{n-j}(D_r^{(q,p^j)} + p^{j-k}b)$ for $j = k+1, k+2, \cdots, n$. By Lemma 2, $D_r^{(q,p^j)} + p^{j-k}b = D_r^{(q,p^j)} (\mathrm{mod} p^j)$. Thus, $p^{n-j}D_r^{(q,p^j)} + \tau = p^{n-j}D_r^{(q,p^j)}$ for $j = k+1, k+2, \cdots, n$. Therefore, we have

$$\sum_{r=0}^{q-1} \sum_{t \in p^{n-j} D_r^{(q,p^j)}} w^{s(t)-s(t+\tau)} = \sum_{r=0}^{q-1} \sum_{t \in p^{n-j} D_r^{(q,p^j)}} w^0 = p^{j-1}(p-1) \tag{8}$$

for $j = k+1, k+2, \cdots, n$, where we use the facts that $|p^{n-j}Z_{p^j}^*| = p^{j-1}(p-1)$ and $\bigcup_{r=0}^{q-1} p^{n-j}D_r^{(q,p^j)} = p^{n-j}Z_{p^j}^*$.

Similarly, $p^{n-j}D_r^{(q,p^j)} + \tau = p^{n-k}(p^{k-j}D_r^{(q,p^j)} + b) \subset p^{n-k}D_a^{(q,p^k)}$ for $j = 1, 2, \cdots, k-1$. Hence,

$$\begin{aligned} \sum_{r=0}^{q-1} \sum_{t \in p^{n-j} D_r^{(q,p^j)}} w^{s(t)-s(t+\tau)} &= \sum_{r=0}^{q-1} \sum_{t \in p^{n-j} D_r^{(q,p^j)}} w^{s(t)-a} \\ &= w^{-a} \frac{p^{j-1}(p-1)}{q} \sum_{r=0}^{q-1} w^r = 0 \end{aligned} \tag{9}$$

for $j = 1, 2, \cdots, k-1$.

By (8) and (9), we have

$$\begin{aligned} R_{\mathbf{s}}(\tau) &= w^{q-1-a} + p^{n-1}(p-1) + \cdots + p^k(p-1) + \sum_{r=0}^{q-1} \sum_{t \in p^{n-k} D_r^{(q,p^k)}} w^{s(t)-s(t+\tau)} + 0 \\ &= w^{q-1-a} + p^n - p^k + \sum_{r=0}^{q-1} \sum_{t \in p^{n-k} D_r^{(q,p^k)}} w^{s(t)-s(t+\tau)}. \end{aligned} \tag{10}$$

Let

$$A(\tau) = \sum_{r=0}^{q-1} \sum_{t \in p^{n-k} D_r^{(q,p^k)}} w^{s(t)-s(t+\tau)}.$$

Note that [4],

$$D_r^{(q,p^k)} (\mathrm{mod}\ p) = \{\underbrace{x, \cdots, x}_{p^{k-1}} : x \in D_r^{(q,p)}\}. \tag{11}$$

From Lemma 1 and Lemma 4, $-b \pmod{p^k} \in D_a^{(q,p^k)}$ if f is even and $-b \pmod{p^k} \in D_{a+\frac{q}{2}(\mathrm{mod}\ q)}^{(q,p^k)}$ if f is odd. By (11), there exist p^{k-1} c's in $D_{a+v}^{(q,p^k)}$ such that $c \equiv -b (\mathrm{mod}\ p)$ and 0 c's in $Z_{p^k}^* \setminus D_{a+v}^{(q,p^k)}$ such that $c \equiv -b (\mathrm{mod}\ p)$, where

$v = 0$ if f is even, and $v = q/2$, otherwise. Let $\tau' = p^{n-1} \cdot (b \bmod p)$ and $\Delta = \{p^{n-k}c : c \in D^{(q,p^k)}_{a+v(\bmod q)} \text{ and } c \equiv -b(\bmod p)\}$, i.e., Δ is such a set that $\forall\ p^{n-k}c \in \Delta$, $p^{n-1} \cdot (c \bmod p) = -\tau'$. Then,

$$A(\tau) = p^{k-1}\left(\sum_{r=0}^{q-1} \sum_{\substack{t \in p^{n-1}D^{(q,p)}_r, \\ t \neq -\tau'}} w^{s(t)-s(t+\tau')}\right) + \sum_{t \in \Delta} w^{s(t)-s(t+\tau)}, \tag{12}$$

which is from the fact that $s(t) = s(t')$ when $t = p^{n-j}c \in p^{n-j}D^{(q,p^j)}_r$ and $t' = p^{n-1} \cdot (c \bmod p)$ for $j = 1, 2, \cdots, n$ and $r = 0, 1, \cdots, q-1$.

Note that, $\forall\ p^{n-k}c \in \Delta$, $p^{n-k}c + p^{n-k}b \equiv 0(\bmod\ p^{n-k+1})$ from $c + b \equiv 0(\bmod\ p)$. Therefore, when $t \in \Delta$, $t + \tau$ is a multiple of p^{n-k+1}. Thus, when t ranges over Δ, $t+\tau$ enumerates every element of $p^{n-k+1}Z_{p^{k-1}}$ exactly once from $|Z_{p^{k-1}}| = p^{k-1}$. Therefore, we have

$$\begin{aligned} A(\tau) = p^{k-1}\Bigg(&\sum_{r=0}^{q-1} \sum_{\substack{t \in p^{n-1}D^{(q,p)}_r, \\ t \neq -\tau'}} w^{s(t)-s(t+\tau')} + w^{-s(\tau')} + w^{s(-\tau')} \\ &- w^{-s(\tau')} - w^{s(-\tau')}\Bigg) + w^{a+v} \sum_{t \in p^{n-k+1}Z_{p^{k-1}}} w^{-s(t)} \\ = p^{k-1}&R_{\mathbf{u}}(\delta) - p^{k-1}(w^{-a} + w^{a+v}) + w^{a+v-(q-1)}, \end{aligned} \tag{13}$$

where the second equality is from Definition 1 and the balanced property of $\mathbf{s}$, $\delta \equiv b(\bmod\ p)$, and $R_{\mathbf{u}}(\delta)$ denotes the autocorrelation of the q-ary power residue sequence $\mathbf{u}$ of period p.

By (13), (10) can be simplified as follows,

$$\begin{aligned} R_{\mathbf{s}}(\tau) &= w^{q-1-a} + p^n - p^k + p^{k-1}R_{\mathbf{u}}(\delta) - p^{k-1}(w^{-a} + w^{a+v}) + w^{a+v-(q-1)} \\ &= w^{-1-a} + p^n - p^k + p^{k-1}R_{\mathbf{u}}(\delta) - p^{k-1}(w^{-a} + w^{a+v}) + w^{a+v+1}, \end{aligned} \tag{14}$$

where $w^q = 1$.

Note that $w^{\frac{q}{2}} = -1$. Thus, combining Lemma 3 and (14), the conclusion follows. □

4 The Linear Complexity of the Prime n-Square Sequence over the Prime Field F_q

Let $p = qf + 1$ with q a prime and F_{q^m} be a finite field with q^m elements. In this section, we will determine the linear complexity of the prime n-square sequence $\mathbf{s}$ over the prime field F_q.

Definition 2. *If a sequence* $\mathbf{s} = \{s(0), s(1), \cdots, s(N-1)\}$ *over the finite field* F_q *of length* N *has linear complexity* L, *then there exist constants* $c_0 = 1, c_1, \cdots, c_L \in F_q$ *such that*

$$s(t) = c_1 s(t-1) + c_2 s(t-2) + \cdots + c_L s(t-L), \text{ for } L \leq t \leq N-1.$$

The polynomial $c(x)=c_0+c_1x+\cdots+c_Lx^L$ *is called the minimal polynomial of* $\mathbf{s}$.

The characteristic polynomial of $\mathbf{s}$ is defined as

$$S(x) = s(0) + s(1)x + \cdots + s(N-1)x^{N-1}. \tag{15}$$

It is well known that [15]

1). The minimal polynomial of $\mathbf{s}$ is given by

$$c(x) = (x^N - 1)/\gcd(x^N - 1, S(x)); \tag{16}$$

2). The linear complexity of $\mathbf{s}$ is given by

$$C_N = N - \deg(\gcd(x^N - 1, S(x))). \tag{17}$$

Let m be the order of q modulo p^n and θ be a primitive p^nth root of unity in F_{q^m}. By (17), the linear complexity of $\mathbf{s}$ defined in (1) is

$$L(\mathbf{s}) = p^n - |\{a : S(\theta^a) = 0, 0 \le a \le p^n - 1\}|. \tag{18}$$

From now on, all calculations are performed in F_{q^m}. Note that, for $k = 1, 2, \cdots, n$,

$$\begin{aligned}\theta^{p^n} - 1 &= (\theta^{p^{n-k}} - 1)(1 + \theta^{p^{n-k}} + \theta^{2p^{n-k}} + \cdots + \theta^{(p^k-1)p^{n-k}}) \\ &= \left(\theta^{p^{n-k}} - 1\right)\left(1 + \sum_{j=1}^{k} \sum_{i \in p^{n-j} Z_{p^j}^*} \theta^i\right) \\ &= 0.\end{aligned}$$

Thus,

$$1 + \sum_{j=1}^{k} \sum_{i \in p^{n-j} Z_{p^j}^*} \theta^i = 0. \tag{19}$$

When $k = 1$, we have

$$1 + \sum_{i \in p^{n-1} Z_p^*} \theta^i = 0. \tag{20}$$

From (19) and (20), we can derive that

$$\sum_{i \in p^{n-k} Z_{p^k}^*} \theta^i = 0 \tag{21}$$

for $k = 2, 3, \cdots, n$.

Now we define the index of $i \in Z_{p^n} \setminus \{0\}$ by

$$ind_{g,q}(i) = j \text{ if } i \in C_j.$$

From the definition of $S(x)$ in (15), the characteristic polynomial of $\mathbf{s}$ is as follows,

$$S(x)=q-1+\sum_{i\in Z_{p^n}^*} ind_{g,q}(i)x^i+\sum_{i\in pZ_{p^{n-1}}^*} ind_{g,q}(i)x^i+\cdots+\sum_{i\in p^{n-1}Z_p^*} ind_{g,q}(i)x^i.$$

When $q=2$, the sequence $\mathbf{s}$ defined in (1) coincides with that considered in [10] and the linear complexity of the binary prime n-square sequence of order 2 has been determined by Kim *et al.* [10]. Therefore, we only consider the case $q>2$.

Definition 3. *For $k=1,2,\cdots,n$, let $t_k(\theta)$ be defined as follows,*

$$t_k(\theta)=\sum_{i\in p^{n-k}Z_{p^k}^*} ind_{g,q}(i)\theta^i+\sum_{i\in p^{n-k+1}Z_{p^{k-1}}^*} ind_{g,q}(i)\theta^i+\cdots+\sum_{i\in p^{n-1}Z_p^*} ind_{g,q}(i)\theta^i. \quad (22)$$

Lemma 5. *$t_k(\theta)\in F_q$ if and only if $q\in D_0^{(q,p^n)}$ for $k=1,2,\cdots,n$.*

Proof. Note that

$$t_k(\theta)^q=t_k(\theta^q)=\sum_{i\in p^{n-k}Z_{p^k}^*} ind_{g,q}(i)\theta^{qi}+\cdots+\sum_{i\in p^{n-1}Z_p^*} ind_{g,q}(i)\theta^{qi}.$$

For $q\in Z_{p^n}^*$, there exists an inverse $q^{-1}\in Z_{p^n}^*$ of q such that $q^{-1}q\equiv 1(\mathrm{mod}\ p^n)$. Assume $q\in D_u^{(q,p^n)}$, then $q^{-1}\in D_{-u(\mathrm{mod}\ q)}^{(q,p^n)}$. Note that $q^{-1}D_v^{(q,p^j)}(\mathrm{mod}\ p^j)=D_{v-u(\mathrm{mod}\ q)}^{(q,p^j)}(\mathrm{mod}\ p^j)$ for $j=1,2,\cdots,n$. Then,

$$q^{-1}p^{n-j}D_v^{(q,p^j)}=p^{n-j}D_{v-u(\mathrm{mod}\ q)}^{(q,p^j)}.$$

Hence, we have $ind_{g,q}(q^{-1}i)=ind_{g,q}(i)-ind_{g,q}(q)$. Thus,

$$\begin{aligned}
t_k(\theta)^q &= \sum_{i\in p^{n-k}Z_{p^k}^*} ind_{g,q}(q^{-1}i)\theta^i+\cdots+\sum_{i\in p^{n-1}Z_p^*} ind_{g,q}(q^{-1}i)\theta^i\\
&= \sum_{i\in p^{n-k}Z_{p^k}^*} ind_{g,q}(i)\theta^i+\cdots+\sum_{i\in p^{n-1}Z_p^*} ind_{g,q}(i)\theta^i\\
&\quad -ind_{g,q}(q)\Big(\sum_{i\in p^{n-k}Z_{p^k}^*}\theta^i+\cdots+\sum_{i\in p^{n-1}Z_p^*}\theta^i\Big)\\
&= \sum_{i\in p^{n-k}Z_{p^k}^*} ind_{g,q}(i)\theta^i+\cdots+\sum_{i\in p^{n-1}Z_p^*} ind_{g,q}(i)\theta^i+ind_{g,q}(q),
\end{aligned}$$

where the third equality is from (20) and (21).

If $q\in D_0^{(q,p^n)}$, then $t_k(\theta)^q=t_k(\theta)$, i.e., $t_k(\theta)\in F_q$. We finish the proof. □

Lemma 6

$$S(\theta^a) = \begin{cases} q-1, & \text{if } a = 0 \\ t_k(\theta) + s + q - 1, & \text{if } a \in p^{n-k} D_s^{(q,p^k)} \end{cases}$$

for $s = 0, 1, \cdots, q-1$ *and* $k = 1, 2, \cdots, n$.

Proof. Note that $|Z_{p^j}^*| = p^{j-1}(p-1)$, then

$$|p^{n-j} D_i^{(q,p^j)}| = \frac{p^{j-1}(p-1)}{q} \tag{23}$$

for $j = 1, 2, \cdots, n$. Thus, when $a = 0$, we have

$$\begin{aligned} S(\theta^a) &= S(1) \\ &= q - 1 + \sum_{i \in Z_{p^n}^*} ind_{g,q}(i) + \sum_{i \in pZ_{p^{n-1}}^*} ind_{g,q}(i) + \cdots + \sum_{i \in p^{n-1} Z_p^*} ind_{g,q}(i) \\ &= q - 1 + \sum_{r=0}^{q-1} r \sum_{i \in D_r^{(q,p^n)}} 1 + \sum_{r=0}^{q-1} r \sum_{i \in pD_r^{(q,p^{n-1})}} 1 + \cdots + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-1} D_r^{(q,p)}} 1 \\ &= q - 1 + \sum_{r=0}^{q-1} r \left(\frac{p^{n-1}(p-1)}{q} + \frac{p^{n-2}(p-1)}{q} + \cdots + \frac{p-1}{q} \right) \\ &= \frac{(p^n+1)(q-1)}{2}. \end{aligned}$$

When $a \in p^{n-k} Z_{p^k}^*$ for $k = 1, 2, \cdots, n$, let $a = p^{n-k} b$, where $b \in Z_{p^k}^*$. Then,

$$\begin{aligned} S(\theta^a) &= q - 1 + \sum_{i \in Z_{p^n}^*} ind_{g,q}(i) \theta^{p^{n-k} bi} + \sum_{i \in pZ_{p^{n-1}}^*} ind_{g,q}(i) \theta^{p^{n-k} bi} + \cdots \\ &\quad + \sum_{i \in p^{n-1} Z_p^*} ind_{g,q}(i) \theta^{p^{n-k} bi} \\ &= q - 1 + \sum_{r=0}^{q-1} r \sum_{i \in D_r^{(q,p^n)}} \theta^{p^{n-k} bi} + \sum_{r=0}^{q-1} r \sum_{i \in pD_r^{(q,p^{n-1})}} \theta^{p^{n-k} bi} + \cdots \\ &\quad + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-1} D_r^{(q,p)}} \theta^{p^{n-k} bi} \\ &= q - 1 + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-k} \cdot D_r^{(q,p^n)}} \theta^{bi} + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-k} \cdot pD_r^{(q,p^{n-1})}} \theta^{bi} + \cdots \\ &\quad + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-k} \cdot p^{n-1} D_r^{(q,p)}} \theta^{bi}. \end{aligned} \tag{24}$$

For any integer n_1, it is obvious that

$$p^{n_1} \cdot p^{n-j} D_i^{(q,p^j)} = \begin{cases} 0 \pmod{p^n}, & \text{if } n-j+n_1 \geq n \\ p^{n-j+n_1} D_i^{(q,p^{j-n_1})} \pmod{p^n}, & \text{if } n-j+n_1 < n. \end{cases} \tag{25}$$

By (23),

$$|D_i^{(q,p^j)}| = \frac{p^{j-1}(p-1)}{q} = p^{n_1} \frac{p^{j-n_1-1}(p-1)}{q} = p^{n_1} |D_i^{(q,p^{j-n_1})}|. \tag{26}$$

Thus, from (25) and (26), (24) can be rewritten as,

$$\begin{aligned} S(\theta^a) = q-1+p^{n-k} \Bigg(\underbrace{\sum_{r=0}^{q-1} r \sum_{i \in p^{n-k} D_r^{(q,p^k)}} \theta^{bi} + \cdots + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-1} D_r^{(q,p)}} \theta^{bi}}_{k \text{ summations}} \Bigg) + \\ \underbrace{\cdots + \sum_{r=0}^{q-1} r \sum_{i \in p^{k} D_r^{(q,p^{n-k})}} \theta^{0} + \cdots + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-1} D_r^{(q,p)}} \theta^{0}}_{n-k \text{ summations}} \\ = p^{n-k} \Bigg(\sum_{r=0}^{q-1} r \sum_{i \in p^{n-k} D_r^{(q,p^k)}} \theta^{bi} + \cdots + \sum_{r=0}^{q-1} r \sum_{i \in p^{n-1} D_r^{(q,p)}} \theta^{bi} \Bigg) + \frac{(p^{n-k}+1)(q-1)}{2}. \end{aligned}$$

Suppose that $b \in D_s^{(q,p^k)}$. Then, $bD_r^{(q,p^j)} = D_{r+s(\bmod q)}^{(q,p^j)} (\bmod p^j)$ for $j = 1, 2, \cdots, k$. Hence, $bp^{n-j} D_r^{(q,p^j)} = p^{n-j} D_{r+s(\bmod q)}^{(q,p^j)}$. Therefore, we have

$$\begin{aligned} S(\theta^a) &= p^{n-k} \sum_{r=0}^{q-1} r \sum_{i \in p^{n-k} D_{r+s}^{(q,p^k)}} \theta^i + p^{n-k} \sum_{r=0}^{q-1} r \sum_{i \in p^{n-k+1} D_{r+s}^{(q,p^{k-1})}} \theta^i + \cdots \\ &\quad + p^{n-k} \sum_{r=0}^{q-1} r \sum_{i \in p^{n-1} D_{r+s}^{(q,p)}} \theta^i + \frac{(p^{n-k}+1)(q-1)}{2} \\ &= p^{n-k} \sum_{r=0}^{q-1} (r+s) \sum_{i \in p^{n-k} D_{r+s}^{(q,p^k)}} \theta^i + p^{n-k} \sum_{r=0}^{q-1} (r+s) \sum_{i \in p^{n-k+1} D_{r+s}^{(q,p^{k-1})}} \theta^i \\ &\quad + \cdots + p^{n-k} \sum_{r=0}^{q-1} (r+s) \sum_{i \in p^{n-1} D_{r+s}^{(q,p)}} \theta^i - p^{n-k} \Bigg[s \sum_{r=0}^{q-1} \sum_{i \in p^{n-k} D_{r+s}^{(q,p^k)}} \theta^i \\ &\quad + s \sum_{r=0}^{q-1} \sum_{i \in p^{n-k+1} D_{r+s}^{(q,p^{k-1})}} \theta^i + \cdots + s \sum_{r=0}^{q-1} \sum_{i \in p^{n-1} D_{r+s}^{(q,p)}} \theta^i \Bigg] + \frac{(p^{n-k}+1)(q-1)}{2}, \end{aligned}$$

where the addition $r+s$ is calculated modulo q.

Substituting r with $r+s$, we get

$$\begin{aligned}
S(\theta^a) &= p^{n-k}\sum_{r=0}^{q-1} r \sum_{i\in p^{n-k}D_r^{(q,p^k)}} \theta^i + p^{n-k}\sum_{r=0}^{q-1} r \sum_{i\in p^{n-k+1}D_r^{(q,p^{k-1})}} \theta^i + \cdots \\
&\quad + p^{n-k}\sum_{r=0}^{q-1} r \sum_{i\in p^{n-1}D_r^{(q,p)}} \theta^i - p^{n-k}s\left[\sum_{i\in p^{n-k}Z_{p^k}^*} \theta^i + \cdots + \sum_{i\in p^{n-1}Z_p^*} \theta^i\right] \\
&\quad + \frac{(p^{n-k}+1)(q-1)}{2} \\
&= p^{n-k}\left(\sum_{i\in p^{n-k}Z_{p^k}^*} ind_{g,q}(i)\theta^i + \cdots + \sum_{i\in p^{n-1}Z_p^*} ind_{g,q}(i)\theta^i\right) + p^{n-k}s \\
&\quad + \frac{(p^{n-k}+1)(q-1)}{2} \\
&= p^{n-k}t_k(\theta) + p^{n-k}s + \frac{(p^{n-k}+1)(q-1)}{2},
\end{aligned}$$

where the second equality follows from (20) and (21).

Note that $p \equiv 1 (\mathrm{mod}\ q)$, thus $p^{n-k} \equiv 1 (\mathrm{mod}\ q)$, $\frac{(p^n+1)(q-1)}{2} \equiv q-1 (\mathrm{mod}\ q)$ and $\frac{(p^{n-k}+1)(q-1)}{2} \equiv q-1 (\mathrm{mod}\ q)$ from $2|(q-1)$. Thus, by reducing modulo q, we have

$$S(\theta^0) = q-1$$

and

$$S(\theta^a) = t_k(\theta) + s + q - 1$$

for $a \in p^{n-k}D_s^{(q,p^k)}$. This completes the proof. □

Theorem 2. *If $q \in D_0^{(q,p^n)}$, then $L(\mathbf{s}) = \frac{(q-1)p^n+1}{q}$. If $q \notin D_0^{(q,p^n)}$, then $L(\mathbf{s}) = p^n$.*

Proof. By (18), it suffices to determine the number of a such that $S(\theta^a) = 0$ when a ranges from 0 to $p^n - 1$. When $q \in D_0^{(q,p^n)}$, from Lemma 5, $t_k(\theta) \in F_q$ for $k = 1, 2\cdots, n$. Given k with $1 \le k \le n$, let $t_k(\theta) = u$ where $u \in F_q$. From Lemma 6, when $a \in p^{n-k}D_{q-u+1(\mathrm{mod}\ q)}^{(q,p^k)}$, $S(\theta^a) = 0$. Therefore, when $t_k(\theta) = u$ for some fixed k, there exist $\frac{p^{k-1}(p-1)}{q}$ a's such that $S(\theta^a) = 0$. When k runs through $1, 2, \cdots, n$, there exist $\frac{p-1}{q} + \frac{p(p-1)}{q} + \cdots + \frac{p^{n-1}(p-1)}{q} = \frac{p^n-1}{q}$ a's with $a \in Z_{p^n}$ such that $S(\theta^a) = 0$. Therefore, the linear complexity of $\mathbf{s}$ is $L(\mathbf{s}) = p^n - \frac{p^n-1}{q} = \frac{(q-1)p^n+1}{q}$.

When $q \notin D_0^{(q,p^n)}$, $t_k(\theta) \notin F_q$ for $k = 1, 2\cdots, n$. Thus, for any $a \in Z_{p^n}$, $S(\theta^a) \neq 0$, which is from Lemma 6. Hence, $L(\mathbf{s}) = p^n$. We finish the proof. □

5 Conclusions

In this paper, we determine the autocorrelation of the q-ary prime n-square sequences. When q is a prime, we calculate the linear complexity of the prime n-square sequences over the prime field F_q. It is shown that the linear complexity of these sequences takes on one of $\frac{(q-1)p^n+1}{q}$ and p^n, depending on whether $q \in D_0^{(q,p^n)}$ or not, which is considered as quite good.

References

1. Burton, D.M.: Elementary Number Theory, 4th edn. McGraw-Hill International Editions, New York (1998)
2. Ding, C.: Linear Complexity of Generalized Cyclotomic Binary Sequences of Order 2. Finite Fields and Their Applications 3, 159–174 (1997)
3. Ding, C., Helleseth, T., Shan, W.: On the Linear Complexity of Legendre Sequences. IEEE Trans. Inform. Theory 44, 1276–1278 (1998)
4. Ding, C., Helleseth, T.: New Generalized Cyclotomy and its Applications. Finite Fields and their Applications 4, 140–166 (1998)
5. Ding, C.: Linear Complexity of Some Generalized Cyclotomic Sequences. International Journal on Algebra and Computation 8, 431–442 (1998)
6. Bai, E., Liu, X., Xiao, G.: Linear Complexity of New Generalized Cyclotomic Sequences of Order Two of Length pq. IEEE Trans. Inform. Theory 51, 1849–1853 (2005)
7. Yan, T., Sun, R., Xiao, G.: Autocorrelation and Linear Complexity of the New Generalized Cyclotomic Sequences. IEICE Trans. Fundamentals E90-A, 857–864 (2007)
8. Yan, T., Hong, L., Xiao, G.: The Linear Complexity of New Generalized Cyclotomic Binary Sequences of Order Four. Information Sciences 178, 807–815 (2008)
9. Kim, Y.J., Jin, S.Y., Song, H.Y.: Linear Complexity and Autocorrelation of Prime Cube Sequences. In: Boztaş, S., Lu, H.-F(F.) (eds.) AAECC 2007. LNCS, vol. 4851, pp. 188–197. Springer, Heidelberg (2007)
10. Kim, Y.J., Song, H.Y.: Linear Complexity of Prime n-Square Sequences. In: IEEE International Symposium on Information Theory, Toronto, Canada, pp. 2405–2408 (2008)
11. Meidl, W.: Remarks on a Cyclotomic Sequence. Designs, Codes, and Cryptography 51, 33–43 (2009)
12. Sidelnikov, V.M.: Some k-Valued Pseudo-random Sequences and Nearly Equidistance Codes. Problems of Information Transmission 5, 12–16 (1969)
13. Storer, T.: Cyclotomy and Difference Sets. Markham Publishing Co., Chicago (1967)
14. Whiteman, A.L.: A Family of Difference Sets. Illinois J. Math. 6, 107–121 (1962)
15. Lidl, R., Niederreiter, H.: Finite Fields. In: Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading (1983)

An Improved Approximation Algorithm for Computing the k-Error Linear Complexity of Sequences Using the Discrete Fourier Transform

Ana Sălăgean[1] and Alexandra Alecu[2]

[1] Department of Computer Science, Loughborough University, UK
A.M.Salagean@lboro.ac.uk
[2] Google, Inc., Zürich, Switzerland
alecu@google.com

Abstract. In our previous work we transformed the optimisation problem of finding the k-error linear complexity of a sequence into an optimisation problem in the DFT (Discrete Fourier Transform) domain, using Blahut's theorem. We then gave an approximation algorithm of polynomial complexity for the transformed problem by restricting the search space to error sequences whose DFT have period up to k. However, when applying the inverse transformation, the error vectors obtained are in general in an extension of the original field.

In the present paper we develop our previous approximation algorithm so that now it can be constrained to only obtain errors over the original field. Essentially, we give a polynomial approximation algorithm for the computation of the k-error linear complexity of a sequence. More precisely, the algorithm will find the optimum among a restricted set of errors over the original field. While this restricted search space is still exponential, the complexity of the algorithm is polynomial, $\mathcal{O}(N^2 \log N \log \log N)$.

Keywords: periodic sequences, linear complexity, k-error linear complexity, discrete Fourier transform.

1 Introduction

The linear complexity of a sequence of terms over a field is defined as the length of the smallest linear recurrence relation which generates that sequence. The k-error linear complexity of a periodic sequence is a natural generalisation of the notion of linear complexity and it represents the length of the smallest linear recurrence relation which generates a sequence which differs from the original in at most k positions in each period.

Algorithms for computing in polynomial time the k-error linear complexity only exists for periodic sequences of period N over a Galois field in the particular cases when $x^N - 1$ has only one or two distinct irreducible factors over that Galois field (see [9,7,6,10]).

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 151–165, 2010.

In our previous work [1] we transformed the optimisation problem of finding the k-error linear complexity of a sequence s of period N over a field K into an optimisation problem in the DFT (Discrete Fourier Transform) domain, using Blahut's theorem. Namely we aim to find a sequence E of linear complexity at most k which minimises the Hamming weight of a period of $DFT(s)+E$. We do not know of an efficient algorithm for this transformed problem, so we gave an approximation algorithm for it by restricting the search space to error sequences E of period up to k. However, when applying the inverse transformation, the error sequence $e = DFT^{-1}(E)$ may not be in the original field but an extension thereof. We therefore introduced a generalisation of the notion of k-error linear complexity, which we called extension field k-error linear complexity defined as the k-error linear complexity of s when working in the smallest extension field of K which contains an N-th root of unity. Our approximation algorithm did therefore produce an approximation of the extension field k-error linear complexity rather than of the classical k-error linear complexity.

In the present paper we develop our previous approximation algorithm so that it can now be constrained to only obtain errors over the original field. This is achieved by making sure the necessary conjugacy constraints are satisfied by E in the DFT domain so that $DFT^{-1}(E)$ is in the original field. We also add a new step of cyclically shifting the input sequence in order to cover a larger search space in our approximation. The algorithm will find the optimum among the restricted set of errors over the original field which have their up to k possible non-zero entries evenly spaced at intervals of $\frac{N}{d}$ positions for some $d|N$, $d \leq k$. While this search space is still exponential, the complexity of the algorithm is polynomial, $\mathcal{O}(N^2 \log N \log\log N)$.

The algorithms were implemented in GAP and the results of running them on a series of sequences are discussed in Section 5.

2 Background

We introduce some definitions and known results about linear complexity, k-error linear complexity and the discrete Fourier transform.

Definition 1. *Given an infinite sequence $s = s_0, s_1, \ldots$ with elements in a field K, we say that s is a linear recurrent sequence if it satisfies a homogeneous linear recurrence relation, i.e. a relation of the form*

$$s_j + c_{L-1}s_{j-1} + \ldots + c_1 s_{j-L+1} + c_0 s_{j-L} = 0 \tag{1}$$

for all $j = L, L+1, \ldots$ where $c_0, c_1, \ldots, c_{L-1} \in K$ are constants. We associate to it a characteristic polynomial *$C(X) = X^L + c_{L-1}X^{L-1} + \ldots + c_1 X + c_0$. If L is minimal for the given sequence, we call L the* linear complexity *of s, denoted $L(s)$, and we call $C(X)$ a* minimal polynomial.

For infinite sequences the minimal polynomial is unique and any other characteristic polynomial is a multiple of the minimal polynomial.

A sequence s is called *periodic* if there is an N such that $s_{i+N} = s_i$ for all $i \geq 0$. N is called a *period* of the sequence. Obviously $X^N - 1$ is in this case a characteristic polynomial of s, so its minimal polynomial must be a factor of $X^N - 1$ and the linear complexity is at most N.

For any finite sequence s we will denote by $w_H(s)$ the Hamming weight i.e. the number of non-zero entries of s. When considering infinite sequences s of period N we will identify the sequence s with the N-tuple $(s_0, s_1, \ldots, s_{N-1})$, so for example $w_H(s)$ means $w_H((s_0, s_1, \ldots, s_{N-1}))$.

The notion of linear complexity has been generalised to k-error linear complexity, defined as the minimal linear complexity of a sequence in which at most k positions are changed, (see Ding, Xiao, Shan [3], Stamp and Martin [9]).

Definition 2. *Given an infinite sequence s of period N, with elements in a field K and a fixed integer k, $0 \leq k \leq w_H(s)$, the* k-error linear complexity *of the sequence s is defined as*

$$L_{k,N}(s) = \min\{L(s+e) | e \in K^N, w_H(e) \leq k\}.$$

In the set above, e is a sequence of period N and is called an error sequence.

We recall the definition of the discrete Fourier transform (DFT) and a number of its well known properties (see for example [8]) which will be needed later.

Definition 3. *Let F be a field containing a primitive N-th root of the unity α and let s be a sequence of period N over F. The* discrete Fourier transform *(DFT) of s is the sequence $S = DFT(s) = (S_0, S_1, \ldots, S_{N-1})$ defined by*

$$S_i = \sum_{j=0}^{N-1} s_j \alpha^{ij}, \text{ for all } i = 0, 1, \ldots, N-1.$$

The inverse discrete Fourier transform *relation $s = DFT^{-1}(S)$ is given by:*

$$s_j = N^{-1} \sum_{i=0}^{N-1} S_i \alpha^{-ij}, \text{ for all } j = 0, 1, \ldots, N-1.$$

Note that the assumption that F contains a primitive N-root of unity means N should not be divisible by the characteristic of the field F. For sequences over a field K which does not contain an N-th root of unity, provided N is not divisible by the characteristic of K, we would first determine an extension field F of K which does contain an N-th root of unity, and only then we are able to compute the DFT.

It is well known that the discrete Fourier transform is linear:

Property 1. Let N be a positive integer and F be an arbitrary field which contains a primitive N-th root of unity. The discrete Fourier transform and the inverse discrete Fourier transform are linear operators on the vector space F^N.

Let $s^{(h)}$ denote the periodic infinite sequence over F obtained by cyclically shifting all periods of s to the right by h positions, i.e. $s^{(h)}_{i+h} = s_i$, for all $0 \leq i < N$ where indices are taken modulo N. The Discrete Fourier Transform of the shifted sequence is related to the one of the original sequence as follows:

Property 2. If $S = DFT(s)$ and $S' = DFT(s^{(h)})$ then $S'_i = \alpha^{hi} S_i$, for all $0 \leq i < N$.

In 1979, Blahut [2] used the link between the linear complexity of a periodic sequence and its DFT:

Theorem 1 (Blahut theorem). *The linear complexity of a periodic sequence $s = (s_0, s_1, \ldots, s_{N-1})$ of period N, equals the Hamming weight of $DFT(s)$. Reciprocally, the linear complexity of the periodic sequence $S = (S_0, S_1, \ldots, S_{N-1})$ equals the Hamming weight of $DFT^{-1}(S)$.*

When the original sequence s is in a subfield K of F we will be interested in distinguishing the sequences S in F^N which were obtained as DFT of sequences in K^N rather than F^N. We examine this issue in the case of finite fields, which is particularly important for cryptographic applications.

We will denote by $K = \mathrm{GF}(p^m)$ the Galois field of p^m elements. When N is not divisible by p, the smallest extension F of K which contains a (primitive) N-the root of unity is $F = \mathrm{GF}(p^r)$ where r is the smallest multiple of m with the property $N | p^r - 1$.

Recall that the cyclotomic coset of j modulo $p^r - 1$ with respect to powers of p^m is the set $C_j = \{j, jp^m, jp^{2m}, \ldots, jp^{(\frac{r}{m}-1)m}\}$ (with all integers modulo $p^r - 1$). More generally for a factor d of $p^r - 1$ the cyclotomic set of j modulo d with respect to powers of p^m is the set having the same elements as C_j above but with all integers considered modulo d. We will denote this set $C_{j,d}$, so C_j is the same as C_{j,p^r-1}. We have $C_{j,d} = \{j, jp^m, jp^{2m}, \ldots, jp^{(|C_{j,d}|-1)m}\}$ and $j = jp^{m|C_{j,d}|}$. The cardinalities of the cyclotomic cosets modulo different integers are related as follows: if $d | N | p^r - 1$ then $|C_{j,d}| \leq |C_{j,N}|$, in fact $|C_{j,d}|$ is a divisor of $|C_{j,N}|$.

Recall that the conjugates of an element $a \in \mathrm{GF}(p^r)$ with respect to $\mathrm{GF}(p^m)$ are defined as $a, a^{p^m}, a^{p^{2m}}, \ldots a^{p^{(\frac{r}{m}-1)m}}$. If α is a primitive element of $\mathrm{GF}(p^r)$, then the conjugates of α^j are $\{\alpha^i \mid i \in C_j\}$.

We can distinguish whether an element $a \in \mathrm{GF}(p^r)$ is in $\mathrm{GF}(p^m)$ or in $\mathrm{GF}(p^r) \setminus \mathrm{GF}(p^m)$ by checking whether $a^{p^m} = a$ or not. Writing this condition for each element of s and taking into account that $s = DFT^{-1}(S)$, we obtain the following known result:

Property 3. Let $\mathrm{GF}(p^r)$ be the smallest extension field of $\mathrm{GF}(p^m)$ which contains a primitive N-th root of unity. Let s be a sequence over $\mathrm{GF}(p^r)$ of period N and $S = DFT(s)$. Then $s \in \mathrm{GF}(p^m)^N$ iff $S_{p^m i} = S_i^{p^m}$ for all $i = 0, 1, \ldots, N-1$, (with indices taken modulo N). In particular, $S_0 \in \mathrm{GF}(p^m)$.

3 Problem Transformation

In this section we recall results from [1], to be further developed in the next section.

The k-error linear complexity problem can be viewed as an optimisation problem: given integers N and k with $k \leq N$ and a sequence s of period N over a field K, find e, a sequence of period N over the extension field F such that $w_H(e) \leq k$ and $L(s+e)$ is minimal (F is the extension field of K containing an N-th root of unity). We can transform this problem into an optimisation problem in the DFT domain. Using Blahut's theorem and the linearity of DFT we see that we can search for sequences E of linear complexity at most k and which minimize the weight of $DFT(s)+E$. The resulting sequence E is then transformed back obtaining an optimal error sequence as $e = DFT^{-1}(E)$. Note that this error sequence can be in the extension field used for computing the DFT rather than in the original field K over which s was defined. We defined therefore a notion of extension field k-error linear complexity, which is the k-error linear complexity of a sequence of period N when viewed as a sequence over the smallest extension field that contains an N-th root of unity.

Theorem 2. *[1] Let s be a sequence of period N over a field K such that N is not divisible by the characteristic of K, and let $k \leq N$. Let F be the smallest extension field of K which contains an N-th root of unity and let $S = DFT(s)$. For all sequences e, E of period N over F with $E = DFT(e)$ we have the equivalence: (e is such that $w_H(e) \leq k$ and $L(s+e)$ is minimal) $\Leftrightarrow$ (E is such that $L(E) \leq k$ and $w_H(S+E)$ is minimal)*

The generic algorithm $kDFT$ based on Theorem 2 was proposed in [1].

Algorithm $kDFT$

Input: s a sequence of period N over a field K,
N not divisible by the characteristic of K, $k \leq N$,
Output: e, a sequence of period N over F with $w_H(e) \leq k$ and $L(s+e)$ minimal.
The second output is $L_{k,N}(s)$
STEP 1. Determine F, α such that F is the smallest extension of K which contains a primitive N-th root of unity α.
STEP 2. Calculate $S = DFT(s)$ of period N over F.
STEP 3. Find E a sequence over F of period N and linear complexity $L(E) \leq k$ such that $w_H(S+E)$ is minimal.
STEP 4. **return**$(DFT^{-1}(E), w_H(S+E))$.

Algorithm $kDFT$ is of theoretic interest, however we do not know of an algorithm for STEP 3 other than exhaustive search (for finite fields). In [1] we proposed therefore an approximation algorithm. Namely, given a sequence $S \in F^N$ we aim to find a sequence E of linear complexity at most k such that $w_H(S+E) \leq w_H(S)$, but $w_H(S+E)$ is not necessarily minimal. To this end, we limit our search to sequences E which have minimal period at most k besides having period N. This minimal period d must therefore be a divisor of N. Obviously any sequence of period at most k will also have linear complexity at most k. In

order to decrease $w_H(S+E)$ as much as possible we choose the elements of E so that they cancel out as many elements of S as possible.

Theorem 3. *Let S be a sequence of period N over a field F. Suppose N is not prime and d is a proper divisor of N. For each $j = 0, 1, \ldots, d-1$ denote by β_j (one of) the most frequent element among $S_j, S_{d+j}, \ldots, S_{(\frac{N}{d}-1)d+j}$. Let E be the sequence of period d defined as $E = (-\beta_0, -\beta_1, \ldots, -\beta_{d-1})$. Then E achieves the minimal value of $w_H(S+E)$ (E is viewed as a sequence of period N for the purpose of computing this weight) among all sequences E over F of period d.*

By computing E as above and taking the best value over all d with $d \leq k$ and $d|N$ we obtained an approximation for STEP 3 of *kDFT* and we called the resulting algorithm *kDFT-Approximation*.

4 Approximation Algorithm for the *k*-Error Linear Complexity

In order to design an algorithm that only produces sequences $E \in F^N$ with the property that $DFT^{-1}(E) \in K^N$, we examine closer the properties of such sequences in relation to Theorem 3. From now on we only work in finite fields with $K = \mathrm{GF}(p^m)$ and $F = \mathrm{GF}(p^r)$.

Lemma 1. *Let $s \in \mathrm{GF}(p^m)^N$ and $S = DFT(s)$. Let d be a proper divisor of N and consider S arranged in an $\frac{N}{d} \times d$ matrix. The number of occurrences of an element $a \in GF(p^r)$ in column j equals to the number of occurrences of a^{p^m}, in column $(jp^m \bmod d)$.*

Proof. Indexing the rows of the matrix from 0 to $\frac{N}{d}-1$ and the columns from 0 to $d-1$, the entry in row i column j will be S_{id+j}. Note that because $d|N$, we have $(u \bmod N) \bmod d = u \bmod d$ for any integer u. From Property 3, $S^{p^m}_{id+j} = S_{p^m(id+j) \bmod N} = S_{((p^m i + \lfloor \frac{p^m j}{d} \rfloor) \bmod \frac{N}{d})d + (p^m j \bmod d)}$, i.e. the power p^m of the entry in row i, column j appears in row $((p^m i + \lfloor \frac{p^m j}{d} \rfloor) \bmod \frac{N}{d})$, column $(p^m j \bmod d)$. It can be easily verified that for a fixed j, $((p^m i + \lfloor \frac{p^m j}{d} \rfloor) \bmod \frac{N}{d})$ takes distinct values for distinct row indices i. Hence each entry in column $(p^m j \bmod d)$ is the p^m power of a distinct entry in column j.

Corollary 1. *With the notations of Lemma 1, if $\mathrm{GF}(p^{um})$ is a subfield of $\mathrm{GF}(p^r)$ (i.e. $1 \leq u \leq \frac{r}{m}$), and β_j is the most frequent among those elements in column j which are also in $\mathrm{GF}(p^{um})$, then $\beta_j^{p^m}$ is the most frequent among those elements in column $p^m j \bmod d$ which are also in $\mathrm{GF}(p^{um})$.*

Proof. We use Lemma 1 and the fact that for any element $a \in \mathrm{GF}(p^r)$ we have $a \in \mathrm{GF}(p^{um})$ iff all the conjugates of a with respect to $\mathrm{GF}(p^m)$ are in $\mathrm{GF}(p^{um})$.

Theorem 4. *Let $E \in \mathrm{GF}(p^r)^N$ be a sequence which also has a smaller period $d|N$. The following statements are equivalent:*

i. $DFT^{-1}(E) \in \mathrm{GF}(p^m)^N$
ii. *For all* $j = 0, 1, \ldots, d-1$ *we have* $E_j^{p^m} = E_{jp^m \bmod d}$
iii. *Let* $0, j_1, j_2, \ldots, j_v$ *be coset representatives modulo* d *(with respect to powers of* p^m*). For each* $j \in \{0, j_1, j_2, \ldots, j_v\}$ *we have* $E_j \in \mathrm{GF}(p^{m|C_{j,d}|})$ *and* $E_{jp^{um} \bmod d} = E_j^{p^{um}}$ *for all* $u = 1, 2, \ldots, |C_{j,d}| - 1$.

Proof. The equivalence of the first two assertions follows easily from Property 3 and the fact that E has period d.

The equivalence of the second and third assertion is immediate and we will only add that applying repeatedly the equality $E_j^{p^m} = E_{jp^m \bmod d}$ from ii. yields $E_{jp^{2m} \bmod d} = E_{jp^m \bmod d}^{p^m} = (E_j^{p^m})^{p^m} = E_j^{p^{2m}}$. More generally $E_{jp^{um} \bmod d} = E_j^{p^{um}}$ for any positive integer u. In particular for $u = |C_{j,d}|$ we obtain $E_{jp^{m|C_{j,d}|} \bmod d} = E_j^{p^{m|C_{j,d}|}}$. By the definition of $C_{j,d}$ we have $jp^{m|C_{j,d}|} \bmod d = j$, and therefore $E_j = E_j^{p^{m|C_{j,d}|}}$, which occurs iff $E_j \in \mathrm{GF}(p^{m|C_{j,d}|})$.

The following theorem follows from Corollary 1 and Theorem 4. It generalises Theorem 3 which becomes the particular case $m = r$:

Theorem 5. *Let* s *be a sequence of period* N *over* $\mathrm{GF}(p^m)$ *and* $S = DFT(s) \in \mathrm{GF}(p^r)^N$*. Suppose* N *is not prime and* d *is a proper divisor of* N*. Let* $0, j_1, \ldots, j_v$ *be coset representatives modulo* d *(with respect to powers of* p^m*). For each* $j \in \{0, j_1, j_2, \ldots, j_v\}$ *denote by* β_j *(one of) the most frequent element among those elements of the list* $S_j, S_{d+j}, \ldots, S_{(\frac{N}{d}-1)d+j}$ *which are also in* $\mathrm{GF}(p^{m|C_{j,d}|})$*. If none of these elements is in* $\mathrm{GF}(p^{m|C_{j,d}|})$*, set* $\beta_j = 0$*. Set* $\beta_{jp^{um}} = \beta_j^{p^{um}}$*, for* $u = 1, 2, \ldots, |C_{j,d}| - 1$*. Let* E *be the sequence of period* d *defined as* $E = (-\beta_0, -\beta_1, \ldots, -\beta_{d-1})$.

Then E *(viewed as a sequence of period* N*) achieves the minimal value of* $w_H(S + E)$ *among all sequences* E *over* $\mathrm{GF}(p^r)$ *of period* d *which have the additional property* $DFT^{-1}(E) \in \mathrm{GF}(p^m)^N$.

Based on the above results we devise an algorithm *GetErrorBaseField* for finding a candidate sequence E (corresponding to STEP 3 in $kDFT$ Algorithm from previous section). The cardinalities of the cyclotomic cosets $C_{j,d}$ (as defined in Section 2) do not depend on s or S so they can be precomputed in $\mathcal{O}(d)$ time as each element of $\{0, 1, \ldots, d-1\}$ only appears in one cyclotomic coset.

Example 1. The following sequence S of length 63 over the field $\mathrm{GF}(2^6)$, defined by a primitive element α, is written row by row as a 9×7 matrix:

$$
\begin{array}{ccccccc}
0 & \alpha^9 & \alpha^{18} & 0 & \alpha^{36} & 0 & 0 \\
0 & \alpha^9 & \alpha^{36} & 0 & \alpha^{32} & 0 & 0 \\
0 & \alpha & \alpha^{18} & 0 & \alpha^9 & 0 & 0 \\
0 & \alpha & \alpha^{16} & 0 & \alpha^4 & 0 & 0 \\
0 & \alpha & \alpha^2 & 0 & \alpha^{36} & 0 & 0 \\
0 & \alpha^{18} & \alpha^{16} & 0 & \alpha^{32} & 0 & 0 \\
0 & \alpha^8 & \alpha^2 & 0 & \alpha^{32} & 0 & 0 \\
0 & \alpha^8 & \alpha^{16} & 0 & \alpha^4 & 0 & 0 \\
0 & \alpha^8 & \alpha^2 & 0 & \alpha^4 & 0 & 0
\end{array}
$$

Algorithm $GetErrorBaseField(S, N, d, p^m)$

Input: S, sequence of period N over $\mathrm{GF}(p^r)$ with $DFT^{-1}(S) \in \mathrm{GF}(p^m)^N$, $m|r$. d a proper divisor of N
Output: E, a sequence of period N over $\mathrm{GF}(p^r)$ such that E achieves the minimal value of $w_H(S+E)$ among all sequences of period d with the property that $DFT^{-1}(E) \in \mathrm{GF}(p^m)^N$.
for $j \leftarrow 0, 1, 2, \ldots, d-1$ **do**
  $flag[j] \leftarrow 0$ (keeps track of columns processed so far)
for $j \leftarrow 0, 1, 2, \ldots, d-1$ **do**
  if $flag[j] = 0$ **then**
    compute β_j as (one of) the most frequent value among those values in the list $S_j, S_{d+j}, \ldots S_{(\frac{N}{d}-1)d+j}$ which are also in $\mathrm{GF}(p^{m|C_{j,d}|})$; if none of them is in $\mathrm{GF}(p^{m|C_{j,d}|})$ then set $\beta_j = 0$
    $flag[j] \leftarrow 1$; $u \leftarrow j$; $v \leftarrow p^m u \bmod d$
    while $flag[v] = 0$ **do** $\beta_v \leftarrow \beta_u^{p^m}$; $flag[v] \leftarrow 1$; $u \leftarrow v$; $v \leftarrow p^m v \bmod d$;
  endif
for $j \leftarrow 0, 1, 2, \ldots, d-1$ **do**
  for $i \leftarrow 0, 1, \ldots, \frac{N}{d} - 1$ **do**
    $E_{di+j} = -\beta_j$
return(E)

It can be verified that this sequence is the DFT of a binary sequence as it satisfies Property 3. Choosing (one of) the most frequent entry in each column, as in Theorem 3, we can obtain for example $E = (0, \alpha, \alpha^{16}, 0, \alpha^4, 0, 0)$. E decreases the weight of S by 9. Note that $DFT^{-1}(E) \notin \mathrm{GF}(2)^{63}$.

We have $|C_{0,7}| = 1$ and $|C_{j,7}| = 3$ for all $1 \le j \le 6$. So in Algorithm $GetErrorBaseField$ we have to choose E_0 to be in $\mathrm{GF}(2)$ and all the other entries of E to be in $\mathrm{GF}(2^3)$, i.e. powers of α^9. E also has to satisfy the conjugacy constraints $E_2 = E_1^2$, $E_4 = E_2^2$, $E_6 = E_3^2$ and $E_5 = E_6^2$. We obtain $E = (0, \alpha^9, \alpha^{18}, 0, \alpha^{36}, 0, 0)$, which decreases the weight of S only by 6, but has the property that $DFT^{-1}(E) \in \mathrm{GF}(2)^{63}$.

If a sequence of period N has also a smaller period $d|N$ (like the sequence E in the discussion above), it can be easily verified by direct computation that its DFT and inverse DFT have a particular form, namely they have zero entries on all positions except possibly the first one and then every $\frac{N}{d}$-th one (i.e. the positions whose indices are multiples of $\frac{N}{d}$):

Theorem 6. *Let E be a sequence of period N over a field F and let $d|N$. Set $e = DFT^{-1}(E)$, $e' = DFT(E)$. We have the equivalence:*
E has period $d \Leftrightarrow e$ and e' are 0 on all positions with indices not divisible by $\frac{N}{d}$
If the conditions above are satisfied, then $(e_0, e_{\frac{N}{d}}, \ldots, e_{(d-1)\frac{N}{d}}) = DFT^{-1}(E_0, E_1, \ldots E_{d-1})$ and $(e'_0, e'_{\frac{N}{d}}, \ldots, e'_{(d-1)\frac{N}{d}}) = \frac{N}{d} DFT(E_0, E_1, \ldots E_{d-1})$, the DFT being computed here for sequences of period d using $\alpha^{\frac{N}{d}}$ as primitive d-th root of unity.

Based on the discussion above we propose the following approximation algorithm, *kDFT-Approximation-BaseField*, for the k-error linear complexity.

Algorithm *kDFT-Approximation-BaseField*

Input: s a sequence of period N over a field K,
N not divisible by the characteristic of K, $k \leq N$.
Output: e, a sequence of period N over K such that $w_H(e) \leq k$ and $L(s+e)$ is minimal among all sequences e for which there is some $d|N$, $d \leq k$ such that e has zeros on all positions with indices not divisible by $\frac{N}{d}$;
The second output is $L(s+e)$.
STEP 1. Determine F, α such that F is the smallest extension of K which contains a primitive N-th root of unity α.
STEP 2. Calculate $S = DFT(s)$ of period N over F.
$L_{best} \leftarrow w_H(S)$; $E_{best} \leftarrow (0, 0, \ldots, 0)$
STEP 3.
for each proper divisor d of N **do**
  $E \leftarrow GetErrorBaseField(S, N, d)$
  if $w_H(S+E) < L_{best}$ **then** $E_{best} \leftarrow E$; $L_{best} \leftarrow w_H(S+E)$
endfor
STEP 4. **return**$(DFT^{-1}(E_{best}), L_{best})$

Note that the linear complexity and the k-error linear complexity of a periodic sequence s are invariant to shifting s. Moreover e is an error sequence which minimises the linear complexity of $s+e$ iff $e^{(h)}$ is an error sequence which minimises the linear complexity of $s^{(h)} + e^{(h)}$ (recall that we denoted by $s^{(h)}$ the sequence s shifted by h positions to the right).

For a given d and h, if we apply the algorithm *kDFT-Approximation-BaseField* to the sequence $s^{(h)}$ and we shift the error obtained back h positions to the left, then we obtain the optimum error for s among all errors which have the non-zero entries "spaced out" every $\frac{N}{d}$ positions starting with position $N-h$. Obviously we would only need to do that for $h = 0, 1, \ldots, \frac{N}{d} - 1$ in order to obtain all optimal error sequences that have the non-zero entries "spaced out" every $\frac{N}{d}$ positions (with no restrictions on where to start). For ease of reference we will call such errors "evenly spaced":

Definition 4. *A periodic sequence $e \in F^N$ is called an* evenly spaced *k-error sequence if there is $d \leq k$, d a proper divisor of N and there is an i with $0 \leq i < \frac{N}{d}$ such that all the non-zero entries of e are among $e_i, e_{\frac{N}{d}+i}, \ldots, e_{\frac{N}{d}(d-1)+i}$. (Note such an error has weight at most d.)*

The results above lead us to the following algorithm *kDFT-Approximation-BaseField-AllShifts*. The function $ShiftDFT(S)$ returns a sequence S' computed as $S'_i = \alpha^i S_i$ for $i = 0, 1, \ldots, N-1$. By Property 2, this means that if $S = DFT(s)$ then $S' = DFT(s^{(1)})$.

Algorithm *kDFT-Approximation-BaseField-AllShifts*

Input: s a sequence of period N over a field K,
N not divisible by the characteristic of K, $k \leq N$,
Output: e, a sequence of period N over K such that $L(s+e)$ is minimal among all evenly spaced k-error sequences e
the second output is $L(s+e)$.
STEP 1. Determine F, α such that F is the smallest extension of K which contains a primitive N-th root of unity α.
STEP 2. Calculate $S = DFT(s)$ of period N over F.
$h_{best} \leftarrow 0$; $L_{best} \leftarrow w_H(S)$; $E_{best} \leftarrow (0, 0, \ldots 0)$
STEP 3.
for each proper divisor d of N **do**
  $E \leftarrow GetErrorBaseField(S, N, d)$; $L \leftarrow w_H(S+E)$
  if $L < L_{best}$ **then** $E_{best} \leftarrow E$; $L_{best} \leftarrow L$; $h_{best} \leftarrow 0$;
  for $h \leftarrow 1, \ldots, \frac{N}{d} - 1$ **do**
    $S \leftarrow ShiftDFT(S)$; $E \leftarrow GetErrorBaseField(S, N, d)$; $L \leftarrow w_H(S+E)$
    if $L < L_{best}$ **then** $E_{best} \leftarrow E$; $h_{best} \leftarrow h$; $L_{best} \leftarrow L$
  endfor
endfor
STEP 4. Compute e, the sequence obtained from $DFT^{-1}(E_{best})$ by cyclically shifting all terms of each period to the left by h_{best} positions
return(e, L_{best})

We examine now the complexity of the algorithms above:

Lemma 2. *The function* $GetErrorBaseField(S, N, d)$ *has a computational complexity of* $\mathcal{O}(N \log \frac{N}{d})$.

Proof. The function *GetErrorBaseField* can be implemented by expressing all non-zero elements as powers of α. In each column we select the entries which are in the correct subfield, sort them in $\mathcal{O}(\frac{N}{d} \log \frac{N}{d})$ according to the exponents and then find in $\mathcal{O}(\frac{N}{d})$ time the most frequent in a column. So a total of $\mathcal{O}(N \log \frac{N}{d})$ operations.

Theorem 7. *The algorithm kDFT-Approximation-BaseField-AllShifts has computational complexity* $\mathcal{O}(N^2 \log N \log \log N)$.

Proof. By Lemma 2, *GetErrorBaseField* takes $\mathcal{O}(N \log \frac{N}{d})$. For each divisor d of N, this function is called $\frac{N}{d}$ times, so a total of $\mathcal{O}(N \sum_{d|N} \frac{N}{d} \log \frac{N}{d}) = \mathcal{O}(N \sum_{d|N} d \log d)$. By Grönwall's Theorem [5], $\sum_{d|N} d$ can be estimated as $\mathcal{O}(N \log \log N)$, so we can estimate $\sum_{d|N} d \log d$ as $\mathcal{O}(N \log N \log \log N)$. We obtain a total of $\mathcal{O}(N^2 \log N \log \log N)$ for STEP 3. The DFT computations in STEP 2 and 4 are dominated by that.

We note that a more refined estimate of $\sum_{d|N} d \log d$ might give an even lower $\mathcal{O}$ complexity for this algorithm.

As our algorithm will obtain in polynomial time an optimum among all evenly spaced k-error sequences, it will be interesting to determine whether this restricted search space is still exponential like the total search space (there are $\sum_{i=0}^{k} \binom{N}{i}(|K|-1)^i$ errors of weight up to k) or it is polynomial in size, in which case our algorithm would be less interesting. For a given d in Definition 4 there are $\frac{N}{d}|K|^d$ error sequences. The sets of error sequences for different factors d are disjoint only if the values d are coprime, so rather than go into a lengthy inclusion-exclusion argument, let us note that a lower bound on the number of evenly spaced k-error sequences will be $\frac{N}{d}|K|^d$, with d the largest of the factors of N with $1 < d \leq k$. Hence the search space is still exponential in k, so our polynomial time algorithm is indeed efficient.

5 Experimental Results

We implemented the algorithms kDFT-Approximation-BaseField and kDFT-Approximation-BaseField-AllShifts presented in Section 4 using GAP [4].

The results of several experiments are shown in Tables 1, 2 and 3. We tested binary sequences of odd lengths N up to 255 excluding those that are prime and those for which the extension field GF(p^r) in which the primitive N-th root of unity lies has $r \geq 20$ (the latter restriction is only for efficiency reasons). We also tested a few higher lengths of the form $N = 2^r - 1$, namely $N = 1023, 2047$.

Table 1. Experimental results

			kDFT-Approx		AllShifts		kDFT-Approx-BF		BF-AllShifts	
Length	Extension	Divisor	Success	Av. decr. of	Success	Av. decr. of	Success	Av. decr. of	Success	Av. decr. of
N	field	d	rate	lin. compl.	rate	lin. compl.	rate	lin. compl.	rate	lin. compl.
15	$GF(2^4)$	3	92	24.91%	100	40.7%	88	23.2 %	99	38.52%
		5	91	39.3%	97	48.9%	91	39.3%	97	48.9%
21	$GF(2^6)$	3	93	17.75%	100	32.03%	86	17.94%	98	30.90%
		7	99	34.58%	99	42.34%	99	34.58%	99	42.34%
27	$GF(2^{18})$	3	100	10.8%	100	15.11%	47	5.83%	74	9.94%
		9	100	34.2%	100	37.93%	48	7.25%	74	10.66%
33	$GF(2^{10})$	3	90	7.02%	93	10.73%	90	6.95%	92	9.34%
		11	100	32.92%	100	35.63%	100	32.93%	100	35.63%
35	$GF(2^{12})$	5	98	15.2%	99	19.71%	97	14.42%	99	19.52%
		7	100	18.22%	100	23.56%	100	17.58%	100	21.31%
39	$GF(2^{12})$	3	90	6.10%	94	9.45%	90	5.83%	90	7.33%
		13	100	33.61%	100	35.35%	100	33.61%	100	35.35%

Table 2. (*Continued*)

			kDFT-Approx		AllShifts		kDFT-Approx-BF		BF-AllShifts	
Length N	Extension field	Divisor d	Success rate	Av. decr. of lin. compl.	Success rate	Av. decr. of lin. compl.	Success rate	Av. decr. of lin. compl.	Success rate	Av. decr. of lin. compl.
45	$GF(2^{12})$	3	99	9.76%	100	16.67%	52	8.13%	94	13.44%
		5	94	13.48%	96	17.91%	94	13.24%	96	17.73%
		9	100	21.5%	100	27.35%	100	20.49%	100	26.7%
		15	100	35.56%	100	39.64%	94	13.72%	96	18.31%
51	$GF(2^{8})$	3	92	6.36%	100	15.98%	89	5.06%	97	13.97%
		17	100	33.52%	100	35.61%	100	33.52%	100	35.61%
57	$GF(2^{18})$	3	90	3.99%	90	4.23%	90	3.99%	90	4.23%
		19	100	33.38%	100	34.71%	100	33.38%	100	34.71%
63	$GF(2^{6})$	3	93	8.9%	99	16.66%	58	7.05%	99	15.52%
		7	98	14.78%	100	22.06%	98	13.71%	100	21.52%
		9	98	17.72%	100	25.07%	97	17.16%	100	24.42%
		21	100	33.94%	100	37.74%	100	30.82%	100	34.8%
65	$GF(2^{12})$	5	94	7.09%	94	9.38%	94	6.96%	94	8.53%
		13	99	19.93%	100	22.19%	99	19.73%	100	21.42%
85	$GF(2^{8})$	5	99	8.41%	100	14.36%	99	7.16%	99	13.69%
		17	100	20.33%	100	23.67%	100	20.18%	100	23.01%
91	$GF(2^{12})$	7	99	6.84%	100	9.66%	99	6.44%	99	7.15%
		13	100	14.91%	100	16.96%	100	14.55%	100	16.96%
93	$GF(2^{10})$	3	95	4.57%	100	11.43%	90	3.52%	100	10.67%
		31	100	33.63%	100	35.69%	100	33.63%	100	35.69%
105	$GF(2^{12})$	3	93	4.24%	99	9.13%	89	3.81%	99	8.88%
		5	93	5.55%	97	10.46%	92	5.24%	97	10.37%
		7	98	7.33%	100	11.45%	98	6.7%	100	10.85%
		15	100	14.11%	100	17.77%	100	13.67%	100	17.39%
		21	100	19.70%	100	22.94%	100	19.48%	100	22.58%
		35	100	33.54%	100	36.24%	100	33.54%	100	36.28%
117	$GF(2^{12})$	3	100	2.96%	100	6.43%	57	1.92%	83	3.98%
		9	100	7.38%	100	11.45%	100	7.32%	100	10.92%
		13	100	11.43%	100	13.02%	100	11.36%	100	13.02%
		39	100	33.74%	100	34.59%	100	32.12%	100	33.14%

Table 3. (*Continued*)

			kDFT-Approx		AllShifts		kDFT-Approx-BF		BF-AllShifts	
Length	Extension	Divisor	Success	Av. decr. of	Success	Av. decr. of	Success	Av. decr. of	Success	Av. decr. of
N	field	d	rate	lin. compl.	rate	lin. compl.	rate	lin. compl.	rate	lin. compl.
133	$GF(2^{18})$	7	100	4.5%	100	5.17%	100	4.5%	100	4.5%
		19	100	14.63%	100	15.93%	100	14.40%	100	15.93%
171	$GF(2^{18})$	3	97	1.71%	99	2.23%	50	1.13%	69	1.55%
		9	99	4.52%	99	4.9%	99	4.48%	99	4.77%
		19	100	11.08%	100	11.59%	100	11.07%	100	11.59%
		57	100	33.5%	100	33.94%	100	32.42%	100	32.92%
255	$GF(2^{8})$	3	99	2.91%	100	7.01%	95	1.83%	100	6.56%
		5	99	4.11%	100	7.77%	97	3.77%	100	7.54%
		15	100	8.23%	100	11.76%	100	7.31%	100	10.92%
		17	100	9.38%	100	13.29%	100	9.19%	100	13.18%
		51	100	20.92%	100	23.21%	100	20.77%	100	23.08%
		85	100	34.03%	100	34.98%	100	34.03%	100	34.98%
1023	$GF(2^{10})$	3	100	0.82%	100	2.44%	84	0.46%	100	2.34%
		11	100	2.15%	100	3.55%	100	2.08%	100	3.53%
		31	100	4.45%	100	5.92%	100	4.05%	100	5.58%
		33	100	4.32%	100	6.21%	100	4.20%	100	6.11%
		93	100	9.64%	100	11%	100	9.58%	100	10.93%
		341	100	33.44%	100	33.73%	100	33.44%	100	33.73%
2047	$GF(2^{11})$	23	100	2.06%	100	2.72%	100	2.05%	100	2.7%
		89	100	4.77%	100	5.85%	100	4.77%	100	5.85%

For each length we generated a sample of 100 sequences using the standard pseudorandom number generator (linear congruential generator). The Tables show for each length N, the extension field for the primitive N-th root of unity, and, for each of the proper divisors of N, the number of sequences (out of 100) for which an error sequence which decreases the complexity was found (success rate) and the average decrease of complexity which has been thus obtained (where the decrease in complexity is computed as $(L(s) - L(s+e))/L(s)$, where e is the error sequence returned by the algorithm). Note that we include in the average all sequences, even those for which no decrease is obtained. We display this information for each of the algorithms: $kDFT$-Approximation presented in [1], $kDFT$-Approximation-AllShifts ($kDFT$-Approximation with the added shifting presented at the end of Section 4), as well as $kDFT$-Approximation-BaseField and $kDFT$-Approximation-BaseField-AllShifts proposed in Section 4.

For practical applications the cases of interest are those where k is some small percentage (e.g. 5% or 10%) of the length N. In the tables these are the rows where the ratio d/N is below such a percentage.

One can notice that the $kDFT$-Approximation-BaseField algorithms are very successful in finding good error sequences for the majority of cases, the success rate being close to 100% for most of the sequences and divisors. The base field algorithms are giving only slightly lower average decrease in complexity compared to the extension field case. The shifting technique gives significant improvements. See for example the sequences of length 27, when a base field error sequence is found only in 47% of the cases for divisor 3, however the shifting technique gives significantly more successful approximation especially in the base field case.

A comparison with the optimal solution would be interesting, but exhaustive search is infeasible except for very small lengths. We implemented this test for all the 100 sequences of length 15 and $k = d = 3$. The average accuracy of the approximation in this experiment was 2.58 for $kDFT$-Approximation-BaseField and 2.03 for $kDFT$-Approximation-BaseField-AllShifts, where the accuracy is the ratio between the approximate value of $L_3(s)$ returned by each of the algorithms and the exact value calculated using an exhaustive technique. These results are not very good, but that is to be expected as the restricted search space is relatively small compared to the total space.

6 Concluding Remarks

In this paper, we present and evaluate a polynomial approximation algorithm for the computation of the k-error linear complexity of a sequence, by developping our previous approximation algorithm for the extension field k-error linear complexity, to only consider error sequences over the original field.

While the search space is still exponential, the complexity of the algorithm is polynomial, $\mathcal{O}(N^2 \log N \log \log N)$. Our experiments show that the algorithm is successful in finding good error sequences in the majority of the applicable cases.

References

1. Alecu, A., Sălăgean, A.: An approximation algorithm for computing the k-error linear complexity of sequences using the discrete fourier transform. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT 2008), Toronto, Canada, pp. 2414–2418 (July 2008)
2. Blahut, R.E.: Transform techniques for error control codes. IBM J. Res. Develop. 23(3), 299–315 (1979)
3. Ding, C., Xiao, G., Shan, W.: The stability Theory of Stream Ciphers. In: Ding, C., Shan, W., Xiao, G. (eds.) The Stability Theory of Stream Ciphers. LNCS, vol. 561. Springer, Heidelberg (1991)
4. GAP. Groups, Algorithms, and Programming, Version 4.4.9 (2006), http://www.gap-system.org/

5. Grönwall, T.H.: Some asymptotic expressions in the theory of numbers. Trans. Amer. Math. Soc. 14, 113–122 (1913)
6. Kaida, T., Uehara, S., Imamura, K.: An algorithm for the k-error linear complexity of sequences over $GF(p^m)$ with period p^n, p a prime. Inform. Comput. 151, 134–147 (1999)
7. Lauder, A.G.B., Paterson, K.G.: Computing the error linear complexity spectrum of a binary sequence of period 2^n. IEEE Trans. Information Theory 49, 273–280 (2003)
8. Massey, J.L., Serconek, S.: A Fourier Transform Approach to the Linear Complexity of Nonlinearly Filtered Sequences. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 332–340. Springer, Heidelberg (1994)
9. Stamp, M., Martin, C.F.: An algorithm for the k-error linear complexity of binary sequences of period 2^n. IEEE Trans. Information Theory 39, 1398–1401 (1993)
10. Zhou, J., Xu, X.: An algorithm for the k-error linear complexity of a sequence with period $2p^n$ over $GF(q)$ (2005), http://arxiv.org/abs/cs/0512039

Transformations on Irreducible Binary Polynomials

Jean-Francis Michon and Philippe Ravache

Université de Rouen, LITIS EA 4108
BP 12 - 76801 Saint-Étienne du Rouvray cedex, France
{jean-francis.michon,philippe.ravache}@litislab.fr

Abstract. Using the natural action of $GL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ over $\mathbb{F}_2[X]$, one can define different classes of polynomials strongly analogous to self-reciprocal irreducible polynomials. We give transformations to construct polynomials of each kind of invariance and we deal with the question of explicit infinite sequences of invariant irreducible polynomials in $\mathbb{F}_2[X]$. We generalize results obtained by Varshamov, Wiedemann, Meyn and Cohen and we give sequences of invariant irreducible polynomials. Moreover we explain what happens when the given constructions fail. We also give a result on the order of the polynomials of one of the classes: the alternate irreducible polynomials.

Keywords: irreducible polynomials, finite fields, sequences of irreducible invariant polynomials.

1 Introduction

In [6], we studied the natural action of the 6 elements group $\mathfrak{S}_3 \simeq GL_2(\mathbb{F}_2) \simeq PGL_2(\mathbb{F}_2)$ on the set

$$\mathcal{I} = \{P \in \mathbb{F}_2[X] |\ P \text{ irreducible}\} \setminus \{X, X+1\}.$$

This action of $\mathfrak{S}_3$ on $\mathcal{I}$, is defined by the two operations

$$P^+(X) = P(X+1)$$
$$P^*(X) = X^{\deg P} P(\frac{1}{X}).$$

The action of all other elements of $\mathfrak{S}_3$ are obtained by compositions of these two operations. We shall write for example P^{*+} for $(P^*)^+$.

Definition 1. *The **hexagon** of $P \in \mathcal{I}$ is the orbit of P :*

$$Hex(P) = \{P^\sigma | \sigma \in \mathfrak{S}_3\}.$$

*The **degree** of a hexagon is the degree of its polynomials. When $Card(Hex(P)) < 6$ we say that the hexagon is **degenerate**.*

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 166–180, 2010.

Such an orbit has 1, 2, 3 or 6 elements according to the isotropy subgroup of P. In $\mathfrak{S}_3$, apart from the trivial subgroups, we have 3 subgroups of order 2, and one of order 3. Each of them will give a family of invariant irreducible polynomials. The case of 1 element hexagon is easy : $\mathcal{I}(2) = \{X^2+X+1\}$ is the only 1 element degenerate hexagon. This polynomial is the only fixed point of the action.

Let us define for any integer $n > 1$

$$\mathcal{I}(n) = \{P \in \mathcal{I} | \deg P = n\},$$

then this grading of $\mathcal{I}$ is stable under the action (but this is not true for $n = 1$).

2 Self-Reciprocity and the 3 Elements Degenerate Hexagons

Self-reciprocal polynomials are invariant under the action of one subgroup of order 2 (generated by $*$ operation). In fact there is no reason to focus on one subgroup because they are all conjugate.

2.1 The Invariant Polynomials

Definition 2. *Let P be a polynomial, P is said to be **self-reciprocal** (resp. **periodic**, **median**) if $P^* = P$ (resp. $P^+ = P$, $P^{*+*} = P^{+*+} = P$). We easily check that these polynomials are of even degree.*

Definition 3. *Let P and Q, $P \neq Q$, be two polynomials of $\mathcal{I}$, $\{P, Q\}$ is said to be a **reciprocal pair** (resp. **periodic pair**, **median pair**) if $Q = P^*$ (resp. $Q = P^+$, $Q = P^{*+*}$). As the polynomials of a pair have the same degree, by extension, it will also be the degree of the pair.*

Definition 4. *A **3 elements degenerate hexagon** is made of a self-reciprocal irreducible polynomial P, a median irreducible polynomial Q and a periodic irreducible polynomial R such that:*

The next theorem extends Meyn's one (see [4], Theorem 1) to the periodic and median polynomials:

Theorem 1

i) Each self-reciprocal (resp. periodic, median) irreducible polynomial of degree $2n$ ($n \geq 1$) is a factor of the polynomial

$$H_{r,n}(X) = X^{2^n+1} + 1$$

$$\textit{(resp. } H_{p,n}(X) = X^{2^n} + X + 1, \quad H_{m,n}(X) = X^{2^n} + X^{2^n-1} + 1\textit{).}$$

ii) Each irreducible factor of degree ≥ 2 of $H_{r,n}$ (resp. $H_{p,n}$, $H_{m,n}$) is a self-reciprocal (resp. periodic, median) polynomial of degree $2d$, where d divides n such that n/d is odd.

Proof. In [4], Meyn proves the theorem for self-reciprocal polynomials. We trivially extend it to the periodic (resp. median) polynomials noting that, on the one hand, $H_{p,n} = H_{r,n}^{+*}$ (resp. $H_{m,n} = H_{r,n}^{+}$) and on the other hand, a periodic (resp. median) irreducible polynomial is obtained from a self-reciprocal one, applying the transformation $+^*$ (resp. $+$) on it. □

2.2 The Quadratic Transformations

Definition 5. *We define the maps* ϕ_p, ϕ_m, ϕ_r: $\mathbb{F}_2[X] \to \mathbb{F}_2[X]$ *by*

$$\phi_p(P) = P(X^2 + X)$$
$$\phi_m(P) = \phi_p(P)^* = X^{2n}\, P(\frac{X+1}{X^2})$$
$$\phi_r(P) = \phi_p(P)^{*+} = (X^2+1)^n\, P(\frac{X}{X^2+1}).$$

The image by ϕ_p (resp. ϕ_m, ϕ_r) of a polynomial of $\mathcal{I}(n)$ is a periodic (resp. median, self-reciprocal) polynomial of degree $2n$ but is not always irreducible.

Proposition 1. *Let* $\mathcal{P} \subset \mathbb{F}_2[X]$ *be the subset of periodic polynomials, then* $\mathcal{P}$ *is a sub algebra of* $\mathbb{F}_2[X]$ *and* $\phi_p : \mathbb{F}_2[X] \to \mathcal{P}$ *is an algebra isomorphism.*

Proof. Only ϕ_p surjectivity deserves proof. Let Q be a periodic polynomial, its degree is an even integer $2n$. Then, $Q + (X^2 + X)^n$ is a periodic polynomial of degree $< 2n$. Iterating this process, we obtain a polynomial P of degree n such that $\phi_p(P) = Q$. □

We call **trace** of a polynomial $P \neq 0$ of degree n, and write $Tr(P)$, the X^{n-1} coefficient.

The following theorem and corollary can be seen as an extension of Meyn's Lemma (see [4], Lemma 4):

Theorem 2. *Let* $P \in \mathcal{I}(n)$. *If* $Tr(P) = 1$, *then* $\phi_p(P)$ *is a periodic irreducible polynomial of degree* $2n$, *else,* $\phi_p(P)$ *is the product of two irreducible polynomials of degree* n, *which form a periodic pair.*

Conversely, let Q *be an irreducible periodic polynomial of degree* $2n$ *(resp. let* $\{R, R^+\}$ *be a periodic pair of degree* n*), then, there exists a unique* $P \in \mathcal{I}(n)$ *such that* $\phi_p(P) = Q$ *(resp.* $\phi_p(P) = RR^+$*).*

Proof. Let $P \in \mathcal{I}(n)$ and let h be a root of $\phi_p(P)$, then $h^2 + h$ is a root of P by definition and generates the field $\mathbb{F}_{2^n}$. This implies that $\mathbb{F}_2[h] \supset \mathbb{F}_2[h^2+h] = \mathbb{F}_{2^n}$. In turn h cannot be a root of a polynomial whose degree is $< n$. We conclude that the irreducible decomposition of $\phi_p(P)$ contains only polynomials of degree $\geq n$. This leaves only two cases: $\phi_p(P)$ is irreducible of degree $2n$ or is the product of two irreducible polynomials A and B of degree n.

Suppose we are in the second case : AB being periodic, we have two possibilities: $B = A^+$ or A and B are themselves periodic. This last event cannot

occur because if $\phi_p(P) = AB$ with A and B periodic and irreducible, then by Proposition 1, there exist U and V such that $\phi_p(U) = A$ and $\phi_p(V) = B$. Then $\phi_p(P) = \phi_p(U)\phi_p(V) = \phi_p(UV)$ and $P = UV$. This would contradict the irreducibility of P.

We now prove that the trace dispatches the two cases. Suppose $\phi_p(P) = AB$, then we have $h \in \mathbb{F}_{2^n}$. We call $a = h^2+h \in \mathbb{F}_{2^n}$, then $Tr(a) = Tr(h^2)+Tr(h) = 0$ and $Tr(P) = 0$ because a is a root of P. Conversely if $Tr(P) = 0$ then $Tr(a) = 0$ for any root a of P. Then it is well known that the equation $X^2 + X = a$ has roots in $\mathbb{F}_{2^n}$ (using the "half-trace"). This means that $\phi_p(P)$ is reducible since it has a root in $\mathbb{F}_{2^n}$.

We prove now the "conversely" part of the theorem.

Let Q be an irreducible periodic polynomial of degree $2n$ and let h be a root of Q, then, $h+1$ is also a root of Q and, from Theorem 1, we know that $h+1 = h^{2^n}$. Now, if

$$\mathcal{E} = \{h^{2^i} | 0 \leq i < n\},$$

$$Q = \prod_{h \in \mathcal{E}} (X + h)(X + h + 1) = \prod_{h \in \mathcal{E}} (X^2 + X + h(h + 1)).$$

We take

$$P = \prod_{h \in \mathcal{E}} (X + h(h + 1)),$$

it is then clear that $\phi_p(P) = Q$. Let $h(h+1)$ be a root of P, then any other root can be written $h^{2^k}(h^{2^k}+1) = [h(h+1)]^{2^k}$ for some integer $k \geq 1$. In other terms, the roots of P are conjugate by Frobenius. This implies that $P \in \mathbb{F}_2[X]$. If P is reducible, say $P = ST$ then $\phi_p(P) = \phi_p(S)\phi_p(T) = Q$. This decomposition is trivial because Q is irreducible. This forces S or T to be trivial and P to be irreducible. Now, if P is not unique, there exists another irreducible polynomial S such that $\phi_p(S) = Q$, then $h(h + 1)$ is a root of S by definition, so S and P have the same roots and consequently, $S = P$.

In the same manner, let $\{R, R^+\}$ be a periodic pair of degree n and $\mathcal{F}$ be the set of the n roots of R then taking

$$P = \prod_{a \in \mathcal{F}} (X + a(a + 1)),$$

we obtain a $P \in \mathbb{F}_2[X]$ such that $\phi_p(P) = RR^+$.

Suppose $P = ST$ with two non constant polynomials in $\mathbb{F}_2[X]$, then $\phi_p(P) = \phi_p(S)\phi_p(T) = RR^+$. Consequently, we can write $\phi_p(S) = R$ and this is a contradiction because $\phi_p(S)$ is periodic and R is not, so P is irreducible. The unicity of P is proved like previously. □

Corollary 1. *Let $P \in \mathcal{I}(n)$, if $Tr(P) = 1$, then, $\phi_r(P)$(resp. $\phi_m(P)$) is a self-reciprocal (resp. median) irreducible polynomial of degree $2n$, else, it is the product of two irreducible polynomials of degree n, which form a reciprocal (resp. median) pair.*

Conversely, let Q be an irreducible self-reciprocal (resp. median) polynomial of degree $2n$, then, there exists $P \in \mathcal{I}(n)$ such that $\phi_r(P) = Q$ (resp. $\phi_m(P) = Q$). In the same way, let $\{R, R^*\}$ (resp. $\{R, R^{+*+}\}$) be a reciprocal (resp. median) pair of degree n, then, there exists a unique $P \in \mathcal{I}(n)$ such that $\phi_r(P) = RR^*$ (resp. $\phi_m(P) = RR^{+*+}$).

Proof. We prove the corollary only for the self-reciprocal case, the median case being similar.

If $Tr(P) = 1$, from Theorem 2, we know that $\phi_p(P)$ is periodic in $\mathcal{I}(2n)$. Using Definitions 4 and 5, we see that $\phi_r(P)$ is self-reciprocal in $\mathcal{I}(2n)$. If $Tr(P) = 0$, there exists a periodic pair $\{S, S^+\}$ of degree n such that $\phi_p(P) = SS^+$. Now, as the transformations * and $^+$ are distributive with regard to the multiplication in $\mathbb{F}_2[X]$, $\phi_r(P) = (SS^+)^{*+} = S^{*+}S^{+*+} = S^{*+}(S^{*+})^*$, which is a reciprocal pair of degree n.

Using Theorem 2, Definitions 4 and 5, the proof of the second part is obvious. □

We get a simple way to construct 3 and 6 elements hexagons: let P be an irreducible polynomial of degree n such that $Tr(P) = 1$, then $\{\phi_r(P), \phi_m(P), \phi_p(P)\}$ is a 3 elements degenerate hexagon of degree $2n$. This is illustrated by the left-side diagram. If $Tr(P) = 0$, we have the right-side diagram, where $\{Q_1, Q_2\}$, $\{Q_3, Q_4\}$ and $\{Q_5, Q_6\}$ are the pairs such that $\phi_r(P) = Q_1Q_2$, $\phi_m(P) = Q_3Q_4$ and $\phi_p(P) = Q_5Q_6$ respectively.

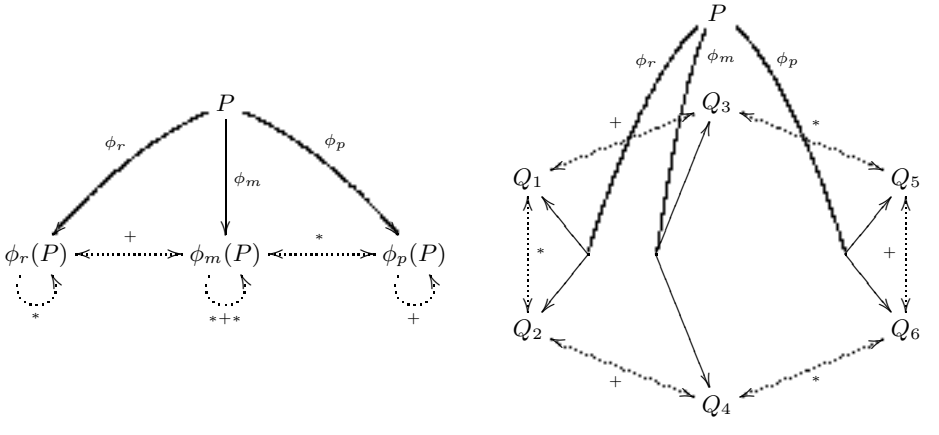


Fig. 1. Construction of hexagons by ϕ_r, ϕ_m and ϕ_p from an irreducible polynomial P such that $Tr(P) = 1$ (*left*) and $Tr(P) = 0$ (*right*).

2.3 Infinite Sequences of Self-reciprocal, Median and Periodic Irreducible Polynomials

Let $P \in \mathcal{I}(n)$, we denote $c_1(P)$ the coefficient of X in P.

Sequences of invariant irreducible polynomials appear implicitely in Varshamov [8] and more explicitely in Wiedemann [9], Meyn [4] and Cohen [1]. These sequences appear in papers devoted to a more general problem: the construction of irreducible polynomials (see Kyuregyan [2] and [3] for recent references).

Our approach shows that, actually, there are three strongly analogous families of invariant irreducible polynomials corresponding to the three conjugated 2-groups of $\mathfrak{S}_3$. The following theorem is an easy extension of the construction of sequences of self-reciprocal irreducible polynomials given by Meyn and Cohen to the median and periodic cases.

Theorem 3. *Let $P \in \mathcal{I}(n)$ be such that $c_1(P) = Tr(P) = 1$. Starting from $\phi_r(P)$ (resp. $\phi_m(P)$, $\phi_p(P)$) and iterating the transformation $P \to \phi_r(P)$ (resp. $P \to \phi_m(P^+)$, $P \to \phi_p(P^{*+})$) one generates an infinite sequence of self-reciprocal (resp. median, periodic) irreducible polynomials of degree $2^i n$, $i > 0$.*

Proof. We know by Theorem 2 that $\phi_r(P)$ is self-reciprocal and irreducible. By explicit computation, we see that $Tr(\phi_r(P)) = 1$ and because of self-reciprocity, $c_1(\phi_r(P)) = 1$. So by recurrence, we get a sequence of self-reciprocal irreducible polynomials. Then, using the Definitions 4 and 5, we obtain sequences of median and periodic polynomials. □

2.4 Equivalent Transformations

In Definition 5 we defined ϕ_m and ϕ_r from ϕ_p in a natural way. Other transformations can be used instead of ϕ_p. They are obtained by choosing one "right" action by an element of the group $\mathfrak{S}_3$ before applying ϕ_p.

We construct in this way new transformation ϕ'_p and consequently new ϕ'_m and ϕ'_r. We recover in this way the transformation ϕ'_r quoted in Section 2.3 which is more frequently used in the mathematical literature for constructing self-reciprocal polynomial. The results of the preceding sections can be transposed with small changes. The following table lists these transformations:

Table 1. Equivalent quadratic transformations

ϕ'_p	$\phi'_m = * \circ \phi'_p$	$\phi'_r = + \circ * \circ \phi'_p$
$P(X^2+X+1) = \phi_p(P^+)$	$X^{2n}P(\frac{X^2+X+1}{X^2})$	$(X^2+1)^n P(\frac{X^2+X+1}{X^2+1})$
$(X^2+X+1)^n P(\frac{1}{X^2+X+1}) = \phi_p(P^{*+})$	$(X^2+X+1)^n P(\frac{X^2}{X^2+X+1})$	$(X^2+X+1)^n P(\frac{X^2+1}{X^2+X+1})$
$(X^2+X+1)^n P(\frac{X^2+X}{X^2+X+1}) = \phi_p(P^{+*+})$	$(X^2+X+1)^n P(\frac{X+1}{X^2+X+1})$	$(X^2+X+1)^n P(\frac{X}{X^2+X+1})$
$(X^2+X)^n P(\frac{X^2+X+1}{X^2+X}) = \phi_p(P^{+*})$	$(X+1)^n P(\frac{X^2+X+1}{X+1})$	$X^n P(\frac{X^2+X+1}{X})$
$(X^2+X)^n P(\frac{1}{X^2+X}) = \phi_p(P^*)$	$(X+1)^n P(\frac{X^2}{X+1})$	$X^n P(\frac{X^2+1}{X})$

3 Alternate Polynomials and 2 Elements Degenerate Hexagons

We introduced in [6] the class of alternate polynomials over $\mathbb{F}_2$:

Definition 6

- *A polynomial P is said to be **alternate** if $P^{*+} = P^{+*} = P$.*
- *Let $P \in \mathcal{I}$, if P is not alternate, then $\{P, P^{*+}, P^{+*}\}$ is said to be an **alternate triplet**. P, P^{*+} and P^{+*} are of the same degree, so by extension, the degree of an alternate triplet is the degree of its polynomials.*
- *A **2 elements degenerate hexagon** is made of two distinct alternate irreducible polynomials P and Q such that:*

$$P \overset{+/*}{\dashleftarrow\!\!\dashrightarrow} Q \ .$$

We refer again to [6] for the details of the following:

Proposition 2. *The irreducible alternate polynomials are exactly the irreducible factors of the polynomials*

$$B_k(X) = X^{2^k+1} + X + 1,$$

for $k \in \mathbb{N}$.

*If P is alternate then $\deg P \equiv 0 \mod 3$ or $P = X^2 + X + 1$. If $\deg P = 3m$ then either P divides B_m and B^*_{2m}, or P divides B^*_m and B_{2m}. In the first case we say that P has **type** 1, in the second P has **type** 2.*

Corollary 2. *The order of an alternate irreducible polynomial of degree $3n$ divides $2^{2n} + 2^n + 1$.*

Proof. Let $P \in \mathcal{I}(n)$ be alternate. We suppose P is of type 1. Let a be a root of P, then, from Proposition 2, $a^{2^n+1}+a+1 = 0$. We put this equation to the 2^n, we get $a^{2^n(2^n+1)}+a^{2^n}+1 = 0$. Now, multiplying by a, we have $a^{2^n(2^n+1)+1}+a^{2^n+1}+a = 0$. Finally, we replace the term in the middle using the first equation, we obtain $a^{2^n(2^n+1)+1} + 1 = 0$.

If P is of type 2, then P^* is of type 1 and as P and P^* have same order, this concludes the proof. □

3.1 The Cubic Transformation

Let $P \in \mathbb{F}_2[X]$ of degree n, we define the map $\psi : \mathbb{F}_2[X] \to \mathbb{F}_2[X]$ by

$$\psi(P)(X) = (X^2 + X)^n \, P\left(\frac{X^3 + X^2 + 1}{X^2 + X}\right).$$

We verify that $\psi(P)$ is alternate.

Let ϵ and ϵ^2 be the roots of $X^2 + X + 1$. For any irreducible $P \neq X^2 + X + 1$ in $\mathbb{F}_2[X]$ we have $P(\epsilon) \in \{1, \epsilon, \epsilon^2\}$. The main result of this section is:

Theorem 4

- *Let $P \in \mathcal{I}(n)$, $n > 2$. If $P(\epsilon) \neq 1$ then $\psi(P)$ is an irreducible alternate polynomial of degree $3n$, else, $\psi(P) = RST$, where $\{R, S, T\}$ is an alternate triplet of degree n.*
- *Conversely, let $Q \in \mathcal{I}(3n)$, $n > 1$ be an alternate polynomial (resp. let $\{R, R^{+*}, R^{*+}\}$ be an alternate triplet of degree n), then there exists a unique $P \in \mathcal{I}(n)$ such that $\psi(P) = Q$ (resp. $\psi(P) = RR^{+*}R^{*+}$).*

To complete the theorem, we precise that the irreducible (alternate) polynomials of degree 3 are obtained from X and $X + 1$:

$$\psi(X) = X^3 + X^2 + 1 \text{ and } \psi(X + 1) = X^3 + X + 1,$$

and for the particular case $X^2 + X + 1$ (whose value in ϵ is 0), we have:

$$\psi(X^2 + X + 1) = (X^2 + X + 1)^3.$$

Before going into the proof of Theorem 4, we need to establish some results.

Let us take $P \in \mathcal{I}(n)$ with $n > 2$, $K = \mathbb{F}_{2^n}$ the splitting field of P, and h a root of $\psi(P)$, then $h \neq 0, 1$ and

$$a = \frac{h^3 + h^2 + 1}{h^2 + h} = h + \frac{1}{h} + \frac{1}{h + 1} \tag{1}$$

is a root of P. This implies $K \subset K(h)$.

As $h \neq 0, 1$, h is a root of the polynomial

$$T_a(X) = X^3 + (1 + a)X^2 + aX + 1. \tag{2}$$

3.2 Proof of the First Part of Theorem 4

Proposition 3. *Let w be a cubic root of $(\epsilon + a)(\epsilon + a^2)$, then the roots of (2) are*

$$h_i = 1 + a + \epsilon^i w + \frac{b}{\epsilon^i w},$$

with $i = 0$, 1 or 2, and $b = a^2 + a + 1$. Moreover, they verify the relations $h_1 = 1/(h_0 + 1)$ and $h_2 = 1 + 1/h_0$.

Proof. The formulas for the h_i are obtained by the classical Cardan's method:

The first step is to cancel the X^2 coefficient in

$$X^3 + (a + 1)X^2 + aX + 1 = 0.$$

We take $X' = X + 1 + a$ and $b = 1 + a + a^2$:

$$X'^3 + bX' + b = 0.$$

The second step is to use two variables u, v and take $X' = u + v$:

$$u^3 + v^3 + (u + v)(uv + b) + b = 0.$$

Choosing $uv = b$, if we can solve

$$\begin{cases} uv & = b \\ u^3 + v^3 & = b \end{cases}$$

in $\overline{K}$, we will have the roots of (2), they would be the

$$1 + a + u + v.$$

We can write:

$$\begin{cases} u^3 v^3 & = b^3 \\ u^3 + v^3 & = b, \end{cases}$$

which is equivalent to a second degree problem. If $Y = u^3$ then:

$$Y^2 + bY + b^3 = 0,$$

and dividing by b^2 we get:

$$\frac{Y^2}{b^2} + \frac{Y}{b} + b = 0.$$

We take $Z = Y/b$ (because $b \neq 0$):

$$Z^2 + Z + b = 0$$

$$Z^2 + Z + 1 + a + a^2 = 0$$

$$(Z + a)^2 + (Z + a) + 1 = 0.$$

So the solutions are $Z = a + \epsilon$ and $Z = a + \epsilon^2$. And we find:

$$u^3 = (1 + a + a^2)(a + \epsilon^2),$$

which can be written equivalently:

$$\begin{aligned} u^3 &= (a + \epsilon)(a + \epsilon^2)(a + \epsilon^2) \\ &= (a + \epsilon)(a^2 + \epsilon). \end{aligned}$$

So we can choose u as one of the three cubic roots of $(a+\epsilon)(a^2+\epsilon)$. The quantity $v = b/u$ is then determined uniquely. The roles of v and u can be exchanged.

We now establish the relations between the roots:

$$\begin{aligned} 1 + \frac{1}{h_0} &= h_0^2 + (1 + a)h_0 + a + 1 \quad \text{(from (2))} \\ &= w^2 + \frac{b^2}{w^2} + (1 + a)(w + \frac{b}{w}) + a + 1 \\ &= \frac{w^3}{w} + \frac{b^2 w}{w^3} + (1 + a)(w + \frac{b}{w}) + a + 1 \\ &= [\frac{b^2}{w^3} + 1 + a]w + [\frac{w^3}{b} + 1 + a]\frac{b}{w} + a + 1. \end{aligned}$$

Then using $b = (\epsilon + a)(\epsilon^2 + a)$ and $w^3 = (\epsilon + a)(\epsilon + a^2)$ we find:

$$1 + \frac{1}{h_0} = \epsilon^2 w + \frac{b}{\epsilon^2 w} + a + 1 = h_2.$$

The first relation can be obtained by the same trick. □

Lemma 1. *If $P(\epsilon) = 1$ and n is even (resp. odd), then $(\epsilon + a)(\epsilon + a^2)$ has cubic roots in $K = \mathbb{F}_{2^n}$ (resp. $K(\epsilon)$).*

Proof. Case n even: If $n = 2m$

$$\begin{aligned} P(\epsilon) &= (\epsilon + a)(\epsilon + a^2)(\epsilon + a^4)(\epsilon + a^8)\dots(\epsilon + a^{2^{2m-2}})(\epsilon + a^{2^{2m-1}}) \\ &= (\epsilon + a)(\epsilon + a^2)((\epsilon + a)(\epsilon + a^2))^4 \dots ((\epsilon + a)(\epsilon + a^2))^{2^{2m-2}}. \end{aligned}$$

So $P(\epsilon) = [(\epsilon + a)(\epsilon + a^2)]^k$ with

$$k = 1 + 4 + \dots + 2^{2(m-1)} = \frac{2^n - 1}{3}.$$

Let w be a cubic root of $(\epsilon + a)(\epsilon + a^2)$ in some extension of $\mathbb{F}_2$ (it always exists). Then, from what we have just said:

$$w^{2^n - 1} = w^{3.\frac{2^n - 1}{3}} = P(\epsilon) = 1,$$

so $w \in K$.

Case n odd: let $n = 2m+1$, we write $P(\epsilon)$ in two different ways, using Fermat's little theorem:

$$\begin{aligned} P(\epsilon) &= (\epsilon + a)(\epsilon + a^2)(\epsilon + a^4)(\epsilon + a^8)\dots(\epsilon + a^{2^{2m-2}})(\epsilon + a^{2^{2m-1}})(\epsilon + a^{2^{2m}}) \\ P(\epsilon) &= (\epsilon + a^{2^{2m+1}})(\epsilon + a^{2^{2m+2}})(\epsilon + a^{2^{2m+3}})(\epsilon + a^{2^{2m+4}})\dots(\epsilon + a^{2^{4m}})(\epsilon + a^{2^{4m+1}}). \end{aligned}$$

Multiplying these equalities, we get

$$\begin{aligned} P(\epsilon)^2 &= [(\epsilon + a)(\epsilon + a^2)][(\epsilon + a)(\epsilon + a^2)]^4 \dots [(\epsilon + a)(\epsilon + a^2)]^{2^{4m}} \\ &= [(\epsilon + a)(\epsilon + a^2)]^k, \end{aligned}$$

with

$$k = 1 + 4 + \dots + 2^{4m} = \frac{4^{2m+1} - 1}{3} = \frac{2^{2n} - 1}{3}.$$

Then

$$w^{2^{2n} - 1} = w^{3.\frac{2^{2n} - 1}{3}} = P(\epsilon)^2 = 1,$$

and $w \in K(\epsilon)$ because $[K(\epsilon) : \mathbb{F}_2] = 2n$. □

Proposition 4. *Let $P \in \mathcal{I}(n)$ be such that $P(\epsilon) = 1$, then, $\psi(P)$ is reducible.*

Proof. If n is even this is a direct consequence of the preceding Lemma and Proposition 3.

If n is odd, $w \in K(\epsilon)$ by the preceding lemma, so by Proposition 3 we have $K(h) \subset K(\epsilon)$. If $\psi(P)$ is irreducible then for any of its root h we have $[K(h) : \mathbb{F}_2] = 3n$ and $[K(h) : K] = 3$. This is a contradiction so $\psi(P)$ is reducible. □

Proposition 5. *Let $P \in \mathcal{I}(n)$, $n > 2$, the polynomial $\psi(P)$ has $3n$ distinct roots and*

$$\psi(P) = \prod_{k=0}^{n-1} T_{a^{2^k}}(X),$$

where $a \in K$ is any root of P.

Proof. If a is a root of P and if h is a root of T_a, then h is a root of $\psi(P)$. Let a' be another root of P, distinct from a, then, the set of roots of T_a is disjoint from the set of roots of $T_{a'}$ because of (11). As P is irreducible, all the roots of P are conjugate and distinct, which concludes the proof of the proposition. □

Proposition 6. *Let $P \in \mathcal{I}(n)$, $n > 2$, if $\psi(P)$ is reducible in $\mathbb{F}_2[X]$ then $\psi(P) = RST$, where $\{R, S, T\}$ is an alternate triplet of degree n, moreover $P(\epsilon) = 1$.*

Proof. Let h be a root of $\psi(P)$, we have seen that $K \subset K(h)$. Thus, the degree of the minimal polynomial of h is divisible by n and is $\leq 3n$. This implies that the irreducible factors of $\psi(P)$ in $\mathbb{F}_2[X]$ are at least of degree n, $< 3n$ and multiples of n. Consequently, one of the irreducible factor of $\psi(P)$ is of degree n. Let R be such a factor.

We consider R^{*+} and R^{+*}. They are polynomials of $\mathbb{F}_2[X]$ of degree n and their roots are roots of $\psi(P)$, thus, they divide $\psi(P)$. If R is not alternate, then we obtain an alternate triplet $\{R, R^{*+}, R^{+*}\}$ of degree n, as expected.

If R is alternate let h be a root of R and a such that

$$a = \frac{h^3 + h^2 + 1}{h^2 + h},$$

then, like previously, a is a root of P and $T_a(X)|R$ because h, $\frac{1}{h+1}$ and $\frac{h+1}{h}$ are distinct roots of R. As $R \in \mathbb{F}_2[X]$ is irreducible of degree n, its roots are the h^{2^k}, with $0 \leq k \leq n-1$. So, as Frobenius commutes with our group transformations, $T_{a^{2^k}}|R$ for every k. The $T_{a^{2^k}}$ are distinct because of the preceding proposition. It follows that R has $3n$ distinct roots which is a contradiction, so R cannot be alternate.

We can explicit the decomposition:

$$\psi(P) = R(X)(X+1)^n R\Big(\frac{1}{X+1}\Big) X^n R\Big(\frac{X+1}{X}\Big),$$

with $R \in \mathbb{F}_2[X]$ irreducible of degree $n > 2$, so $\psi(P)(\epsilon) = \epsilon^{3n} R(\epsilon)^3 = R(\epsilon)^3 = 1$.

Then, taking $X = \epsilon$ in the definition of ψ, we get $\psi(P)(\epsilon) = P(\epsilon^2)$. Consequently, $P(\epsilon^2) = P(\epsilon)^2 = 1$ and $P(\epsilon) = 1$. □

The Propositions 4 and 6 give a demonstration of the first part of Theorem 4.

3.3 Proof of the Second Part of Theorem 4

Proposition 7. *let $Q \in \mathcal{I}(3n)$, $n > 1$ be an alternate polynomial (resp. let $\{R, R^{+*}, R^{*+}\}$ be an alternate triplet of degree n), then, there exists a unique $P \in \mathcal{I}(n)$ such that $\psi(P) = Q$ (resp. $\psi(P) = RR^{+*}R^{*+}$).*

Proof. Let a be a root of Q, suppose $type(Q) = 1$ (type 2 is similar), then, $1/(1+a)$ and $1+1/a$ are also roots of Q, moreover, from Proposition 2, we know that $1 + 1/a = a^{2^n}$ and that $1/(1 + a) = a^{2^{2n}}$. Now, we take

$$\mathcal{E} = \{a^{2^i} | 0 \leq i < n\},$$

from what we have just seen, we can write

$$\begin{aligned} Q &= \prod_{a \in \mathcal{E}} (X + a)(X + 1 + \frac{1}{a})(X + \frac{1}{1+a}) \\ &= (X^2 + X)^n \prod_{a \in \mathcal{E}} \Big(\frac{X^3 + X^2 + 1}{X^2 + X} + \frac{a^3 + a^2 + 1}{a^2 + a} \Big). \end{aligned}$$

We take

$$P = \prod_{a \in \mathcal{E}} \Big(X + \frac{a^3 + a^2 + 1}{a^2 + a} \Big),$$

it is then clear that $\psi(P) = Q$. Let $\frac{a^3+a^2+1}{a^2+a}$ be a root of P, then any other root can be written $a^{2^k}(1 + 1/a^{2^k})(1/(1 + a^{2^k})) = [a(1 + 1/a)(1/(1 + a))]^{2^k}$ for some integer $k \geq 1$. In other terms, the roots of P are conjugate by Frobenius. This implies that $P \in \mathbb{F}_2[X]$.

To show that P is irreducible, we suppose that $P = ST$, with two non constant polynomials in $\mathbb{F}_2[X]$, then, as $\deg ST = degS + \deg T$:

$$\psi(P) = \psi(S)\psi(T) = Q,$$

and this decomposition is non trivial. This is impossible because Q is irreducible, so P is irreducible.

And to show that P is unique, we suppose that there exists another irreducible polynomial P_1 such that $\psi(P_1) = Q$, then, $\frac{a^3+a^2+1}{a^2+a}$ is a root of P_1 by definition, so P and P_1 have the same roots and $P = P_1$.

In the same way, let $\{R, R^{+*}, R^{*+}\}$ be an alternate triplet of degree n and $\mathcal{F}$ the set of the n roots of R, then, taking

$$P = \prod_{a \in \mathcal{F}} \Big(X + \frac{a^3 + a^2 + 1}{a^2 + a} \Big),$$

we obtain a P such that $\psi(P) = RR^{+*}R^{*+}$ and $P \in \mathbb{F}_2[X]$.

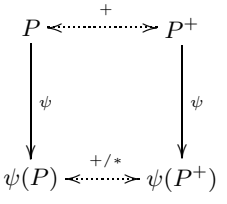
If P is reducible, we can write $P = ST$, with two non constant polynomials in $\mathbb{F}_2[X]$, then

$$\psi(P) = \psi(S)\psi(T) = RR^{+*}R^{*+}.$$

Consequently, we can write $\psi(S) = R$ and this is a contradiction because $\psi(S)$ is alternate and R is not, so P is irreducible. Finally, we can show that P is unique as we did in the first part. □

This completes the proof of Theorem 4.

As we did in the previous section, we propose a simple way to construct 2 elements hexagons: let $P \in \mathcal{I}(n)$ be such that $P(\epsilon) \neq 1$, then, using the fact that $\psi \circ + = + \circ \psi$ (the demonstration is obvious), we deduce that $\{\psi(P), \psi(P^+)\}$ is a 2 elements degenerate hexagon of degree $3n$. This is illustrated by the left-side diagram. On the other hand, if $P(\epsilon) = 1$, we have the right-side diagram, where $\{Q_1, Q_3, Q_5\}$ and $\{Q_2, Q_4, Q_6\}$ are the alternate triplets such that $\psi(P) = Q_1Q_3Q_5$ and $\psi(P^+) = Q_2Q_4Q_6$ respectively:



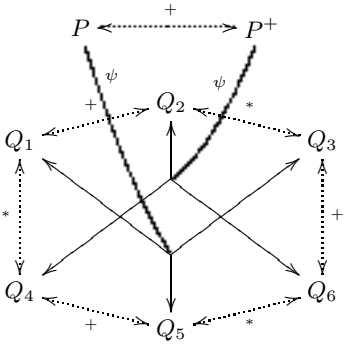


Fig. 2. Construction of hexagons by ψ from an irreducible polynomial P such that $P(\epsilon) \neq 1$ (*left*) and $P(\epsilon) = 1$ (*right*)

3.4 Infinite Sequences of Irreducible Alternate Polynomials

Proposition 8. *If P is an irreducible alternate polynomial of degree > 2, then $\psi(P)$ is an irreducible alternate polynomial.*

Proof. Let P be an irreducible alternate polynomial, by Theorem 4, $P = \psi(Q)$ for some irreducible Q, then $P(\epsilon) = \epsilon$ or ϵ^2. By the same theorem $\psi(P)$ is irreducible and alternate. □

Theorem 5. *Let $P \in \mathcal{I}(n)$ be such that $P(\epsilon) = \epsilon$ or ϵ^2, then the iteration ψ on P generates a sequence of alternate irreducible polynomials of degree $3^i n$, $i > 0$.*

Proof. Theorem 4 and Proposition 8 prove this theorem. □

3.5 Computation of the Type of the Alternate Irreducible Polynomials

Another consequence of Theorem 4 is that it gives a simple way to compute the type:

Theorem 6. *Let Q be an alternate irreducible polynomial of degree > 2 then its type is 1 (resp. 2) if and only if $Q(\epsilon) = \epsilon$ (resp. $Q(\epsilon) = \epsilon^2$).*

Proof. If $\deg Q = 3$, we verify the theorem by calculus. We now suppose that $\deg Q = 3n$, $n > 1$. We know from the preceding that $Q = \psi(P) \in \mathcal{I}(3n)$ for some irreducible polynomial P and $Q(\epsilon) = P(\epsilon)^2$.

If n is even, let h_0 be a root of Q, then with the notations used in Proposition 3 we have $h_0 = 1 + a + w + \frac{b}{w}$. Consequently:

$$h_0^{2^n} = 1 + a + w^{2^n} + \frac{b}{w^{2^n}}.$$

From the demonstration of Lemma 1 we have $w^{2^n} = P(\epsilon)w$, and

$$h_0^{2^n} = 1 + a + P(\epsilon)w + \frac{b}{P(\epsilon)w}.$$

If $Q(\epsilon) = \epsilon$ (resp. ϵ^2), then $P(\epsilon) = \epsilon^2$ (resp. ϵ) and using again Theorem 4:

$$h_0^{2^n} = 1 + \frac{1}{h_0} \quad (\text{ resp. } h_0^{2^n} = \frac{1}{h_0 + 1}\ ).$$

This is equivalent to say that Q is of type 1 (resp. type 2).

If n is odd the demonstration follows the same line except that we must use $w^{2^{2n}} = P(\epsilon)^2 w = Q(\epsilon)w$. We compute:

$$h_0^{2^{2n}} = 1 + a + Q(\epsilon)w + \frac{b}{Q(\epsilon)w}.$$

If $Q(\epsilon) = \epsilon$ (resp. ϵ^2), then $P(\epsilon) = \epsilon^2$ (resp. ϵ). We obtain:

$$h_0^{2^{2n}} = \frac{1}{h_0 + 1} \quad (\text{ resp. } h_0^{2^{2n}} = 1 + \frac{1}{h_0}\ ).$$

This implies (by iteration for example) that:

$$h_0^{2^n} = 1 + \frac{1}{h_0} \quad (\text{ resp. } h_0^{2^n} = \frac{1}{h_0 + 1}\ ),$$

and Q has type 1 (resp. 2). □

3.6 Equivalent Transformations

Other cubic transformations can be used instead of ψ. As previously, they are obtained by a right action of the group elements on ψ.

Table 2. Equivalent cubic transformations

ψ'
$(X^2+X)^n P(\frac{X^3+X+1}{X^2+X}) = \psi(P^+)$
$(X^3+X+1)^n P(\frac{X^2+X}{X^3+X+1}) = \psi(P^{*+})$
$(X^3+X+1)^n P(\frac{X^3+X^2+1}{X^3+X+1}) = \psi(P^{+*+})$
$(X^3+X^2+1)^n P(\frac{X^3+X+1}{X^3+X^2+1}) = \psi(P^{+*})$
$(X^3+X^2+1)^n P(\frac{X^2+X}{X^3+X^2+1}) = \psi(P^*)$

4 Conclusion

To conclude, in this paper, we defined the different classes of irreducible polynomials obtained by the action of $GL_2(\mathbb{F}_2)$ on $\mathbb{F}_2[X]$. We gave transformations to get invariant polynomials of each class, ways to generate infinite sequences of them and we showed the perfect analogy between self-reciprocal irreducible polynomials and alternate ones.

Now, the perspectives would be to study the action of $GL_2(\mathbb{F}_q)$ on $\mathbb{F}_q[X]$. For that, the first step would be the action of $GL_2(\mathbb{F}_{2^n})$ on $\mathbb{F}_{2^n}[X]$.

Acknowledgment. For our computations, we used the open source Mathematics software SAGE [7], so, we would like to thank the developers and contributors of SAGE. We also thank the reviewers for helping us to clarify the paper.

References

1. Cohen, S.D.: The Explicit Construction of Irreducible Polynomials over Finite Fields. Designs, Codes and Cryptography 2, 169–174 (1992)
2. Kyuregyan, M.: Recurrent Methods for Constructing Irreducible Polynomials over GF(2s). Finite Fields and Their Applications 8(3), 52–68 (2002)
3. Kyuregyan, M.: Iterated Constructions of Irreducible Polynomials over Finite Fields with Linearly Independant Roots. Finite Fields and Their Applications 10(1), 323–341 (2004)
4. Meyn, H.: On the Construction of Irreducible Self-reciprocal Polynomials over Finite Fields. Appl. Algebra Eng. Comm. Comp. 1, 43–53 (1990)
5. Meyn, H., Götz, W.: Self-reciprocal Polynomials over Finite Fields. Publ. IRMA Strasbourg 413/S-21, 82–90 (1990)
6. Michon, J.-F., Ravache, P.: On Different Families of Invariant Irreducible Polynomials over GF(2). Finite Fields and Their Applications 16(3), 163–174 (2010)
7. SAGE, http://www.sagemath.org
8. Varshamov, R.R.: A General Method of Synthesis for Irreducible Polynomials over Galois Fields. Soviet Math. Dokl. 29, 334–336 (1984)
9. Wiedemann, D.: An Iterated Quadratic Extension of GF(2). Fibonacci Quart 26, 290–295 (1988)

Power Permutations in Dimension 32

Emrah ÇakÇak[1] and Philippe Langevin[2]

[1] Department of Mathematics, Mimar Sinan Fine Arts University
emrah.cakcak@msu.edu.tr
[2] Imath, université du sud Toulon Var.
langevin@univ-tln.fr
http://langevin.univ-tln.fr

Abstract. In this note, we analyze power permutations having a three valued spectrum. We give new results and new proofs of results previously obtained by coding theory. We apply them to prove that Hellesth's conjecture is true for dimension 32.

1 Introduction

Let m be a positive integer. Let L a finite field of order $q = 2^m$. Let μ be the canonical additive character of L, defined as $\mu(x) = (-1)^{\mathrm{Tr}(x)}$ where $\mathrm{Tr}(x)$ is the absolute trace of x. Let f be a mapping from L into L. The *Fourier coefficient* of f at $a \in L$ is defined by

$$\widehat{f}(a) = \sum_{x \in L} \mu(f(x) + a.x).$$

In this paper, we analyze the situation where a power permutation $f : x \mapsto x^d$ (d coprime to $q-1$) has a three valued spectrum :

$$\mathrm{spec}\, f = \{\widehat{f}(a) \mid a \in L\} = \{0, A, B\}.$$

One can already remark that the spectrum corresponding to the exponent d is exactly the same as the spectrum of the exponents $2^i d$ and $2^i d^{-1}$. We will say that these exponents are equivalent and we denote by $\sim$ this relation.

From the numerical experiments done in the framework of sequences in the seventies, i.e. crosscorrelation of maximal sequences and their decimations, one of the main conjecture in this context is :

Conjecture 1. If the spectrum of a power permutation takes two distinct non zero values A and B then $A + B = 0$.

A secondary conjecture, see [3], is :

Conjecture 2 (Helleseth). If m is a power of 2 the spectrum of a power permutation takes at least four values except the trivial case $d \sim 1$, in which it takes only two values.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 181–187, 2010.

It is known [2] that the first conjecture implies the second one. The goal of this note is to prove Helleseth's conjecture for dimension 32. Before to continue in the direction of the above conjecture, it is interesting to see that some more general claims on the spectra of power permutations are false [5].

Let $\min(d)$ be the minimal value of the absolute value of the non zero Fourier coefficient of x^d.

- It is wrong to claim that $\min(d)$ is always a power of two. There exist 3 (and only 3, for $m \leq 25$) counter examples, they are in dimension 24.
- It is wrong to claim that $\mathrm{spec}\,(d)$ contains the two values $\pm\min(d)$. There are 3 counter-examples in dimension 18, and 3 others in dimension 21.

If we denote by $\mathrm{nbz}\,(d)$ the number of Fourier coefficients of x^d which are equal to zero, the numerical experiments indicate that for all d, $\mathrm{nbz}\,(d) \geq \mathrm{nbz}\,(-1)$, a very strange fact remarked by Leander, checked up to $m = 25$. One can risk to a conjecture that has every appearance of difficulty. Indeed, on one hand, we know (see [4]) that $\mathrm{nbz}\,(-1)$ is greater or equal to the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{1-4q})$, and on another hand another conjecture proposed by Helleseth claiming $\mathrm{nbz}\,(d) > 1$ is still open.

2 Basic Facts

For any integer n, $\mathrm{val}_2(n)$ will denote the dyadic valuation of n i.e. the greater integer r such that 2^r divides n. The valuation of a power permutation x^d , denoted by $\mathrm{val}\,(d)$, is defined to be the minimal dyadic valuation of the Fourier coefficients of x^d.

Proposition 1. *For all m, and all d*

$$\mathrm{val}\,(d) = \min_{1 \leq j < q-1} \mathrm{wt}\,(dj) + \mathrm{wt}\,(-j)$$

where $\mathrm{wt}\,(x)$ *denotes the binary weight of the positive residue of x modulo $q-1$.*

The above proposition is often seen as a consequence of divisibility McEliece Theorem in coding theory. It is also a straightforward consequence, see [6], of Stickelberger's congruences on Gauss sums.

In the rest of the paper we assume that m is even, we denote by K the subfield of index 2 in L and we denote by μ_K the canonical additive character of K, for all $x \in L$:

$$\mu(x) = \mu_K(\mathrm{Tr}_{L/K}(x)), \quad \mathrm{Tr}_{L/K}(x) = x + x^{\sqrt{q}}.$$

It is easy but important to see that $\mathrm{Tr}_{L/K}(x) = 0$ iff $x \in K$. Let A, B be the nonzero Fourier coefficients of a power permutation, $f(x) = x^d$, with three valued spectrum. We denote by x_A, x_B and x_Z the number of times each Fourier coefficient A, B and 0 appears, and by α and β the dyadic valuations of A and B. We also assume that $\alpha \leq \beta$. From Parseval identity and Fourier inversion, we have

$$\begin{pmatrix} A & B \\ A^2 & B^2 \end{pmatrix} \begin{pmatrix} x_A \\ x_B \end{pmatrix} = \begin{pmatrix} q \\ q^2 \end{pmatrix}$$

solving this system, we get

$$x_A = \frac{q(q-B)}{A(A-B)}, \quad x_B = \frac{q(A-q)}{B(A-B)}. \quad \frac{AB}{q} x_Z = q - (A+B) + AB.$$

We will see that the dyadic valuation of $\frac{AB}{q}$ plays an important role. This value, which obviously depends on d, will be denoted by r_d, and we will see later that r_d is a positive integer.

Lemma 1. *Given $a \in L^\times$, we have the relation:*

$$\sum_{c \in K} \widehat{f}(ac) = \begin{cases} q, & a \in K; \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. Indeed,

$$\begin{aligned} \sum_{c \in K} \widehat{f}(ac) &= \sum_{c \in K} \sum_{x \in L} \mu(x^d + acx) = \sum_{x \in L} \mu(x^d) \sum_{c \in K} \mu(acx) \\ &= \sqrt{q} \sum_{ax \in K} \mu(x^d) = \sqrt{q} \sum_{x \in K} \mu(a^{-d} x^d) \\ &= \sqrt{q} \sum_{x \in K} \mu_K\left(\mathrm{Tr}_{L/K}(a^{-d})\, x^d\right) \\ &= q\delta_K(a). \end{aligned}$$

□

Lemma 2. *In the case of a three valued spectrum, the positive Fourier coefficient is greater than $\sqrt{q}$.*

Proof. Use Lemma 1 with $a = 1$. □

Lemma 3. *Let $f(x) = x^d$ be a power permutation having of a three valued spectrum. If m is a power of 2 then the dyadic valuation of $\widehat{f}(1)$ is greater than* $\mathrm{val}\,(d)$.

Proof. It is an application of Stickelberger's congruences. Denoting by J the set of residues modulo $q-1$ such that

$$J = \{1 \le j < q-1 \mid \mathrm{wt}\,(dj) + \mathrm{wt}\,(-j) = \mathrm{val}\,(d)\}.$$

Since f is not linear, we have (see [6] for details),

$$\widehat{f}(1) \equiv 2^{\mathrm{val}\,(d)} |J| \pmod{2^{\mathrm{val}\,(d)+1}}.$$

Since m is a power of 2, the cardinality of a cyclotomic class of $j \neq 0$ modulo $(q-1)$ is even. The set J is a union of cyclotomic classes, its cardinality must be even. □

3 Fourier Analysis

Let $N_n(u,v)$ be the number of solutions of the system.

$$f(x_1) + f(x_2) + \ldots + f(x_n) = v$$
$$x_1 + x_2 + \ldots + x_n = u$$

Let S_n be the character sum

$$\sum_{x_1+x_2+\ldots+x_n=0} \mu(f(x_1) + f(x_2) + \ldots + f(x_n)).$$

Note that $S_n = S_{n-1} - q^{n-2} + qN_{n-1}(1,1)$. We are ready to present a result obtained by Blokhuis and Calderbank [1] :

Proposition 2. *In the case of three valued spectrum,*

$$N_2(1,1) = A + B - \frac{AB}{q}.$$

In particular, $\frac{AB}{q}$ *is a positive integer, and*

$$\alpha + \beta = m + r_d, \quad r_d = \mathrm{val}_2(N_2(1,1));$$

where $N_2(1,1)$ *is also the number of solutions of* $(x+1)^d + x^d = 0$ *in* L.

Proof. By Fourier analysis

$$\begin{aligned}\frac{1}{q}\sum_a \widehat{f}(a)^n &= f_\mu^{[n]}(0)\\ &= \sum_{x_1+x_2+\ldots+x_n=0} \mu(f(x_1) + f(x_2) + \ldots + f(x_n))\\ &= S_n\\ &= S_{n-1} - q^{n-2} + qN_{n-1}(1,1).\end{aligned}$$

The proposition corresponds to the case $n = 3$, since $S_2 = q$:

$$x_A A^3 + x_B B^3 = A^2\frac{q^2 - Bq}{A-B} + B^2\frac{-q^2 + Aq}{A-B} = (A+B)q^2 - ABq\square$$

Lemma 4. *The valuations* α *and* β *are greater than* $\frac{m}{4}$.

Proof. If the valuations are equal then the minimal valuation is greater than $\frac{m}{2}$. If they are different

$$m + \beta - 2\alpha = \mathrm{val}_2(x_A) < m \Longrightarrow 2\alpha > \beta \geq \frac{m}{2} \Longrightarrow \alpha > \frac{m}{4}. \qquad \square$$

Following theirs ideas, we recover a nice result of Calderbank-McGuire-Poonen

Proposition 3. *If $m = 0 \pmod 4$, a power permutation with symmetric spectrum of valuation $\frac{m+2}{2}$ does not exist.*

Proof. Note that symmetry implies that A and B are powers of two. Of course, $\mathrm{val}\,(d) = \frac{m+2}{2}$ and Proposition (2) implies $N_2(1,1) = 4$. Considering $d \mod 15$ there are two cases. Recall that an exponent d is said to be equivalent to any exponent of the form $2^i d$ or $2^i d^{-1}$. So up to equivalence, $d \equiv 1 \mod 15$ or $d \equiv 7 \mod 15$. In the first case, the number of solutions of $(x+1)^d + x^d = 1$ is greater or equal to 2^4, contradicting $N_2(1,1) = 4$. In the second case, consider $j = -2^{\frac{2^m-1}{15}}$ then

$$\mathrm{wt}\,(dj) + \mathrm{wt}\,(-j) = 2 \times \frac{m}{4} = \frac{m}{2}$$

contradicting $\mathrm{val}\,(d) = \frac{m+2}{2}$. □

The following restriction is due to Calderbank-Blokhuis:

Lemma 5. *If m is a power of 2 and if an exponent has a three valued spectrum, then up to equivalence :*

$$d \equiv 1 \mod 15 \text{ and } \quad r_d \geq 4.$$

Proof. We start from the relation :

$$\widehat{f}(a)^4 - (A+B)\widehat{f}(a)^3 + AB\widehat{f}(a)^2 = 0\ .$$

Remember that $\alpha \geq 3$. Summing over a, dividing by q :

$$\begin{aligned} S_3 - q^2 + qN_3(1,1) - (A+B)qN_2(1,1) + ABq &= 0 \\ S_3 + qN_3(1,1) &= 0 \pmod{16q} \\ S_2 - q + qN_2(1,1) + qN_3(1,1) &= 0 \pmod{16q} \\ N_2(1,1) + N_3(1,1) &= 0 \pmod{16}. \end{aligned}$$

For $d \not\equiv 1 \pmod{15}$, using a computer we find that

$$N_2(1,1,256) + N_3(1,1,256) = 8 \pmod{16}$$

This congruence holds over the extension fields of $\mathrm{GF}(2,8)$, indeed the solutions of degree greater than 8 can be collected in disjoint subsets of cardinality 16. □

For further works, It may be interesting to notice that for all $c \in L^\times$, the mapping $f_c \colon x \mapsto \mu(cx)$ satisfy the integral relation :

$$f_c * f_c(x) - (A+B)f_c(x) + AB\delta_0(x) = \frac{AB}{q}\sum_{z \in Z} \mu(zc^t x) \tag{1}$$

where t denotes the inverse of d modulo $q-1$.

4 Checking Helleseth Conjecture in Dimension 32

Numerical experiments, computing Fourier spectra of all exponents, show that Helleseth conjecture is true in dimension 4, 8 and 16, see [5]. In this section, we describe the procedure that we used to verify its validity in the case where the dimension m is equal to 32.

Using Lemma 5 the candidate exponents to contradict Helleseth's conjecture must be congruent to 1 modulo 15. Up to equivalence, there are 17586223 such exponents. The computation of their Fourier spectra is still too expensive, we have to reduce the number of candidates.

Let us denote by K of the field of order $\sqrt{q}$, and let G the subgroup of order $\sqrt{q}+1$ in $L^\times$. For u and $v \in K$, we introduce the character sums :

$$S(u,v) = \sum_{x \in K^\times} \mu_K(ux^d + vx).$$

and also for $c \in K^\times$, the notation :

$$\widehat{f}_K(c) = \sum_{x \in K^\times} \mu_K(x^d + cx).$$

$$\begin{aligned}
\widehat{f}(a) &= 1 + \sum_{y \in G} \sum_{x \in K^\times} \mu_K(x^d \mathrm{Tr}_{L/K}(y^d) + x\mathrm{Tr}_{L/K}(ay)) \\
&= 1 + \sum_{y \in G} S(\mathrm{Tr}_{L/K}(y^d), \mathrm{Tr}_{L/K}(ay)) \\
&= \sqrt{q}\delta_K(a) + \sum_{1 \neq y \in G} \widehat{f}_K(\mathrm{Tr}_{L/K}(y^d)^{-t}\mathrm{Tr}_{L/K}(ay)) \\
&\quad \text{(where } t \text{ is the inverse of } d \text{ modulo } q-1) \\
&= \sqrt{q}\delta_K(a) + \sum_{b \in K} n_a(b)\widehat{f}_K(b)
\end{aligned}$$

where

$$n_a(b) = \sharp\{1 \neq y \in G \mid \mathrm{Tr}_{L/K}(ya)\mathrm{Tr}_{L/K}(y^d)^{-t} = b\},$$

Lemma 6. *One can compute the Fourier coefficients at* 1 *of all the power permutations in* $\mathrm{O}(q\sqrt{q})$ *steps.*

Proof. Using the above formula, one can compute the Fourier coefficients at 1 by generating the exponents as $d = d_K + (\sqrt{q}-1)d_G$ where $1 \leq d_K < \sqrt{q}$ and $0 \leq d_G \leq \sqrt{q}$. □

We computed the Fourier coefficients at 1 for all d with $\mathrm{wt}\,(d \mod 15) = 1$ up to equivalence. The CPU time of our program for this task was about 92520 seconds i.e. one day. The repartition of the valuations of these exponents are summarized in Table (1). We see there are only 549501 candidate exponents to contradict Helleseth's conjecture.

Table 1. The repartition of the valuation of 17586223 Fourier coefficients at one. In each square the valuation at one, and the number of exponents corresponding to this valuation : 127681 exponents have a Fourier coefficient equal to zero at one, 421821 have a Fourier coefficient at one of valuation greater or equal to 16. Only these 549702 exponent must be checked.

2	3	4	5	6	7	8
3184	49334	298984	228494	115057	60927	507643
9	10	11	12	13	14	15
428477	2591563	4808533	4221710	2127437	1064607	530771
16	17	18	19	20	32	∞
266562	137976	17234	40	8	1	127681

After this sieving step, for all candidate power permutations f, we computed the Fourier coefficients $\widehat{f}(a)$ for $a = 1, \beta, \beta^2, \ldots$ where β is an element of order $\sqrt{q}+1$, stopping the loop when 2 distincts non-zero Fourier coefficients A and B (with $\mathrm{val}_2(A) \leq \mathrm{val}_2(B)$) not satisfying the following conditions are discovered : $AB < 0$, $\frac{m}{4} < \mathrm{val}_2(A)$, $\frac{m}{2} \leq \mathrm{val}_2(B)$, $\sqrt{q} \leq \max\{|A|, |B|\}$.

The running time of this task was about 2 hours. According to the output of the program, a counter example to the Helleseth'conjecture does not exist in dimension 32.

Acknowledgement. Part of this work was done, while the first author was visiting IMATH, Université Du Sud Toulon Var and was partially supported by Université Du Sud Toulon Var. He acknowledge the hospitality. The first author was also partially supported by his previous affiliation: Institute of Applied Mathematics, Middle East Technical University.

References

1. Calderbank, A.R., Blokhuis, A.: (unpublished)
2. Calderbank, A.R., McGuire, G., Poonen, B., Rubinstein, M.: On a conjecture of Helleseth regarding pairs of binary m-sequences. IEEE Trans. Inform. Theory 42(3), 988–990 (1996)
3. Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discrete Math. 16(3), 209–232 (1976)
4. Katz, N., Livné, R.: Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. C. R. Acad. Sci. Paris Sér. I. Math. 309(11), 723–726 (1989)
5. Langevin, P.: Numerical projects page (2007), http://langevin.univ-tln.fr/project/spectrum
6. Langevin, P., Véron, P.: Non-linearity of power functions. Designs Codes and Cryptography 37(1) (2005)
7. McGuire, G.M., Calderbank, A.R.: Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences. IEEE Trans. Inform. Theory 41(4), 1153–1155 (1995)

Multiplicative Character Sums with Counter-Dependent Nonlinear Congruential Pseudorandom Number Generators

Domingo Gomez*

Faculty of Sciences,
University of Cantabria,
Avd. Los Castros, Santander, Spain
domingo.gomez@unican.es

Abstract. Nonlinear congruential pseudorandom number generators can have unexpectedly short periods. Shamir and Tsaban introduced the class of counter-dependent generators which admit much longer periods. In this paper we present a bound for multiplicative character sums for nonlinear sequences generated by counter-dependent generators.

1 Introduction

Let $q = p^r$, where p is a prime number. In this paper we study a multiplicative character sum related with the distribution properties of the powers and primitive elements of *counter-dependent nonlinear congruential pseudorandom number generators*. This class of generators was introduced by [1] and it is defined by a recurrence of the form

$$u_{n+1} = f(u_n, n), \quad u_n \in \mathbb{F}_q, \qquad n = 0, 1, \ldots, \tag{1}$$

with some *initial value* u_0, where $f(X, Y) \in \mathbb{F}_q[X, Y]$ is a polynomial over the field $\mathbb{F}_q$ of q elements of local degree in X at least 2. It is well-known that the problem of studying the distribution of primitive roots and powers can be reduced to bound a multiplicative character sum, see, for example [2].

It is obvious that the sequence (1) eventually becomes periodic with some period $t \le qp$. Throughout this paper we assume that this sequence is *purely periodic*, that is, $u_n = u_{n+t}$ beginning with $n = 0$, otherwise we consider a shift of the original sequence.

The case $f(X, Y) = h(X) \in \mathbb{F}_q[X]$, which does not depend on the second variable, is the well-studied *nonlinear congruential pseudorandom number generators*, see [3,4,5], the surveys [6,7] and references therein. A bound in the corresponding multiplicative character sum was given in [8]. On the other hand,

* This work was partially supported by the Spanish Government. Research Grant MTM 2004-07086. Also, I want to thank Arne Winterhof for his friendship and patience.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 188–195, 2010.

these generators have their own limits, for example the period t is at most q. So, it is interesting to study more general pseudorandom number generators.

The *counter-assisted nonlinear congruential pseudorandom number generators* were defined in [1]. They are defined by the following linear recurrence:

$$u_{n+1} = h(u_n) + n \bmod p \quad 0 \le u_n \le p-1, \qquad n = 0, 1, \ldots,$$

where $h(X) \in \mathbb{F}_p[X]$. For this specific class, the linear complexity and exponential sums were studied in [9]. These generators are related to *nonlinear congruential pseudorandom number generators of order* 2 defined by

$$u_{n+2} = f(u_{n+1}, u_n) \bmod p, \quad 0 \le u_n \le p-1, \qquad n = 0, 1, \ldots$$

Nonlinear congruential pseudorandom number generators of order $m \ge 2$ have been analyzed in [10,11] in particular cases and solve for the general case in [12]. The results in these papers treat the distribution of values, not distribution of powers. The linear complexity was studied in [13], so this shows that the problem is not trivial at all.

A general class of pseudorandom number generators of higher orders has been studied in [14,15]. This class has attracted a lot of attention, however to get a bound on the corresponding multiplicative character sum can only be done under certain conditions, see [16].

2 Definitions and Auxiliary Results

All the needed results are adapted, but the general properties of resultants and their proofs can be found in [17]. We use the classical abbreviation of $\deg_X$ to refer to the degree of a polynomial in the variable X.

The resultant is a classical concept that arises from commutative algebra. We suppose that we are working in $\mathbb{K}[X, Y]$, the ring of bivariate polynomials with coefficients in a field $\mathbb{K}$. Given two polynomials $f(X, Y), g(X, Y) \in \mathbb{K}[X, Y]$, where

$$f(X, Y) = \sum_{i=0}^{d_1} f_i(Y) X^i, \qquad g(X, Y) = \sum_{i=0}^{d_2} g_i(Y) X^i.$$

the *Sylvester matrix respect the variable* X is

$$\begin{pmatrix}
f_0(Y) & f_1(Y) & \ldots & f_{d_1}(Y) & 0 & \ldots & 0 & 0 \\
0 & f_0(Y) & f_1(Y) & \ldots & f_{d_1}(Y) & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & f_0(Y) & \ldots & f_{d_1-1}(Y) & f_{d_1}(Y) \\
g_0(Y) & g_1(Y) & \ldots & g_{d_2}(Y) & 0 & \ldots & 0 & 0 \\
0 & g_0(Y) & g_1(Y) & \ldots & g_{d_2}(Y) & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & g_0(Y) & \ldots & g_{d_2-1}(Y) & g_{d_2}(Y)
\end{pmatrix}.$$

This matrix is a $(d_1 + d_2) \times (d_1 + d_2)$ matrix, the first row is the coefficients of $f(X, Y)$ depending on Y, adding zeros to fill the $(d_1 + d_2)$ positions. Notice that

the next $d_2 - 1$ rows are shifts of the first row. The other rows are built using the polynomial $g(X, Y)$.

The determinant of this matrix is known as the resultant of the polynomials f and g respect of the variable X. We will denote it by $Res_X(f(X, Y), g(X, Y))$. The following Lemma shows the relation between resultant and common factors. It is a Corollary of [17, Proposition 1, Section 3.6].

Lemma 1. *Given* $f(X, Y), g(X, Y) \in \mathbb{F}_q[X, Y]$ *then*

$$\deg_X(\gcd(f(X, Y), g(X, Y))) \geq 1$$

if and only if

$$Res_X(f(X, Y), g(X, Y)) = 0.$$

In [18, Corollary 5.1], the author presented a relation between the composition of polynomials and resultants. His result is very general, so here is an adapted version for the proofs.

Lemma 2. *Let* $f(X, Y)$, $g(X, Y)$, $h(X, Y) \in \mathbb{K}[X, Y]$ *be polynomials such as* $\deg_X(f(X, Y)), \deg_X(g(X, Y)), \deg_X(h(X, Y)) \geq 1$ *then,*

$$Res_X(f(h(X, Y), Y), g(h(X, Y), Y)) = Res_X(f(X, Y), g(X, Y))^{\deg_X(h(X,Y))}.$$

The next Lemma is a weaker version of the Bezout Theorem.

Lemma 3. *Let* $f(X, Y), g(X, Y) \in \mathbb{K}[X, Y]$, *with* $\gcd(f(X, Y), g(X, Y)) = 1$ *then the number of common roots is at most the product of the degrees of the polynomials.*

For a polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$ of total degree d we define the sequence of polynomials $f_k(X, Y) \in \mathbb{F}_q[X, Y]$ by the recurrence relation

$$f_{k+1}(X, Y) = f_k\left(f(X, Y), Y + 1\right), \qquad k = 0, 1, \ldots, \tag{2}$$

where $f_0(X, Y) = X$. It is clear that $\deg(f_k(X, Y)) \leq d^k$ and for the sequence define in (1) that

$$u_{n+k} = f_k\left(u_n, n\right). \tag{3}$$

The following property will be necessary in the proof of the main theorem:

Lemma 4. *Given the sequence* $f_k(X, Y) \in \mathbb{F}_q[X, Y]$ *defined in* (2) *and if*

$$\deg_X(\gcd(f_k(X, Y), f_l(X, Y))) \geq 1$$

then

$$\deg_X(\gcd(f_{k-i}(X, Y), f_{l-i}(X, Y))) \geq 1, \quad \forall i \leq \min(k, l).$$

Proof. Now, we regard the polynomials $f_k(X, Y)$, $f_l(X, Y)$ as polynomials in the variable X whose coefficients are in the ring $\mathbb{F}_q[Y]$ and let

$$H(Y) = Res_X(f_{k-1}(X, Y), f_{l-1}(X, Y)).$$

Using simple properties of the Sylvester Matrix, we have:

$$Res_X(f_{k-1}(X, Y+1), f_{l-1}(X, Y+1)) = H(Y+1)$$

and, using Lemma 2, we get that:

$$Res_X(f_{k-1}(f(X,Y), Y+1), f_{l-1}(f(X,Y), Y+1) = H(Y+1)^{\deg_X(f(X,Y))}.$$

Applying the Lemma 1,

$$H(Y+1)^{\deg_X(f(X,Y))} = Res_X(f_k(X,Y), f_l(X,Y)) = 0.$$

This clearly implies that $H(Y) = 0$, therefore, again by Lemma 1 we get

$$\gcd(f_{k-1}(X,Y), f_{l-1}(X,Y)) = H_1(X,Y),\ \deg_X(H_1(X,Y)) \geq 1.$$

Applying the same argument i times, we get the result. □

Now, we are going to introduce some notation. Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$, with the standard convention $\chi(0) = 0$. We want to prove an upper bound on this character sum

$$S_\chi(N) = \sum_{n=0}^{N-1} \chi(u_n).$$

Next, we recall the classical Weil bound on multiplicative character sums (see [19, Chapter 5]) for univariate polynomials.

Lemma 5. *Let χ be a character of $\mathbb{F}_q$ of order s and let $F(X) \in \mathbb{F}_q[X]$ be a polynomial of positive degree that is not, up to a multiplicative constant, an sth power of a polynomial. Let d be a bound on the number of distinct roots in its splitting field over $\mathbb{F}_q$. Under these conditions, the following inequality*

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(F(x)\right) \right| \leq dq^{1/2}$$

holds.

With this Lemma we can prove another result that we will use through later.

Lemma 6. *Let χ be a character of $\mathbb{F}_q$ of order s and let $F(X,Y) \in \mathbb{F}_q[X,Y]$ be a polynomial of positive degree such that $F(X,Y)$ is not, up to a multiplicative constant, an sth power of a polynomial. Let $F(X,Y) = F_1(X,Y)^{d_1} \cdots F_h(X,Y)^{d_h}$ the decomposition of the polynomial in a product of irreducible polynomials. Let D be a bound on the total degree of $F_1(X,Y) \cdots F_h(X,Y)$. Under these conditions, the following inequality holds*

$$\left| \sum_{x,y \in \mathbb{F}_q} \chi\left(F(x,y)\right) \right| \leq 2Dq^{3/2}.$$

Proof. This Lemma is trivial when $2D \geq q^{1/2}$ so suppose that $2D \leq q^{1/2}$. Without loss of generality, d_1 is not an integer multiple of s, because $F(X,Y)$ is not an sth power of a polynomial up to a multiplicative constant. Next,

$$\left|\sum_{x,y\in\mathbb{F}_q} \chi\left(F_1(x,y)^{d_1}\dots F_h(x,y)^{d_h}\right)\right| \leq \sum_{y\in\mathbb{F}_q}\left|\sum_{x\in\mathbb{F}_q} \chi\left(F_1(x,y)^{d_1}\dots F_h(x,y)^{d_h}\right)\right|.$$

Our aim is to apply Lemma 5 to each of the sums for y fixed. We have to count how many times we can not apply Lemma 5. The special cases are:

- When the polynomial $F(X,y)$ is a constant polynomial.
- When the polynomial $F(X,y)$ is an sth power.

There are, at most, D different values y where the polynomial $F(X,y)$ could be a constant polynomial.

Now, we consider in which cases the polynomial $F(X,y)$ is an sth power of a polynomial and how these cases will be counted.

First of all, we remark that $F(X,Y)$ is not an sth power of a polynomial, so if $F(X,y)$ is an sth power of a polynomial then we have this two possible nonexclusive situations:

- $F_1(X,y)^{d_1}$ is an sth power, so because d_1 is not an s multiple then we must have that $F_1(X,b)$ has, at least, one multiple root. This is only possible if $F_1(X,b)$ and the first derivative of the polynomial have a common root. $F_1(X,Y)$ is an irreducible polynomial, so Lemma 3 applies. We remark that the first derivative is a nonzero polynomial. Otherwise $F_1(X,Y)$ is a power of a polynomial, thus reducible. This can only happen in $\deg_X(F_1)(\deg_X(F_1)-1)$ cases.
- $F_1(X,b)$ and $F_s(X,b)$ have a common root and, by the same argument, there are at most $\deg_X(F_1)\deg_X(F_s)$ possible values where it happens.

So, for each value of $y \in \mathbb{F}_q$, we apply Lemma 6 if the two previous cases do not occur. In the other cases, we apply the trivial bound,

$$\begin{aligned}\sum_{y\in\mathbb{F}_q}\left|\sum_{x\in\mathbb{F}_q}\chi\left(F(x,y)\right)\right| &\leq Dq + q\deg_X(F_1)\sum_{i=1}^{h}\deg_X(F_i) + Dq^{3/2}\\ &\leq (D^2+D)q + Dq^{3/2} \leq 2Dq^{3/2}.\end{aligned}$$

The last inequality holds because $2 \leq 2D \leq q^{1/2}$ and this remark finishes the proof. □

We call the sequence (v_n), given by (11) with $v_0 = 0$. Note that under the assumption that (u_n) is purely periodic, the sequence (v_n) need not be purely periodic. Let t_0 be the least period of the sequence (v_n) if it is purely periodic and put $t_0 = \infty$ otherwise. We are ready to prove the principal theorem:

Theorem 7. *Let the sequence (u_n), given by (1) with a polynomial $f(X,Y)$ with coefficients in $\mathbb{F}_q[X,Y]$ and total degree $d \geq 2$ be purely periodic with period t and $t \geq N \geq 1$. If $f_k(X,Y), 1 \leq k \leq \lceil 0.4(\log q)/\log d \rceil$ is not, up to a multiplicative constant, an sth power of a polynomial, then the bound*

$$S_\chi(N) = O\left(N^{1/2} q \left(\min\left(\frac{\log q}{\log d}, t_0\right)\right)^{-1/2}\right)$$

holds, where the implied constant is absolute.

Proof. We can suppose that $q \geq 3$. For any integer $k \geq 0$ we have

$$\left|S_\chi(N) - \sum_{n=0}^{N-1} \chi(u_{n+k})\right| \leq 2k,$$

so for any $K \geq 1$ and summing over $k = 0, 1 \ldots, K-1$, we get

$$K|S_\chi(N)| \leq W + \left|\sum_{k=0}^{K-1}\left(S_\chi(N) - \sum_{n=0}^{N-1}\chi(u_{n+k})\right)\right| \leq W + K^2$$

where

$$W = \sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\chi(u_{n+k})\right|.$$

By the Cauchy-Schwarz inequality and (3) we obtain

$$W^2 \leq N\sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\chi(u_{n+k})\right|^2 = N\sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\chi(f_k(u_n,n))\right|^2$$

$$\leq N\sum_{x,y\in\mathbb{F}_q}\left|\sum_{k=0}^{K-1}\chi(f_k(u_n,n))\right|^2 \leq N\sum_{k,l=0}^{K-1}\left|\sum_{x,y\in\mathbb{F}_q}\chi(f_k(x,y))\overline{\chi}(f_l(x,y))\right|$$

where $\overline{\chi}(f_l(x,y))$ denotes the conjugate of $\chi(f_l(x,y))$.

Because χ is a multiplicative character it is trivial to see that $\chi(a^{q-2}) = \overline{\chi}(a),\ \forall a \in \mathbb{F}_q$.

Substituting the conjugates, we get the following inequality:

$$W^2 \leq N\sum_{k,l=0}^{K-1}\left|\sum_{x,y\in\mathbb{F}_q}\chi(f_k(x,y)f_l(x,y)^{q-2})\right|.$$

Next we have to show that for $0 \leq l \leq k \leq K-1$ the polynomial $F(X,Y) = f_k(X,Y)f_l(X,Y)^{q-2},\ k \geq l$ is, up to a multiplicative constant, an sth power of a polynomial only if $k = l \mod t_0$, where $k = l \mod \infty$ means $k = l$.

Suppose $g(X,Y) = \gcd(f_k(X,Y), f_l(X,Y))$ has degree at least 1 in X. By Lemma 4, $\gcd(f_0(X,Y) = X, f_{k-l}(X,Y))$ is a non constant polynomial in X.

Because X is a prime polynomial, we have that the greatest common divisor between $f_0(X,Y)$ and $f_{k-l}(X,Y)$ is X so $v_{k-l} = 0$ and, consequently, $k - l = 0 \mod t_0$.

Now suppose $k \neq l \mod t_0$ and thus $g(X,Y) = 1$. Hence, if $F(X,Y)$ is (up to a multiplicative constant) an sth power, then both $f_k(X,Y)$ and $f_l(X,Y)$ are (up to multiplicative constants) sth powers, which is a contradiction to our assumption provided that K is small enough (this will be guaranteed by the subsequent choice of K). Now the number of pairs $(k,l) \in \mathbb{Z}^2$ with $0 \leq l < k \leq K-1$ and $k = l \mod t_0$ is at most $K^2/(2t_0)$. For these pairs (k,l) we estimate the inner sum in the last bound on W^2 trivially by q. For all other pairs we can use Lemma 6 and get

$$W^2 < KNq^2 + K^2N\left(\frac{q^2}{t_0} + 2d^{K-1}q^{3/2}\right).$$

With

$$K := \left\lceil 0.4\frac{\log q}{\log d}\right\rceil$$

we get the result and this finishes the proof. □

References

1. Shamir, A., Tsaban, B.: Guaranteeing the diversity of number generators. Inform. and Comput. 171(2), 350–363 (2001)
2. Niederreiter, H., Shparlinski, I.E.: On the distribution of power residues and primitive elements in some nonlinear recurring sequences. Bull. London Math. Soc. 35(4), 522–528 (2003)
3. Gutierrez, J., Shparlinski, I.E., Winterhof, A.: On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators. IEEE Trans. Inform. Theory 49(1), 60–64 (2003)
4. Niederreiter, H., Shparlinski, I.E.: On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. Finite Fields Appl. 5(3), 246–253 (1999)
5. Niederreiter, H., Winterhof, A.: Exponential sums for nonlinear recurring sequences. Finite Fields Appl. 14(1), 59–64 (2008)
6. Topuzoğlu, A., Winterhof, A.: Pseudorandom sequences. In: Topics in Geometry, Coding Theory and Cryptography. Algebr. Appl., vol. 6, pp. 135–166. Springer, Dordrecht (2007)
7. Winterhof, A.: Recent results on recursive nonlinear pseudorandom number generators. In: Sequences and their Applications SETA 2010. LNCS. Springer, Heidelberg (2010)
8. Niederreiter, H., Winterhof, A.: Multiplicative character sums for nonlinear recurring sequences. Acta Arith. 111(3), 299–305 (2004)
9. El-Mahassni, E., Winterhof, A.: On the distribution and linear complexity of counter-dependent nonlinear congruential pseudorandom number generators. Journal of Algebra, Number Theory and Applications 2, 1–6 (2006)

10. Griffin, F., Niederreiter, H., Shparlinski, I.E.: On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders. In: Fossorier, M.P.C., Imai, H., Lin, S., Poli, A. (eds.) AAECC 1999. LNCS, vol. 1719, pp. 87–93. Springer, Heidelberg (1999)
11. Gutierrez, J., Gomez-Perez, D.: Iterations of multivariate polynomials and discrepancy of pseudorandom numbers. In: Bozta, S., Sphparlinski, I. (eds.) AAECC 2001. LNCS, vol. 2227, pp. 192–199. Springer, Heidelberg (2001)
12. Ostafe, A., Pelican, E., Shparlinski, I.E.: On pseudorandom numbers from multivariate polynomial systems. Finite Fields and their Applications (to appear 2010)
13. Topuzoğlu, A., Winterhof, A.: On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders. Appl. Algebra Engrg. Comm. Comput. 16(4), 219–228 (2005)
14. Ostafe, A.: Multivariate permutation polynomial systems and nonlinear pseudorandom number generators. Finite Fields and Their Applications 16(3), 144–154 (2010)
15. Ostafe, A., Shparlinski, I.E.: On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators. Math. Comp. 79(269), 501–511 (2010)
16. Ostafe, A., Shparlinski, I.E., Winterhof, A.: Multiplicative character sums of a class of nonlinear recurrence vector sequences (2010) (Preprint)
17. Cox, D., Little, J., O'Shea, D.: Ideals, varieties, and algorithms, 3rd edn. Undergraduate Texts in Mathematics. Springer, New York (2007); An introduction to computational algebraic geometry and commutative algebra
18. Hong, H.: Subresultants under composition. J. Symbolic Comput. 23(4), 355–365 (1997)
19. Lidl, R., Niederreiter, H.: Finite fields. In: Encyclopedia of Mathematics and its Applications, 2nd edn., vol. 20. Cambridge University Press, Cambridge (1997), With a foreword by P. M. Cohn

Ternary Kloosterman Sums Modulo 18 Using Stickelberger's Theorem

Faruk Göloğlu*, Gary McGuire**, and Richard Moloney***

School of Mathematical Sciences
University College Dublin
Ireland

Abstract. A result due to Helleseth and Zinoviev characterises binary Kloosterman sums modulo 8. We give a similar result for ternary Kloosterman sums modulo 9. This leads to a complete characterisation of values that ternary Kloosterman sums assume modulo 18. The proof uses Stickelberger's theorem and Fourier analysis.

Keywords: Kloosterman sums, Stickelberger's theorem.

1 Introduction

Let $\mathcal{K}_{p^n}(a)$ denote the p-ary Kloosterman sum defined by

$$\mathcal{K}_{p^n}(a) := \sum_{x \in \mathbb{F}_{p^n}} \zeta^{\mathrm{Tr}(x^{p^n-2}+ax)},$$

for any $a \in \mathbb{F}_{p^n}$, where ζ is a primitive p-th root of unity and the trace map $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ defined as usual as

$$\mathrm{Tr}(c) := c + c^p + c^{p^2} + \cdots + c^{p^{n-1}},$$

for any $c \in \mathbb{F}_{p^n}$. Kloosterman sums have attracted attention thanks to their various links to other related fields. For instance, a zero of a binary Kloosterman sum on $\mathbb{F}_{2^n}$ leads to a bent function from $\mathbb{F}_{2^{2n}} \to \mathbb{F}_2$ as proven by Dillon in [2]. Similarly, zeros of ternary Kloosterman sums give rise to ternary bent functions [6]. However determining a zero of a Kloosterman sum is not easy. A recent result in this direction is the following: a binary or ternary Kloosterman sum $\mathcal{K}_{p^n}(a)$ is not zero if a is in a proper subfield of $\mathbb{F}_{p^n}$ except when $p = 2, n = 4, a = 1$,

* Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

** Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

*** Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006, and the Irish Research Council for Science, Engineering and Technology.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 196–203, 2010.

see [14]. Given the difficulty of the problem of finding zeros (or explicit values) of Kloosterman sums, and that they sometimes do not exist, one is generally satisfied with divisibility results.

It is easy to see that binary Kloosterman sums are divisible by 4. They also satisfy (see [10])

$$-2^{n/2+1} \leq \mathcal{K}_{2^n}(a) \leq 2^{n/2+1},$$

and take every value which is divisible by 4 in that range.

The ternary version of this result is due to Katz and Livné [8]. It is easy to see that ternary Kloosterman sums are divisible by 3. Ternary Kloosterman sums satisfy (see [8])

$$-2\sqrt{3^n} < \mathcal{K}_{3^n}(a) < 2\sqrt{3^n}$$

and take every value which is divisible by 3 in that range.

Given the above results for binary Kloosterman sums modulo 4, and for ternary Kloosterman sums modulo 3, one next considers binary sums modulo 8 and ternary sums modulo 9. The following is known in the binary case.

Theorem 1. *[7] Let $n > 2$. For $a \in \mathbb{F}_{2^n}$,*

$$\mathcal{K}_{2^n}(a) \equiv \begin{cases} 0 \pmod 8 \text{ if } \mathrm{Tr}(a) = 0, \\ 4 \pmod 8 \text{ if } \mathrm{Tr}(a) = 1. \end{cases}$$

The result in this paper is the following theorem, concerning ternary sums modulo 9.

Theorem 2. *Let $n > 1$. For $a \in \mathbb{F}_{3^n}$,*

$$\mathcal{K}_{3^n}(a) \equiv \begin{cases} 0 \pmod 9 \text{ if } \mathrm{Tr}(a) = 0, \\ 3 \pmod 9 \text{ if } \mathrm{Tr}(a) = 1, \\ 6 \pmod 9 \text{ if } \mathrm{Tr}(a) = 2. \end{cases}$$

When $p = 3$, it is not hard to show that $\mathcal{K}_{p^n}(a)$ is always an integer. This is not (necessarily) the case for $p > 3$. Also note that Lisoněk previously proved that $9|\mathcal{K}_{3^n}(a)$ if and only if $\mathrm{Tr}(a) = 0$ (see [13]), using curves and division polynomials.

The following result on ternary Kloosterman sums modulo 2 was given in [14]. We will combine this result with our Theorem 2 to give the complete characterisation of ternary Kloosterman sums modulo 18.

Theorem 3. *[3] Let $\sqrt{a}$ denote any $b \in \mathbb{F}_{3^n}$ such that $b^2 = a$.*

$$\mathcal{K}_{3^n}(a) \equiv \begin{cases} 0 \pmod 2 \text{ if } a = 0 \text{ or } a \text{ is a square and } \mathrm{Tr}(\sqrt{a}) \neq 0, \\ 1 \pmod 2 \text{ otherwise.} \end{cases}$$

A partial result modulo 4 was also given in [3]. This can be combined with our result to give a partial result modulo 36.

The tools we use are Stickelberger's theorem which we explain in the next section, and some Fourier analysis which we explain in Section 3. In Section 4

we give the proof of Theorem 2. Corollary 1 of Section 4 gives the characterisation of ternary Kloosterman sums modulo 18 using the above mentioned results. Note that for the binary case there are many results concerning Kloosterman sums modulo $3, 8, 24$ (see [4,1,15]).

Remarks Added For Revised Version. We thank the referees for helpful comments. Since this paper was submitted we have extended the modulo 9 theorem in this article, Theorem 2, to a modulo 27 theorem. However, the techniques are not a simple advance of the methods in this paper; we use the Gross-Koblitz formula. Also, just before submitting this revised version to the proceedings we found an article by van der Geer-van der Vlugt [17] which uses Stickelberger's theorem and contains some of the results of this article (but not the modulo 27 results).

2 Stickelberger's Theorem

Let p be a prime (in Section 4 we set $p = 3$) and let $q = p^n$. We consider multiplicative characters taking their values in an algebraic extension of the p-adic numbers $\mathbb{Q}_p$. Let ξ be a primitive $(q-1)^{\text{th}}$ root of unity in a fixed algebraic closure of $\mathbb{Q}_p$. The group of multiplicative characters of $\mathbb{F}_q$ (denoted $\widehat{\mathbb{F}_q^\times}$) is cyclic of order $q-1$. The group $\widehat{\mathbb{F}_q^\times}$ is generated by the Teichmüller character $\omega : \mathbb{F}_q^\times \to \mathbb{Q}_p(\xi)$, which, for a fixed generator t of $\mathbb{F}_q^\times$, is defined by

$$\omega(t^j) = \xi^j.$$

We extend ω to $\mathbb{F}_q$ by setting $\omega(0)$ to be 0.

Let ζ be a primitive p-th root of unity in the fixed algebraic closure of $\mathbb{Q}_p$. Let μ be the canonical additive character of $\mathbb{F}_q$,

$$\mu(x) = \zeta^{\mathrm{Tr}(x)}$$

where Tr denotes the absolute trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$.

The Gauss sum (see [12,19]) of a character $\chi \in \widehat{\mathbb{F}_q^\times}$ is defined as

$$\tau(\chi) = -\sum_{x \in \mathbb{F}_q} \chi(x)\mu(x)\,.$$

We define

$$g(j) := \tau(\omega^{-j})\,.$$

For any positive integer j, let $\mathrm{wt}_p(j)$ denote the p-weight of j, i.e.,

$$\mathrm{wt}_p(j) = \sum_i j_i$$

where $\sum_i j_i p^i$ is the p-ary expansion of j.

Let π be the unique $(p-1)$th root of $-p$ in $\mathbb{Q}_p(\xi,\zeta)$ satisfying

$$\pi \equiv \zeta - 1 \pmod{\pi^2}.$$

Wan [18] noted that the following improved version of Stickelberger's theorem is a direct consequence of the Gross-Koblitz formula [5,16].

Theorem 4. *[18] Let $1 \le j < q-1$ and let $j = j_0 + j_1 p + \cdots + j_{n-1}p^{n-1}$. Then*

$$g(j) \equiv \frac{\pi^{\mathrm{wt}_p(j)}}{j_0! \cdots j_{n-1}!} \pmod{\pi^{\mathrm{wt}_p(j)+p-1}}.$$

Stickelberger's theorem, as usually stated, is the same congruence modulo $\pi^{\mathrm{wt}_p(j)+1}$.

We have (see [5]) that (π) is the unique prime ideal of $\mathbb{Q}_p(\zeta,\xi)$ lying above p. Since $\mathbb{Q}_p(\zeta,\xi)$ is an unramified extension of $\mathbb{Q}_p(\zeta)$, a totally ramified (degree $p-1$) extension of $\mathbb{Q}_p$, it follows that $(\pi)^{p-1} = (p)$ and $\nu_p(\pi) = \frac{1}{p-1}$. Here ν_p denotes the p-adic valuation.

Therefore Theorem 4 implies that $\nu_\pi(g(j)) = \mathrm{wt}_p(j)$, and because $\nu_p(g(j)) = \nu_\pi(g(j)) \cdot \nu_p(\pi)$ we get

$$\nu_p(g(j)) = \frac{\mathrm{wt}_p(j)}{p-1}. \tag{1}$$

In this paper we have $p = 3$. In that case, $\pi = -2\zeta - 1$ and equation (1) becomes

$$\nu_3(g(j)) = \frac{\mathrm{wt}_3(j)}{2}. \tag{2}$$

3 Fourier Coefficients

The Fourier transform of a function $f : \mathbb{F}_q \to \mathbb{C}$ at $a \in \mathbb{F}_q$ is defined to be

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_q} f(x)\mu(ax).$$

The complex number $\widehat{f}(a)$ is called the Fourier coefficient of f at a.

Consider monomial functions defined by $f(x) = \mu(x^d)$. When $d = -1$ we have $\widehat{f}(a) = \mathcal{K}_{p^n}(a)$. By a similar Fourier analysis argument to that in Katz [9] or Langevin-Leander [11], for any d we have

$$\widehat{f}(a) = \frac{q}{q-1} + \frac{1}{q-1} \sum_{j=1}^{q-2} \tau(\bar{\omega}^j)\ \tau(\omega^{jd})\ \bar{\omega}^{jd}(a)$$

and hence

$$\widehat{f}(a) \equiv -\sum_{j=1}^{q-2} \tau(\bar{\omega}^j)\ \tau(\omega^{jd})\ \bar{\omega}^{jd}(a) \pmod{q}.$$

We will use this to obtain congruence information about Kloosterman sums. Putting $d = -1 = p^n - 2$, the previous congruence becomes

$$\mathcal{K}(a) \equiv -\sum_{j=1}^{q-2} (g(j))^2 \ \omega^j(a) \pmod{q}. \tag{3}$$

In this paper, $p = 3$. Equation (2) gives the 3-adic valuation of the Gauss sums $g(j)$, and the 3-adic valuation of each term in equation (3) follows. Our proofs will consider (3) at various levels, i.e., modulo 3^2 and 3^3.

4 Ternary Kloosterman Sums Modulo 9

In this section we will prove our result using Stickelberger's theorem. First we need a lemma which helps us in our proof.

Lemma 1. *Let p be a prime, $q = p^n$ and $r \in \mathbb{F}_p^\times$. If T_r denotes the set $\{a \in \mathbb{F}_q \mid \mathrm{Tr}(a) = r\}$, then*

$$\sum_{t \in T_r} t^{-1} = r^{-1}.$$

Proof. Consider the polynomials

$$g(x) = \prod_{t \in T_r} (x - t),$$

$$h(x) = \prod_{t \in T_r} (x - t^{-1}).$$

Note that $g(x)$ vanishes on the p^{n-1} elements of T_r. Thus

$$g(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x - r.$$

In particular,

$$\prod_{t \in T_r} (-t) = -r,$$

so

$$\prod_{t \in T_r} (-t^{-1}) = -r^{-1}.$$

The reciprocal polynomial of g is $g^*(x) = x^{p^{n-1}} g(1/x)$.

We therefore get

$$\begin{aligned} h(x) &= -r^{-1} g^*(x) \\ &= -r^{-1} x^{p^{n-1}} g(1/x) \\ &= x^{p^{n-1}} - r^{-1} x^{p^{n-1}-1} - \cdots - r^{-1} x^{p^{n-1}-p^{n-2}} - r^{-1}. \end{aligned}$$

Thus

$$\sum_{t \in T_r} (-t^{-1}) = -r^{-1}.$$

□

From now on, we set $p = 3$, so that $\mathcal{K}_q(a)$ is an integer for $a \in \mathbb{F}_q$. Since there will not be any confusion with binary Kloosterman sums we will write $\mathcal{K}(a)$ for $\mathcal{K}_q(a)$. We consider the function $f(x) = \mu(x^{-1}) = \mu(x^{q-2})$. Then $\widehat{f}(a)$ is the Kloosterman sum $\mathcal{K}(a)$. The following lemma will be needed.

Lemma 2. *Let $q = 3^n$, and T_1 be as defined above. Then*

$$\sum_{z \in T_1} \bar{\omega}(z) \equiv 1 \pmod 3.$$

Proof. Follows directly from Lemma 1 and the definition of the Teichmüller character. □

We can now prove our main result.

Proof (of Theorem 2). By equation (3)

$$\mathcal{K}(a) \equiv -\sum_{j=1}^{q-2} g(j)^2\, \omega^j(a) \pmod q. \tag{4}$$

Let, for any $0 < t < q-1$, the 3-adic expansion of t be $t = t_0 + 3t_1 + \cdots + 3^{n-1}t_{n-1}$ and let $\mathcal{P}$ be the prime of $\mathbb{Q}_3(\xi, \zeta)$ lying above 3. As we mentioned in Section 2, Stickelberger's theorem implies that

$$\begin{aligned} \nu_{\mathcal{P}}(g(t)) &= \mathrm{wt}_3(t) = t_0 + t_1 + \cdots + t_{n-1} \\ \nu_3(g(t)) &= \frac{\mathrm{wt}_3(t)}{2}, \\ \text{and so } \nu_3((g(t))^2) &= \mathrm{wt}_3(t). \end{aligned} \tag{5}$$

Now (5) implies that any term in the sum in (4) with $\mathrm{wt}_3(j) > 1$ will be 0 modulo 9, so (4) modulo 9 becomes a sum over terms of weight 1 only:

$$\mathcal{K}(a) \equiv -\sum_{0 \le i < n} g(3^i)^2\, \omega^{3^i}(a) \pmod 9.$$

By Lemma 6.5 of [19], $g(3^i) = g(1)$, so we obtain

$$\mathcal{K}(a) \equiv -g(1)^2 \sum_{0 \le i < n} \omega^{3^i}(a) \pmod 9. \tag{6}$$

By definition of ω, we have

$$\sum_{0 \le i < n} \omega^{3^i}(a) \equiv \mathrm{Tr}(a) \pmod 3. \tag{7}$$

Since $\nu_3(g(1)^2) = \mathrm{wt}_3(1) = 1$, the proof of the theorem reduces to determining $g(1)^2 \mod 9$. We calculate, using the notation of Lemma 1,

$$\begin{aligned} g(1) &= -\sum_{x\in\mathbb{F}_q^\times} \bar{\omega}(x)\zeta^{\mathrm{Tr}(x)} \\ &= -\sum_{x\in T_0} \bar{\omega}(x) - \sum_{x\in T_1} \bar{\omega}(x)\zeta - \sum_{x\in T_1} \bar{\omega}(-x)\zeta^2 \\ &= (\zeta^2-\zeta)\sum_{x\in T_1} \bar{\omega}(x) \end{aligned}$$

because $\bar{\omega}(-x) = -\bar{\omega}(x)$, $T_2 = -T_1$, and the sum over T_0 is 0. This implies

$$g(1)^2 = (\zeta^2-\zeta)^2 \left(\sum_{x\in T_1} \bar{\omega}(x)\right)^2.$$

But we have $(\zeta^2-\zeta)^2 = -3$. This, together with Lemma 2, implies

$$g(1)^2 \equiv 6 \pmod 9.$$

Combining this with (7), the congruence (6) becomes

$$\mathcal{K}(a) \equiv 3\ \mathrm{Tr}(a) \pmod 9$$

as required. □

Theorem 2 and Theorem 3 together give a full characterisation of ternary Kloosterman sums modulo 18, which we summarise in the following corollary.

Corollary 1. *Let $q = 3^n$. For $a \in \mathbb{F}_q^\times$,*

$$\mathcal{K}_q(a) \equiv \begin{cases} 0 \pmod{18} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } a \text{ square with } \mathrm{Tr}(\sqrt{a}) \neq 0, \\ 3 \pmod{18} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } a \text{ non-square or } \mathrm{Tr}(\sqrt{a}) = 0, \\ 6 \pmod{18} & \text{if } \mathrm{Tr}(a) = 2 \text{ and } a \text{ square with } \mathrm{Tr}(\sqrt{a}) \neq 0, \\ 9 \pmod{18} & \text{if } \mathrm{Tr}(a) = 0 \text{ and } a \text{ non-square or } \mathrm{Tr}(\sqrt{a}) = 0, \\ 12 \pmod{18} & \text{if } \mathrm{Tr}(a) = 1 \text{ and } a \text{ square with } \mathrm{Tr}(\sqrt{a}) \neq 0, \\ 15 \pmod{18} & \text{if } \mathrm{Tr}(a) = 2 \text{ and } a \text{ non-square or } \mathrm{Tr}(\sqrt{a}) = 0. \end{cases}$$

References

1. Charpin, P., Helleseth, T., Zinoviev, V.: The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd. Journal of Combinatorial Theory 114, 332–338 (2007)
2. Dillon, J.F.: Elementary Hadamard Difference Sets. PhD thesis, University of Maryland (1974)
3. Garaschuk, K., Lisoněk, P.: On ternary Kloosterman sums modulo 12. Finite Fields Appl. 14(4), 1083–1090 (2008)
4. Garaschuk, K., Lisoněk, P.: On binary Kloosterman sums divisible by 3. Designs, Codes and Cryptography 49, 347–357 (2008)
5. Gross, B.H., Koblitz, N.: Gauss sums and the p-adic Γ-function. Ann. of Math. (2) 109(3), 569–581 (1979)

6. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory 52(5), 2018–2032 (2006)
7. Helleseth, T., Zinoviev, V.: On $\mathbb{Z}_4$-linear Goethals codes and Kloosterman sums. Designs, Codes and Cryptography 17, 269–288 (1999)
8. Katz, N., Livné, R.: Sommes de Kloosterman et courbes elliptiques universelles caractéristiques 2 et 3. C. R. Acad. Sci. Paris Sér. I. Math. 309(11), 723–726 (1989)
9. Katz, N.M.: Gauss sums, Kloosterman sums, and monodromy groups. Annals of Mathematics Studies, vol. 116. Princeton University Press, Princeton (1988)
10. Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inform. Theory 36(3), 686–692 (1990)
11. Langevin, P., Leander, G.: Monomial bent functions and Stickelberger's theorem. Finite Fields and Their Applications 14, 727–742 (2008)
12. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1986)
13. Lisoněk, P.: On the connection between Kloosterman sums and elliptic curves. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 182–187. Springer, Heidelberg (2008)
14. Lisoněk, P., Moisio, M.: On zeros of Kloosterman sums (to appear 2009)
15. Moisio, M.: The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even. Finite Fields and Their Applications 15, 174–184 (2009)
16. Robert, A.: The Gross-Koblitz formula revisited. Rendiconti del Seminario Matematico della Università di Padova 105, 157–170 (2001)
17. van der Geer, G., van der Vlugt, M.: Kloosterman sums and the p-torsion of certain Jacobians. Math. Ann. 290(3), 549–563 (1991)
18. Wan, D.Q.: Minimal polynomials and distinctness of Kloosterman sums. Finite Fields Appl. 1(2), 189–203 (1995); Special issue dedicated to Leonard Carlitz
19. Washington, L.C.: Introduction to Cyclotomic Fields. Springer, Heidelberg (1982)

Appended m-Sequences with Merit Factor Greater than 3.34

Jonathan Jedwab and Kai-Uwe Schmidt

Department of Mathematics, Simon Fraser University
Burnaby, BC V5A 1S6, Canada
{jed,kuschmidt}@sfu.ca

Abstract. We consider the merit factor of binary sequences obtained by appending an initial fraction of an m-sequence to itself. We show that, for all sufficiently large n, there is some rotation of each m-sequence of length n that has merit factor greater than 3.34 under suitable appending. This is the first proof that the asymptotic merit factor of a binary sequence family can be increased under appending. We also conjecture, based on numerical evidence, that *each* rotation of an m-sequence has asymptotic merit factor greater than 3.34 under suitable appending. Our results indicate that the effect of appending on the merit factor is strikingly similar for m-sequences as for rotated Legendre sequences.

1 Introduction

A *binary sequence* A of length n is an n-tuple $(a_0, a_1, \ldots, a_{n-1})$, where each a_j takes the value -1 or 1. The *aperiodic autocorrelation* of the binary sequence A at shift u is defined to be

$$C_A(u) := \sum_{j=0}^{n-u-1} a_j a_{j+u} \quad \text{for } u = 0, 1, \ldots, n-1,$$

and, provided that $n \geq 2$, its *merit factor* is

$$F(A) := \frac{n^2}{2\sum_{u=1}^{n-1} [C_A(u)]^2}.$$

The merit factor is important both practically and theoretically. For example, the larger the merit factor of a binary sequence that is used to transmit information by modulating a carrier signal, the more uniformly the signal energy is distributed over the frequency range; this is particularly important in spread-spectrum communication [1]. The merit factor of binary sequences is also studied

J. Jedwab is supported by NSERC of Canada.
K.-U. Schmidt is supported by Deutsche Forschungsgemeinschaft (German Research Foundation) under Research Fellowship SCHM 2609/1-1.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 204–216, 2010.

in complex analysis, in statistical mechanics, and in theoretical physics and theoretical chemistry (see [6] for a survey of the merit factor problem, and [7] for a survey of related problems). The general objective is to understand the behaviour, as $n \longrightarrow \infty$, of the optimal merit factor $F(A)$ as A ranges over the set of all 2^n binary sequences of length n.

The only non-trivial infinite families of binary sequences for which the asymptotic merit factor is known are: Legendre sequences, m-sequences, Rudin-Shapiro sequences, and some generalisations of these three families. The largest proven asymptotic merit factor of a binary sequence family is 6, which is attained by rotated Legendre sequences (see Theorem 13).

There is considerable numerical evidence that an asymptotic merit factor greater than 6 can be achieved [9,10,2]. The idea of [2], based on earlier work [9], is to start with a near-optimal rotation of a Legendre sequence (which has asymptotic merit factor close to 6) and append an initial fraction of the sequence to itself. Based on partial explanations and extensive numerical computations, [2] exhibits a binary sequence family that apparently has asymptotic merit factor greater than 6.34, although a proof for this has not yet been found.

In this paper we apply the idea of sequence appending to m-sequences and prove, for the first time, that the asymptotic merit factor of a binary sequence family can be increased under appending. The asymptotic merit factor of all m-sequences is known to equal 3 (see Theorem 3). We show that, for all sufficiently large n, there is some rotation of an m-sequence of length n that has merit factor greater than 3.34 under suitable appending. Our analysis makes critical use of the "shift-and-add" property of m-sequences (see Lemma 1 (ii)). We also conjecture, based on numerical evidence, that *each* rotation of an m-sequence has asymptotic merit factor greater than 3.34 under suitable appending. Our results reveal that the effect of appending is strikingly similar for m-sequences as for rotated Legendre sequences; this is discussed in the final section of the paper.

2 Notation

In this section we introduce further definitions and notation for the paper.

Given a binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, we denote by $[A]_j$ the sequence element a_j. Let $A = (a_0, a_1, \ldots, a_{n-1})$ and $B = (b_0, b_1, \ldots, b_{m-1})$ be binary sequences of length n and m, respectively. The *concatenation* $A; B$ of A and B is the length $n + m$ binary sequence given by

$$[A; B]_j := \begin{cases} a_j & \text{for } 0 \le j < n \\ b_{j-n} & \text{for } n \le j < n + m. \end{cases}$$

Let r and t be real numbers, where $t \in [0, 1]$. Following [2], the *rotation* A_r of A by a fraction r of its length is the binary sequence of length n given by

$$[A_r]_j := a_{(j+\lfloor rn \rfloor) \bmod n} \quad \text{for } 0 \le j < n,$$

and the *truncation* A^t of A by a fraction t of its length is the binary sequence of length $\lfloor tn \rfloor$ given by

$$[A^t]_j := a_j \quad \text{for } 0 \le j < \lfloor tn \rfloor.$$

We also use the standard definition of the *periodic autocorrelation* of the binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ at an integer shift u, namely

$$R_A(u) := \sum_{j=0}^{n-1} a_j a_{(j+u) \bmod n}. \tag{1}$$

3 Properties of *m*-Sequences

This section provides background and some required results on m-sequences.

Let $\mathrm{GF}(2^m)$ be the finite field containing 2^m elements, and let $\mathrm{Tr} : \mathrm{GF}(2^m) \to \mathrm{GF}(2)$ be the absolute trace function on $\mathrm{GF}(2^m)$ given by

$$\mathrm{Tr}(z) := \sum_{j=0}^{m-1} z^{2^j}.$$

An *m-sequence* $Y = (y_0, y_1, \ldots, y_{n-1})$ of length $n = 2^m - 1$ (for $m \ge 2$) is defined by

$$y_j := (-1)^{\mathrm{Tr}(\beta \alpha^j)} \quad \text{for } 0 \le j < n \tag{2}$$

for some primitive element α of $\mathrm{GF}(2^m)$ and some nonzero element β of $\mathrm{GF}(2^m)$. By writing β as a power of α, it is seen that different choices for β correspond to different rotations of the sequence defined by a particular β. This implies that each rotation of an m-sequence is an m-sequence, as noted in Lemma 1 (i) below. For each $n = 2^m - 1$, there are exactly $n\phi(n)/m$ distinct m-sequences [4, Cor. 4.7], where ϕ is Euler's totient function (there are n choices for β, and $\phi(n)/m$ choices for α that arise by taking one representative of each conjugacy class of the $\phi(n)$ primitive elements of $\mathrm{GF}(2^m)$).

We shall require the following properties of m-sequences (see [4] for a detailed modern treatment; these properties were originally derived using an alternative definition of m-sequences involving a linear recurrence relation [3]).

Lemma 1. *Let $Y = (y_0, y_1, \ldots, y_{n-1})$ be an m-sequence of length $n = 2^m - 1$, as in (2).*

(i) *The rotated sequence Y_r is an m-sequence for every real r.*

(ii) ([3, p. 44, Thm. 4.3]) *There is a permutation σ of $\{1, 2, \ldots, n-1\}$, determined by the primitive element α in (2), for which*

$$y_j y_{(j+u) \bmod n} = y_{(j+\sigma(u)) \bmod n} \quad \text{for } 1 \le u < n \text{ and } 0 \le j < n. \tag{3}$$

(iii) ([3, p. 45]) *The periodic autocorrelation of Y satisfies*

$$R_Y(u) = \begin{cases} n & \text{for } u \equiv 0 \pmod{n} \\ -1 & \text{otherwise.} \end{cases}$$

Given an m-sequence Y of length n, Sarwate [12] computed $\mathbb{E}_k[1/F(Y_{k/n})]$ (throughout this paper, $\mathbb{E}_k$ denotes expectation over $k \in \{0, 1, \ldots, n-1\}$, where all such k occur with equal probability).

Theorem 2 (Sarwate [12]). *Let Y be an m-sequence of length $n = 2^m - 1$. Then*

$$\mathbb{E}_k \left[\frac{1}{F(Y_{k/n})} \right] = \frac{(n-1)(n+4)}{3n^2}.$$

As a consequence, there is some rotation of an m-sequence Y of length n having merit factor at least $3n^2/((n-1)(n+4))$, which asymptotically equals 3. This suggests the possibility that a particular rotation of an m-sequence has asymptotic merit factor greater than 3, but Jensen and Høholdt [8] showed that this is impossible.

Theorem 3 (Jensen and Høholdt [8]). *Let Y be an m-sequence of length $n = 2^m - 1$. Then*

$$\lim_{n \longrightarrow \infty} F(Y) = 3.$$

(The limit in Theorem 3 is taken over all n of the form $n = 2^m - 1$ (for $m \geq 2$) and, for each such n, one of the $n\phi(n)/m$ different m-sequences is selected. The theorem states that the limit of $F(Y)$ is always 3, regardless of which m-sequence is chosen for a particular n.)

We shall need an upper bound on the aperiodic autocorrelation of truncated m-sequences. Given an m-sequence Y of length $n = 2^m - 1$, Sarwate [13] established that

$$|C_Y(u)| \leq 1 + \tfrac{2}{\pi}\sqrt{n+1}\log\left(\tfrac{4n}{\pi}\right) \quad \text{for } 1 \leq u < n. \tag{4}$$

We will now show that Lemma 1 (ii) implies that the same bound also holds for truncated m-sequences.

Lemma 4. *Let Y be an m-sequence of length $n = 2^m - 1$, and let ℓ be an integer satisfying $2 \leq \ell \leq n$. Then*

$$|C_{Y^{\ell/n}}(u)| \leq 1 + \tfrac{2}{\pi}\sqrt{n+1}\log\left(\tfrac{4n}{\pi}\right) \quad \text{for } 1 \leq u < \ell.$$

Proof. Let α be the primitive element of $\mathrm{GF}(2^m)$ appearing in the definition of $Y = (y_0, y_1, \ldots, y_{n-1})$ given in (2), and let σ be the permutation determined by α

satisfying (3). Now pick an integer u satisfying $1 \le u < \ell$. Applying Lemma 1 (ii) twice, we find that

$$\begin{aligned} C_{Y^{\ell/n}}(u) &= \sum_{j=0}^{\ell-u-1} y_j y_{j+u} \\ &= \sum_{j=0}^{\ell-u-1} y_{(j+\sigma(u)) \bmod n} \\ &= \sum_{j=0}^{\ell-u-1} y_{(j+\sigma(u)-\sigma(n-\ell+u)) \bmod n}\, y_{(j+\sigma(u)-\sigma(n-\ell+u)+n-\ell+u) \bmod n} \\ &= C_{Y_{k/n}}(n-\ell+u) \qquad \text{for } k = \sigma(u) - \sigma(n-\ell+u). \end{aligned}$$

Since $Y_{k/n}$ is an m-sequence by Lemma 1 (i), the result follows from (4). □

4 An Existence Result on the Merit Factor of Appended m-Sequences

In this section we prove a generalisation of Theorem 2 for appended m-sequences. We then conclude that, for all sufficiently large m, given a primitive element α of $\mathrm{GF}(2^m)$ there exists an m-sequence Y of length $n = 2^m - 1$ of the form (2) and a real number t such that $F(Y; Y^t) > 3.34$.

We begin by proving the following lemma on sums of elements of an m-sequence. This generalises to all nonnegative integers δ a result previously given by Lindholm [11, Eq. (6e)] for $\delta \le n$.

Lemma 5. *Let $Y = (y_0, y_1, \ldots, y_{n-1})$ be an m-sequence of length $n = 2^m - 1$. Given nonnegative integers k and δ, define*

$$S_Y(k,\delta) := \sum_{j=0}^{\delta-1} y_{(k+j) \bmod n}. \tag{5}$$

Then

$$n\,\mathbb{E}_k[(S_Y(k,\delta))^2] = \delta(n-\delta+1) + a(n+1)\,(2\delta - n(a+1))\,,$$

where $a = \lfloor \frac{\delta-1}{n} \rfloor$.

Proof. From the definition (5) of $S_Y(k,\delta)$ we have

$$\begin{aligned} n\,\mathbb{E}_k[(S_Y(k,\delta))^2] &= \sum_{k=0}^{n-1} \sum_{i=0}^{\delta-1} \sum_{j=0}^{\delta-1} y_{(k+i) \bmod n}\, y_{(k+j) \bmod n} \\ &= \sum_{i=0}^{\delta-1} \sum_{j=0}^{\delta-1} R_Y(i-j) \end{aligned}$$

by rearranging the summation and by the definition (1) of the periodic autocorrelation. Further manipulations give

$$n\,\mathbb{E}_k[(S_Y(k,\delta))^2] = \sum_{v=-(\delta-1)}^{\delta-1} (\delta - |v|)\,R_Y(v)$$
$$= \delta\,R_Y(0) + 2\sum_{v=1}^{\delta-1} v\,R_Y(\delta - v)$$

since for every binary sequence A we have $R_A(v) = R_A(-v)$ for all v. Now from Lemma 1 (iii) we find that

$$n\,\mathbb{E}_k[(S_Y(k,\delta))^2] = \delta n - 2\sum_{v=1}^{\delta-1} v + 2(n+1) \sum_{\substack{v=1 \\ v\equiv\delta \pmod n}}^{\delta-1} v$$
$$= \delta n - \delta(\delta-1) + 2(n+1) \sum_{\substack{v=1 \\ v\equiv\delta \pmod n}}^{\delta-1} v. \tag{6}$$

Writing $a = \lfloor \frac{\delta-1}{n} \rfloor$, we have

$$\sum_{\substack{v=1 \\ v\equiv\delta \pmod n}}^{\delta-1} v = \sum_{j=1}^{a} (\delta - jn)$$
$$= a\delta - \tfrac{1}{2}na(a+1),$$

which after combination with (6) proves the lemma. □

We now apply the preceding lemma to prove the following result, in which the sequence $Y_{k/n}; (Y_{k/n})^{\ell/n}$ is obtained by rotating the m-sequence Y by k elements and then appending the resulting first ℓ elements.

Theorem 6. *Let Y be an m-sequence of length $n = 2^m - 1$, and let ℓ be an integer satisfying $0 \le \ell \le n$. Then*

$$\mathbb{E}_k\left[\frac{1}{F(Y_{k/n}; (Y_{k/n})^{\ell/n})}\right] = \frac{(n+\ell)(n+\ell-1)(n-2\ell+4) + 12(n+1)\ell(\ell-1)}{3n(n+\ell)^2}.$$

Proof. Let α be the primitive element of $\mathrm{GF}(2^m)$ appearing in the definition of $Y = (y_0, y_1, \ldots, y_{n-1})$ given in (2), and let σ be the permutation determined by α satisfying (3). Then, by Lemma 1 (ii), for each u satisfying $1 \le u < n + \ell$ and $u \ne \ell$, we have

$$C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n+\ell-u) = \sum_{j=0}^{u-1} y_{(k+j) \bmod n}\, y_{(k+j+n+\ell-u) \bmod n}$$
$$= \sum_{j=0}^{u-1} y_{(\tau(k)+j) \bmod n}$$
$$= S_Y(\tau(k), u), \tag{7}$$

where $\tau(k) := k + \sigma((n+\ell-u) \bmod n)$ and $S_Y(k,\delta)$ is defined in (5). We also have

$$C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n) = \ell, \tag{8}$$

using the convention that $C_A(n) = 0$ for all binary sequences A of length n. Now, since $k \mapsto \tau(k) \bmod n$ is a permutation of $\{0,1,\ldots,n-1\}$ for each u, (8) and application of Lemma 5 to (7) give

$$n\,\mathbb{E}_k\left[\left(C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n+\ell-u)\right)^2\right] = \begin{cases} n\ell^2 & \text{for } u = \ell \\ u(n-u+1) & \text{for } 1 \le u \le n \text{ and } u \ne \ell \\ u(n-u+1) + 2(n+1)(u-n) & \text{for } n < u < n+\ell. \end{cases}$$

We therefore obtain

$$\begin{aligned} &\mathbb{E}_k\left[\frac{n(n+\ell)^2}{2F(Y_{k/n};(Y_{k/n})^{\ell/n})}\right] \\ &= \sum_{u=1}^{n+\ell-1} n\,\mathbb{E}_k\left[\left(C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n+\ell-u)\right)^2\right] \\ &= \sum_{\substack{u=1 \\ u\ne\ell}}^{n+\ell-1} u(n-u+1) + n\ell^2 + \sum_{u=n+1}^{n+\ell-1} 2(n+1)(u-n) \\ &= \tfrac{1}{6}(n+\ell)(n+\ell-1)(n-2\ell+4) + 2(n+1)\ell(\ell-1), \end{aligned}$$

proving the theorem. □

Notice that Theorem 2 arises as the special case $\ell = 0$ of Theorem 6. It follows from Theorem 6 that, for every m-sequence Y and integer ℓ satisfying $0 \le \ell \le n$, there exists an integer k such that

$$F(Y_{k/n};(Y_{k/n})^{\ell/n}) \ge \frac{3n(n+\ell)^2}{(n+\ell)(n+\ell-1)(n-2\ell+4) + 12(n+1)\ell(\ell-1)}.$$

Writing $t = \frac{\ell}{n}$, taking the infimum limit as $n \longrightarrow \infty$, and using Lemma 1 (i), we obtain the following asymptotic result.

Corollary 7. *Let $t \in [0,1]$ be a real number. For each integer m and for each primitive element α of $\mathrm{GF}(2^m)$, there exists a nonzero $\beta \in \mathrm{GF}(2^m)$ such that the m-sequence Y of length $n = 2^m - 1$ defined in (2) satisfies*

$$\liminf_{n\longrightarrow\infty} F(Y;Y^t) \ge \frac{3(1+t)^2}{1+9t^2-2t^3}.$$

In particular,

$$\liminf_{n\longrightarrow\infty} F(Y;Y^t) > 3.3420653 \quad \textit{for } t = 0.1157494.$$

The second statement in the corollary implies that, for all sufficiently large m, given a primitive element α of $\mathrm{GF}(2^m)$, we can pick an m-sequence Y of length $n = 2^m - 1$ of the form (2) such that $F(Y; Y^t) > 3.34$ for $t = 0.1157494$.

5 A Conjecture on the Merit Factor of Appended m-Sequences

The results of the previous section imply that, for each sufficiently large $n = 2^m - 1$, we can choose an m-sequence Y of length n such that the maximum of $F(Y; Y^t)$ over $t \in [0, 1]$ is greater than 3.34. In this section and in the following section we shall present compelling evidence, and therefore conjecture, that

$$\lim_{n \longrightarrow \infty} F(Y; Y^t) = \frac{3(1+t)^2}{1 + 9t^2 - 2t^3} \quad \text{for } t \in [0, 1), \tag{9}$$

regardless of the choice of the m-sequence Y for each particular n. Subject to this conjecture, the asymptotic maximum of $F(Y; Y^t)$ over $t \in [0, 1)$ is approximately 3.34, regardless of the choice of the m-sequence Y for each particular n.

We shall first prove the following theorem, which allows us to replace the conjecture (9) by a simpler one. A result similar to Theorem 8, namely [2, Thm. 6.4], is known to hold for Legendre sequences.

Theorem 8. *Let Y be an m-sequence of length $n = 2^m - 1$, and let $t \in (0, 1)$ be a real number. Then, as $n \longrightarrow \infty$,*

$$\frac{1}{F(Y; Y^t)} \sim 2\left(\frac{t}{1+t}\right)^2 \left(\frac{1}{F(Y^t)} + 1\right) + \left(\frac{1-t}{1+t}\right)^2 \frac{1}{F((Y_t)^{1-t})}.$$

Proof. Write $Y = (y_0, y_1, \ldots, y_{n-1})$ and $\ell := \lfloor tn \rfloor$. By definition we have $Y^t = (y_0, y_1, \ldots, y_{\ell-1})$. Now define $Y' = (y_\ell, y_{\ell+1}, \ldots, y_{n-1})$, so that $Y = Y^t; Y'$. Then by the definition (1) of the periodic autocorrelation we have

$$C_{Y;Y^t}(u) = \begin{cases} R_Y(u) + C_{Y^t}(u) & \text{for } 1 \le u < \ell \\ R_Y(\ell) & \text{for } u = \ell \\ R_Y(u) - C_{Y'}(n-u) & \text{for } \ell < u < n \\ \ell & \text{for } u = n \\ C_{Y^t}(u-n) & \text{for } n < u < n + \ell. \end{cases}$$

In what follows, we will assume that n is large enough such that $2 \le \ell \le n - 2$, in which case all of the above ranges for u are nonempty. Since by Lemma 1 (iii), $R_Y(u) = -1$ for $1 \le u < n$, we then obtain

$$\begin{aligned}\frac{(n+\ell)^2}{2F(Y;Y^t)} &= \sum_{u=1}^{n+\ell-1}[C_{Y;Y^t}(u)]^2 \\ &= \sum_{u=1}^{\ell-1}[C_{Y^t}(u)-1]^2 + 1 + \sum_{u=1}^{n-\ell-1}[C_{Y'}(u)+1]^2 + \ell^2 + \sum_{u=1}^{\ell-1}[C_{Y^t}(u)]^2 \\ &= \frac{\ell^2}{F(Y^t)} + \frac{(n-\ell)^2}{2F(Y')} + \ell^2 + n - 1 - 2\sum_{u=1}^{\ell-1} C_{Y^t}(u) + 2\sum_{u=1}^{n-\ell-1} C_{Y'}(u). \end{aligned} \tag{10}$$

Now by comparing Y' with $(Y_t)^{1-t}$, we find that

$$Y' = \begin{cases} (Y_t)^{1-t} & \text{if } tn \text{ is integer} \\ (Y_t)^{1-t}; y_{n-1} & \text{otherwise.} \end{cases}$$

This gives

$$\left|C_{Y'}(u) - C_{(Y_t)^{1-t}}(u)\right| \le 1 \quad \text{for } 0 \le u < n-\ell \tag{11}$$

with the convention that $C_A(s) = 0$ for each length s binary sequence A. Thus, since Y_t is an m-sequence, we conclude from Lemma 4 that the last two sums in (10) are $O(n^{\frac{3}{2}}\log n)$ as $n \longrightarrow \infty$. Also from (11) and Lemma 4 we find that, as $n \longrightarrow \infty$,

$$\frac{(n-\ell)^2}{2F(Y')} = \frac{(\lfloor(1-t)n\rfloor)^2}{2F((Y_t)^{1-t})} + O(n^{\frac{3}{2}}\log n).$$

Hence, since $\ell \sim tn$, we obtain from (10) the asymptotic relationship

$$\frac{(1+t)^2n^2}{2F(Y;Y^t)} \sim \frac{t^2n^2}{F(Y^t)} + \frac{(1-t)^2n^2}{2F((Y_t)^{1-t})} + t^2n^2,$$

as required. □

Theorem 8 and Lemma 1 (i) imply that, in order to find the asymptotic merit factor of an appended m-sequence $Y;Y^t$ for all $t \in (0,1)$, it is sufficient to know the asymptotic value of $t^2/F(Z^t)$ for all m-sequences Z and for all $t \in (0,1)$. Numerical computations suggest that, for each long m-sequence Y, the curve $1/F(Y^t)$ for $t \in (0,1]$ can be fitted very well by a linear function. This leads us to the following conjecture.

Conjecture 9. *Let Y be an m-sequence of length $n = 2^m - 1$, and let $t \in (0,1]$ be a real number. Then, $\lim_{n\to\infty}(t^2/F(Y^t))$ is well-defined and*

$$\lim_{n\longrightarrow\infty} \frac{t^2}{F(Y^t)} = t^2(1 - \tfrac{2}{3}t).$$

We now use Theorem 8 to show that the conjectured asymptotic form (9) of the merit factor of appended m-sequences is implied by Conjecture 9.

Corollary 10. *Let Y be an m-sequence of length $2^m - 1$, and let $t \in [0,1)$ be a real number. Then, subject to Conjecture 9,*

$$\lim_{n\longrightarrow\infty} F(Y;Y^t) = \frac{3(1+t)^2}{1+9t^2-2t^3}.$$

Proof. The case $t = 0$ follows directly from Conjecture 9 (and is known to be correct by Theorem 3). Subject to Conjecture 9 we conclude from Theorem 8 that, for $t \in (0,1)$,

$$\lim_{n\longrightarrow\infty} F(Y;Y^t) = \frac{(1+t)^2}{2t^2(1-\frac{2}{3}t+1)+(1-t)^2(1-\frac{2}{3}(1-t))},$$

which proves the corollary. □

Under the assumption that Conjecture 9 is correct, elementary calculus gives the maximum asymptotic merit factor achievable by appending to m-sequences.

Corollary 11. *Let Y be an m-sequence of length $n = 2^m - 1$, and assume Conjecture 9 to be correct. Then the maximum of $\lim_{n\to\infty} F(Y;Y^t)$ over $t \in [0,1)$ is given by*

$$\lim_{n\longrightarrow\infty} F(Y;Y^{\hat{t}}) = \frac{3(1+\hat{t})^2}{1+9\hat{t}^2-2\hat{t}^3},$$

where $\hat{t}$ is the solution of

$$t^3 + 3t^2 - 9t + 1 = 0 \quad \textit{for } 0 < t < 1.$$

Approximately we have

$$\lim_{n\longrightarrow\infty} F(Y;Y^{\hat{t}}) \simeq 3.3420653 \quad \textit{and} \quad \hat{t} \simeq 0.1157494.$$

6 Evidence in Favour of Conjecture 9

Conjecture 9 implies that, given an m-sequence Y of length $n = 2^m - 1$,

$$\mathbb{E}_k\left[\frac{t^2}{F((Y_{k/n})^t)}\right] \sim t^2(1-\tfrac{2}{3}t) \quad \text{for } t \in (0,1] \text{ as } n \longrightarrow \infty. \tag{12}$$

This asymptotic relation is implied by setting $\ell = tn$ and letting $n \longrightarrow \infty$ in the following result, which therefore provides evidence in favour of Conjecture 9.

Proposition 12. *Let Y be an m-sequence of length $n = 2^m - 1$, and let ℓ be an integer satisfying $2 \le \ell \le n$. Then*

$$\mathbb{E}_k\left[\frac{1}{F((Y_{k/n})^{\ell/n})}\right] = \frac{(\ell-1)(3n-2\ell+4)}{3n\ell}.$$

Proof. The proof is similar to that of Theorem 6. Let α be the primitive element of $\mathrm{GF}(2^m)$ appearing in the definition of Y given in (2), and let σ be the permutation determined by α satisfying (3). By Lemma 1 (ii), for each u satisfying $1 \le u < \ell$, we have

$$C_{(Y_{k/n})^{\ell/n}}(\ell - u) = S_Y(k + \sigma(\ell - u), u),$$

where $S_Y(k, \delta)$ is defined in (5). Then by Lemma 5

$$n\,\mathbb{E}_k\left[\left(C_{(Y_{k/n})^{\ell/n}}(\ell - u)\right)^2\right] = u(n - u + 1) \quad \text{for } 1 \le u < \ell,$$

so that

$$\begin{aligned}\mathbb{E}_k\left[\frac{n\ell^2}{2F((Y_{k/n})^{\ell/n})}\right] &= \sum_{u=1}^{\ell-1} n\,\mathbb{E}_k\left[\left(C_{(Y_{k/n})^{\ell/n}}(\ell - u)\right)^2\right] \\ &= \sum_{u=1}^{\ell-1} u(n - u + 1) \\ &= \tfrac{1}{6}\ell(\ell - 1)(3n - 2\ell + 4),\end{aligned}$$

as required. □

Notice that Theorem 2 arises as the special case $\ell = n$ of Proposition 12. Proposition 12 and its consequence (12) still leave the possibility that, given an m-sequence Y of length $n = 2^m - 1$ and a real $t \in (0, 1]$, the asymptotic form of $t^2/F((Y_r)^t)$ varies as r ranges over $[0, 1]$. However, we now present numerical data showing that this is apparently not the case, therefore providing further evidence in favour of Conjecture 9.

Let α be a primitive element of $\mathrm{GF}(2^m)$, and let $Y = (y_0, y_1, \ldots, y_{n-1})$ be the m-sequence of length $n = 2^m - 1$ given by (2), where β is chosen such that $y_0 = y_1 = \cdots = y_{m-1} = 1$ (which can be done uniquely by the run property of m-sequences; see [3, p. 44, Thm. 4.2] for example). We inspect the *discrepancy*

$$d(r, t) := \frac{t^2}{F((Y_r)^t)} - t^2(1 - \tfrac{2}{3}t)$$

for

$$(r, t) \in L := \{0, 1/64, 2/64, \ldots, 1\} \times \{1/64, 2/64, \ldots, 1\}.$$

We obtain the following example data for the maximum discrepancy on L:

$$\max_{(r,t)\in L} |d(r, t)| = \begin{cases} 0.018453 & \text{for } n = 2^{11} - 1 \text{ using } \alpha^{11} = \alpha^2 + 1 \\ 0.006677 & \text{for } n = 2^{15} - 1 \text{ using } \alpha^{15} = \alpha + 1 \\ 0.001363 & \text{for } n = 2^{19} - 1 \text{ using } \alpha^{19} = \alpha^5 + \alpha^2 + \alpha + 1 \\ 0.000395 & \text{for } n = 2^{23} - 1 \text{ using } \alpha^{23} = \alpha^5 + 1. \end{cases}$$

The data show that the discrepancy apparently tends to zero with increasing length n. We observed a similar behaviour for other choices for the primitive element α.

7 Comparison to Legendre Sequences

A *Legendre sequence* $X = (x_0, x_1, \ldots, x_{n-1})$ of prime length n is defined for $0 \le j < n$ by

$$x_j := \begin{cases} 1 & \text{for } j \text{ a square modulo } n \\ -1 & \text{otherwise.} \end{cases}$$

The asymptotic merit factor of a Legendre sequence was calculated for all periodic rotations by Høholdt and Jensen [5].

Theorem 13 (Høholdt and Jensen [5]). *Let X be a Legendre sequence of prime length $n > 2$, and let r be a real number satisfying $|r| \le \frac{1}{2}$. Then*

$$\frac{1}{\lim\limits_{n\longrightarrow\infty} F(X_r)} = \tfrac{1}{6} + 8\left(|r| - \tfrac{1}{4}\right)^2.$$

The maximum asymptotic merit factor of a rotated Legendre sequence X_r is 6, which occurs for $r = \frac{1}{4}$ and $\frac{3}{4}$ and is the best proven asymptotic merit factor of a binary sequence family. Borwein, Choi, and Jedwab [2] presented an analysis of the effect of appending for rotated Legendre sequences, similar to the analysis for m-sequences given in Section 5. Extensive numerical data for the behaviour of $1/F((X_r)^t)$ were presented, leading to a conjecture on its asymptotic form. Using a result similar to Theorem 8, the authors of [2] showed that, subject to this conjecture, $\lim_{n\to\infty} F(X_r; (X_r)^t)$ exists for all $r, t \in [0, 1]$ and

$$\max_{r\in[0,1]} \lim_{n\longrightarrow\infty} F(X_r; (X_r)^t) = G(t) \quad \text{for } t \in [0, 1],$$

where

$$G(t) = \begin{cases} \dfrac{6(1+t)^2}{1 + 18t^2 - 8t^3} & \text{for } 0 \le t \le \frac{1}{2} \\ \dfrac{6(1+t)^2}{4 - 12t + 30t^2 - 8t^3} & \text{for } \frac{1}{2} \le t \le 1. \end{cases}$$

We now compare this function with

$$H(t) = \frac{3(1+t)^2}{1 + 9t^2 - 2t^3} \quad \text{for } t \in [0, 1],$$

which, subject to Conjecture 9, equals $\lim_{n\to\infty} F(Y; Y^t)$, where Y is an m-sequence of length $n = 2^m - 1$. The left plot of Figure 1 shows the graphs of $G(t)$ and $H(t)$. The maximum of $G(t)$ in the interval $t \in [0, 1]$ is given by

$$G(\hat{t}_L) \simeq 6.3420596 \quad \text{for } \hat{t}_L \simeq 0.0578279,$$

and, as in Corollary 11, the maximum of $H(t)$ in the interval $t \in [0, 1]$ is given by

$$H(\hat{t}_M) \simeq 3.3420653 \quad \text{for } \hat{t}_M \simeq 0.1157494.$$

Surprisingly (to us), we find $G(\hat{t}_L) - 6 \simeq H(\hat{t}_M) - 3$ and $2\hat{t}_L \simeq \hat{t}_M$, but certainly equality does not hold. Indeed, the right plot of Figure 1 shows that $G(t) - 6$ and $H(2t) - 3$ have very similar graphs in the range $t \in [0, \frac{1}{8}]$. It is doubtful these graphs could be distinguished for $t \simeq 0.058$ purely from numerical data.

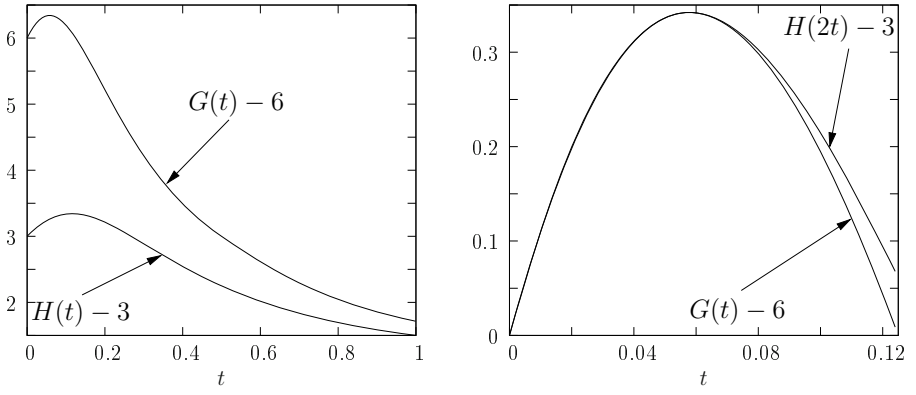


Fig. 1. Comparison of the graphs of $G(t)$ and $H(t)$

References

1. Beenker, G.F.M., Claasen, T.A.C.M., Hermens, P.W.C.: Binary sequences with a maximally flat amplitude spectrum. Philips J. Res. 40, 289–304 (1985)
2. Borwein, P., Choi, K.K.S., Jedwab, J.: Binary sequences with merit factor greater than 6.34. IEEE Trans. Inf. Theory 50(12), 3234–3249 (2004)
3. Golomb, S.W.: Shift register sequences. Holden-Day, Inc., San Francicso (1967)
4. Golomb, S.W., Gong, G.: Signal design for good correlation: for wireless communication, cryptography, and radar. Cambridge University Press, New York (2005)
5. Høholdt, T., Jensen, H.E.: Determination of the merit factor of Legendre sequences. IEEE Trans. Inf. Theory 34(1), 161–164 (1988)
6. Jedwab, J.: A survey of the merit factor problem for binary sequences. In: Helleseth, T., Sarwate, D., Song, H.-Y., Yang, K. (eds.) SETA 2004. LNCS, vol. 3486, pp. 30–55. Springer, Heidelberg (2005)
7. Jedwab, J.: What can be used instead of a Barker sequence? Contemp. Math. 461, 153–178 (2008)
8. Jensen, H.E., Høholdt, T.: Binary sequences with good correlation properties. In: Huguet, L., Poli, A. (eds.) AAECC 1987. LNCS, vol. 356, pp. 306–320. Springer, Heidelberg (1989)
9. Kirilusha, A., Narayanaswamy, G.: Construction of new asymptotic classes of binary sequences based on existing asymptotic classes. Summer Science Program Tech. Report, Dept. Math. Comput. Sci., Univ. Richmond, Richmond, VA (1999)
10. Kristiansen, R.A., Parker, M.G.: Binary sequences with merit factor > 6.3. IEEE Trans. Inf. Theory 50(12), 3385–3389 (2004)
11. Lindholm, J.H.: An analysis of the pseudo-randomness properties of subsequences of long m-sequences. IEEE Trans. Inf. Theory IT-14(4), 569–576 (1968)
12. Sarwate, D.V.: Mean-square correlation of shift-register sequences. IEE Proc. 131, Part F(2), 101–106 (1984)
13. Sarwate, D.V.: An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. IEEE Trans. Inf. Theory IT-30(4), 685–687 (1984)

A With-Carry Walsh Transform
(Extended Abstract)

Andrew Klapper[1,⋆] and Mark Goresky[2]

[1] Department of Computer Science, University of Kentucky,
Lexington, KY 40506-0046, USA
http://www.cs.uky.edu/~klapper/
[2] Department of Mathematics, Institute for Advanced Study
Princeton, N.J. 08540, USA
http://www.math.ias.edu/~goresky/

Abstract. We introduce an arithmetic Walsh transform. It is a with-carry analog, based on modular arithmetic, of the usual Walsh transform of Boolean functions. This is part of our continuing effort to define and investigate with-carry analogs of discrete algebraic structures used in various aspects of communications. We develop tools for analyzing arithmetic Walsh transforms. We prove that the mapping from a Boolean function to its arithmetic Walsh transform is injective. We compute the average arithmetic Walsh transforms and the arithmetic Walsh transforms of affine functions.

Keywords: Walsh transform, 2-adic numbers, Boolean functions.

1 Definitions

A *Boolean function* is a function $f : V_n = \mathbb{F}_2^n \to \mathbb{F}_2$ for some positive integer n. Here $\mathbb{F}_2 = \{0, 1\}$ is the field with 2 elements. We define addition on the set of Boolean functions termwise, $(f + g)(a) = f(a) + g(a)$. The *imbalance* of a Boolean function is the real number $Z(f)$ defined by

$$Z(f) = \sum_{a \in V_n} (-1)^{f(a)}.$$

If $a \in V_n$, then the *shift* of f by a is the real valued function $f_a : V_n \to \mathbb{R}$ defined by $f_a(b) = f(a + b)$. Let $a \cdot b$ denote the inner product of a and b. For any $a \in V_n$, let $T_a(b) = a \cdot b \in \mathbb{F}_2$, $a, b \in V_n$, so that T_a is a linear function. The *Walsh Transform* of f is the real valued function $\widehat{f} : V_n \to \mathbb{R}$ defined by

$$\widehat{f}(a) = Z(f + T_a).$$

⋆ This material is based upon work supported by the National Science Foundation under Grants No. CCF-0514660 and CCF-0914828. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 217–228, 2010.

The Walsh transform plays a central role in the study of the nonlinearity of functions, a study which is central to understanding the cryptographic security of block and stream cipher [1].

We define an arithmetic analog of the Walsh transform by replacing the termwise sum (which is the same as the difference) of functions by the *with-carry* difference. This takes some work since the carries naturally take us outside the domain of the Boolean function. Let $\mathbb{N} = \{0, 1, 2, \cdots\}$ denote the natural numbers. We extend the Boolean function f to $\mathbf{f} : \mathbb{N}^n \to \mathbb{F}_2$ by setting $\mathbf{f}(a_1, \cdots, a_n) = f(a_1 \pmod 2, \cdots, a_n \pmod 2)$. The set P_n of such extensions of Boolean functions is a subset of the set R_n of Boolean valued functions on $\mathbb{N}^n$. It is exactly the set of elements of R_n that are periodic with period 2 in all directions. That is, for every $a, b \in R_n$ we have $\mathbf{f}(a + 2b) = \mathbf{f}(a)$.

In general in this paper we denote Boolean functions by lower case letters and elements of R_n by boldface lowercase letters. The extension of a Boolean function to R_n is denoted by the boldface version of the letter denoting the Boolean function. Vectors in $\mathbb{N}^n$ are denoted by lowercase letters from the beginning of the alphabet. We denote the inner product of two integer vectors a and b by $a \cdot b$. We denote the reduction of an integer x modulo 2 by $[x]_2$. Thus the $\mathbb{F}_2$-inner product of two binary vectors a and b is $[a \cdot b]_2$

We now define an algebraic structure on the set R_n. To understand this definition it is helpful to recall the definition of the 2-adic integers (in fact R_1 is exactly the 2-adic integers). A 2-adic integer is a formal expression

$$\mathbf{f} = \sum_{i=0}^{\infty} f_i 2^i,$$

where $f_i \in \mathbb{F}_2$. We can identify this 2-adic integer with the function on $\mathbb{N}$ that maps i to f_i. We denote the set of 2-adic integers by $\mathbb{Z}_2$. There is a well defined algebraic structure on the set of 2-adic integers that makes it a ring. It is based on doing addition and multiplication with carry. The algebra of 2-adic integers has been studied for more than 100 years [2,5] and recently the authors and others have used this algebra extensively in the study of fast generation of pseudorandom sequences [3,4].

A function $\mathbf{f} \in R_1$ is identified with the 2-adic integer $\sum f(a)2^a$. To generalize this notion to multiple dimensions, we want a multi-term analog of the 2-adic integer in much the same way that we generalize power series in one variable to power series in several variables. The new structure can be thought of as having several "2s". To distinguish them from the ordinary integer 2, we denote them by $t_1, \cdots, t_n$. Then a multi-2-adic integer is a formal expression

$$\sum_{a=(a_1,\cdots,a_n)\in\mathbb{N}^n} f_a t_1^{a_1} \cdots t_n^{a_n},$$

with $f_a \in \mathbb{F}_2$. We can identify an element $\mathbf{f} \in R_n$ with a multi-2-adic integer by simply setting $f_a = \mathbf{f}(a)$. When we do arithmetic, we want a coefficient equal to 2 to induce a carry to "the next place in each variable". That is, to

the monomial with the exponent of each t_i increased by one. For convenience, if $a \in \mathbb{N}^n$, we let t^a denote $t_1^{a_1} \cdots t_n^{a_n}$. Also, let $1^n = (1, 1, \cdots, 1) \in \mathbb{N}^n$ and $0^n = (0, 0, \cdots, 0) \in \mathbb{N}^n$.

We define an addition operation by saying that

$$\sum_{a \in \mathbb{N}^n} f_a t^a + \sum_{a \in \mathbb{N}^n} g_a t^a = \sum_{a \in \mathbb{N}^n} h_a t^a$$

if there exist integers $\{d_a : a \in \mathbb{N}^n\}$ so that $d_a = 0$ if any component of a is zero, and for all $a \in \mathbb{N}^n$, we have

$$f_a + g_a + d_a = h_a + 2d_{a+1^n}.$$

In other words, addition is just 2-adic addition along the diagonals $D_a = \{a + c(1, 1, \cdots, 1) : c \in \mathbb{N}\}$, where $a \in \mathbb{N}$.

We define a multiplication operation by saying that

$$\sum_{a \in \mathbb{N}^n} f_a t^a \cdot \sum_{a \in \mathbb{N}^n} g_a t^a = \sum_{a \in \mathbb{N}^n} h_a t^a$$

if there exist integers $\{d_a : a \in \mathbb{N}^n\}$ so that $d_a = 0$ if any component of a is zero, and for all a

$$\sum_{b+c=a} f_b g_c + d_a = h_a + 2d_{a+1^n}.$$

This is not simply multiplication along the diagonals.

In contrast, we let

$$\mathbb{Z}[[t_1, \cdots, t_n]] = \left\{ \sum_{\substack{a=(a_1,\cdots,a_n),\\ a_j \in \mathbb{N}}} c_a t_1^{a_1} \cdots t_n^{a_n} : c_a \in \mathbb{Z} \right\}$$

be the power series ring in n variables over the integers. In his ring the t_i are treated as variables and are added and multiplied as for polynomials with no carry. We can think of an element of $\mathbb{Z}[[t_1, \cdots, t_n]]$ as a function from $\mathbb{N}^n$ to $\mathbb{Z}$.

Theorem 1. *The ring R_n is isomorphic to the quotient ring*

$$S_n = \mathbb{Z}[[t_1, \cdots, t_n]]/(t_1 t_2 \cdots t_n - 2)$$

The proof (which we omit) of Theorem 1 involves the fact that an element $\mathbf{f} \in R_n$ can be represented either as a function $\mathbf{f}$ from $\mathbb{N}^n$ to $\{0, 1\}$ (i.e., as an element of $\mathbb{Z}[[t_1, \cdots, t_n]]$ with coefficients in $\{0, 1\}$), or as a function $\bar{f}$ from $\{a = (a_1, \cdots, a_n) : a_1, \cdots, a_n \in \mathbb{N}$ and at least one $a_i = 0\}$ to $\mathbb{Z}_2$. We use boldface symbols in the former case and overlined symbols in the latter. These representations are connected by the formula

$$\bar{f}(a) = \sum_{i=0}^{\infty} \mathbf{f}(a + i \cdot 1^n) 2^i. \tag{1}$$

We refer to $\bar{f}(a)$ as the *restriction* of f to the diagonal D_a. The same notation and terminology will be used even if a does not have a zero component.

Let $P_n \subset R_n$ denote the set of functions $\mathbf{f}$ that have period 2 in all directions: $f(a+2b) = f(a)$ for all $a, b \in R_n$. If $\mathbf{f}, \mathbf{g} \in P_n$ then $\mathbf{f}+\mathbf{g}$ may fail to be periodic, but it will be *eventually 2-periodic* in the following sense.

Definition 2. *The element $\mathbf{f} \in R_n$ is eventually p-periodic if there is an integer k so that if $a = (a_1, \cdots, a_n) \in \mathbb{N}^n$, and $a_i \geq k$ for $i = 1, \cdots, n$, then for every $b \in \mathbb{N}^n$, $\mathbf{f}(a+pb) = \mathbf{f}(a)$. If $a = (a_1, \cdots, a_n) \in \mathbb{N}^n$, and $a_i \geq k$ for $i = 1, \cdots, n$, then the restriction of $\mathbf{f}$ to the set $\{a + b : b = (b_1, \cdots, b_n), 0 \leq b_i < p, i = 1, \cdots, n\}$ is called a* complete period *of $\mathbf{f}$.*

We can be more precise. Let $\mathbf{f} = \sum_{i=0}^{\infty} f_i 2^i$ and $\mathbf{g} = \sum_{i=0}^{\infty} g_i 2^i$ be 2-adic integers whose coefficient sequences have period 2. Then the coefficients of index ≥ 2 of $-\mathbf{f}$, $\mathbf{f}+\mathbf{g}$, and $\mathbf{f}-\mathbf{g}$ are periodic.

If $\mathbf{f} : \mathbb{N} \to \{0, 1\}$ is strictly 2-periodic, then in the representation in equation (1) we have

$$\begin{aligned} \bar{f}(a) &= \sum_{i=0}^{\infty} \mathbf{f}(a + i \cdot 1^n) 2^i \\ &= f(a) + f(a+1^n)2 + f(a)2^2 + f(a+1^n)2^3 + \cdots \\ &= -\frac{f(a) + 2f(a+1^n)}{3}. \end{aligned} \tag{2}$$

2 Walsh Transforms

Now we can define the arithmetic Walsh transform. First we extend the notion of imbalance to eventually p-periodic elements.

Definition 3. *Let $\mathbf{f} \in R_n$ be eventually p-periodic. Then the* imbalance *of $\mathbf{f}$ is*

$$Z(\mathbf{f}) = \sum_a (-1)^{\mathbf{f}(a)} \in \mathbb{Z},$$

where the sum is extended over one complete period of $\mathbf{f}$.

Note that $Z(\mathbf{f})$ is independent of the choice of complete period. This definition is consistent with the definition of the imbalance of Boolean functions in the sense that the imbalance of a Boolean function equals the imbalance of its periodic extension to $\mathbb{N}^n$.

Definition 4. *The* arithmetic Walsh transform *of an eventually periodic $\mathbf{f} \in R_n$ is the integer valued function $\widetilde{\mathbf{f}} : V_n \to \mathbb{Z}$ defined by $\widetilde{\mathbf{f}}(a) = Z(\mathbf{f} - \mathbf{T}_a)$. If f is a Boolean function on V_n, then the* arithmetic Walsh Transform *of f is the arithmetic Walsh Transform of the extension $\mathbf{f}$ of f, $\widetilde{f}(a) = \widetilde{\mathbf{f}}(a)$.*

Let $U_n = \{a = (a_1, \cdots, a_n) : a_i \in \{0,1\} \text{ and } a_1 = 0\}$. The restriction of an eventually periodic function $\mathbf{f} \in R_n$ to a diagonal D_a with $a \in U_n$ is eventually periodic. If we select one full period from each of these diagonals, altogether we will have one complete period of $\mathbf{f}$. It follows that the imbalance of $\mathbf{f}$ is the sum of the imbalances of the restrictions of $\mathbf{f}$ to the diagonals. The imbalance of the restriction of $\mathbf{f}$ to diagonal D_a in turn is the imbalance of the 2-adic integer $\bar{f}(a)$ (defined in equation (1)). This then is the imbalance of the 2-adic representation of the rational number in equation (2). Thus

$$Z(f) = \sum_{a \in U_n} Z(\bar{f}(a)). \tag{3}$$

Theorem 5. *Let $f : V_n \to \mathbb{F}_2$ be a Boolean function. If $b \cdot 1^n = 0$, then*

$$\begin{aligned}\widetilde{f}(b) &= \sum_{a \in U_n} 2(1 - f(a) - f(a+1^n) + 2f(a)f(a+1^n)[a \cdot b]_2) \\ &= 2^n - 2\sum_{a \in V_n} f(a) + 4\sum_{a \in U_n} f(a)f(a+1^n)[a \cdot b]_2 \qquad (4) \\ &= 2^n - 2\sum_{a \in V_n} f(a) + 2\sum_{a \in V_n} f(a)f(a+1^n)[a \cdot b]_2 \qquad (5)\end{aligned}$$

If $b \cdot 1^n = 1$, then

$$\begin{aligned}\widetilde{f}(b) &= 2\sum_{a \in U_n} (f(a+1^n) - f(a)f(a+1^n) + (f(a) - f(a+1^n))[a \cdot b]_2) \qquad (6) \\ &= \sum_{a \in V_n} (f(a+1^n) - f(a)f(a+1^n) + (f(a) - f(a+1^n))[a \cdot b]_2). \qquad (7)\end{aligned}$$

Proof. If $b \cdot 1^n = 1 \pmod 2$, then $[(a+1^n) \cdot b]_2 = [a \cdot b]_2 + 1 \pmod 2 = 1 - [a \cdot b]_2$. It then follows from the discussion above that

$$\begin{aligned}\widetilde{f}(b) &= \sum_{a \in U_n} Z((\bar{f} - \bar{T}_b)(a)) \\ &= \sum_{a \in U_n} Z\left(-\frac{f(a) + 2f(a+1^n) - [a \cdot b]_2 - 2[(a+1^n) \cdot b]_2}{3}\right) \\ &= \begin{cases} \displaystyle\sum_{a \in U_n} Z\left(-\frac{f(a) + 2f(a+1^n)}{3} + [a \cdot b]_2\right) & \text{if } b \cdot 1^n = 0 \\ \displaystyle\sum_{a \in U_n} Z\left(-\frac{f(a) + 2f(a+1^n) + [a \cdot b]_2 - 2}{3}\right) & \text{if } b \cdot 1^n = 1. \end{cases}\end{aligned}$$

The 2-adic expansion of $u/3$ is eventually periodic with period 2 and each period equals 10 or 01 unless u is a multiple of 3. In these cases the imbalance is always 0. If u is a multiple of 3, then the eventual period is 1 and each period is either

1 (if u is negative) or 0 (if u is nonnegative). The imbalance is thus -2 if u is negative and is 2 if u is nonnegative. Let $Z_a = Z((\bar{f} - \bar{T}_b)(a))$.

Let $b \cdot 1^n = 0$. From a table of values of Z_a as a function of $f(a)$, $f(a+1^n)$ and $[a \cdot b]_2$, using Lagrange interpolation we find that $Z_a = 2(1 - f(a) - f(a+1^n) + 2f(a)f(a+1^n)[a \cdot b]_2)$. Similarly, if $b \cdot 1^n = 1$ we find that $Z_a = 2(f(a+1^n) - f(a)f(a+1^n) + (f(a) - f(a+1^n))[a \cdot b]_2)$. This definition of Z_a makes sense for $a \notin U_n$ as well. It can be checked that $Z_a = Z_{a+1^n}$. Thus the last equality holds. This proves the theorem. □

Corollary 6. *If f is a Boolean function on V_n, and $b \cdot 1^n = 0$, then $\widetilde{f}(b)$ is even.*

Let us consider for a moment the classical case of Boolean functions and Walsh transforms. If f and g are Boolean functions, then the distance between f and g is $\delta(f,g) = |\{a \in V_n : f(a) \neq g(a)\}|$. This is a true distance measure. It is well-known that $Z(f-g) = 2^n - \delta(f,g)$. In particular, $Z(f-g) = 2^n$ if and only if $\delta(f,g) = 0$ if and only if $f = g$. Also, $Z(f-g) = -2^n$ if and only if f is the complement of g. Thus f has a Walsh coefficient equal to 2^n if and only if f is linear, and has a Walsh coefficient equal to -2^n if and only if f is affine and nonlinear.

Now we return to the arithmetic case. Let f and g be Boolean functions and let $\mathbf{f}$ and $\mathbf{g}$ be their extensions. Suppose that $Z(\mathbf{f} - \mathbf{g}) = 2^n$. From equation (3) it follows that for every $a \in U_n$, $Z(\bar{f}(a) - \bar{g}(a)) = 2$. That is,

$$Z\left(\frac{g(a) - f(a) + 2(g(a+1^n) - f(a+1^n))}{3}\right) = 2.$$

This holds if and only if either (1) $f(a) = g(a)$ and $f(a+1^n) = g(a+1^n)$ or (2) $g(a) = g(a+1^n) = 1$ and $f(a) = f(a+1^n) = 0$. Thus g is obtained from f by choosing some elements $X \subseteq U_n$ so that f is 0 on the diagonal determined by each $a \in X$ and changing the value on these diagonals to 1. Alternatively, f is obtained from g by choosing some elements $Y \subseteq U_n$ so that g is 1 on the diagonal determined by each $a \in Y$ and changing the value on these diagonals to 0.

Now suppose g is a linear function, say $g(a) = [a \cdot b]_2$, $b \neq 0^n$. The function g is constant on some diagonal if and only if $g(1^n) = 0$. In this case g is 1 on exactly 2^{n-2} diagonals, so there are $2^{2^{n-2}} - 1$ nonlinear functions f so that $\widetilde{f}(b) = 2^n$.

3 Uniqueness of Arithmetic Walsh Transforms

In this section we show that a Boolean function is uniquely determined by its arithmetic Walsh transform. We do not, however, know a simple expression for the inverse arithmetic Walsh transform, or even an efficient way to compute it.

It follows from equation (4) that if $b \neq 0^n$ and $\mathrm{wt}(b)$ is even, then

$$\sum_{a \in U_n} f(a)f(a+1^n)[a \cdot b]_2 = \frac{\widetilde{f}(b) + \widetilde{f}(0^n)}{4}. \tag{8}$$

Let M_n be the $(2^{n-1}-1)\times(2^{n-1}-1)$ rational matrix indexed by $U_n-\{0^n\}$ and $W_n=\{b\in V_n : \mathrm{wt}(b) \text{ even}, b\neq 0^n\}$, whose entry with index (a,b) is $[a\cdot b]_2$ treated as a rational number. Similarly, let N_n be the $(2^{n-1}-1)\times(2^{n-1}-1)$ rational matrix indexed by $U_n-\{0^n\}$ and $T_n=\{b\in V_n : \mathrm{wt}(b) \text{ odd}, b\neq 10^{n-1}\}$, whose entry with index (a,b) is $[a\cdot b]_2$ treated as a rational number.

Let v be the vector indexed by $U_n-\{0^n\}$ whose entry with index a is $v(a)=f(a)f(a+1^n)$. Let z be the vector indexed by W_n whose entry with index b is $z(b)=(\widetilde{f}(b)+\widetilde{f}(0^n))/4$. Then equation (8) implies that $vM_n=z$. Thus if M_n is invertible, then the $v(a)$ with $a\neq 0^n$ or 1^n can be determined uniquely from the $\widetilde{f}(b)$.

Similarly, it follows from equation (6) that if $b\neq 10^{n-1}$ and $\mathrm{wt}(b)$ is odd, then

$$\sum_{a\in U_n}(f(a)-f(a+1^n))[a\cdot b]_2=\frac{\widetilde{f}(b)-\widetilde{f}(10^{n-1})}{2}. \tag{9}$$

Let u be the vector indexed by $U_n-\{0^n\}$ whose entry with index a is $u(a)=f(a)-f(a+1^n)$. Let w be the vector indexed by T_n whose entry with index b is $w(b)=(\widetilde{f}(b)-\widetilde{f}(10^{n-1}))/2$. Then equation (9) implies that $uN_n=w$. Thus if N_n is invertible, then the $u(a)$ with $a\neq 10^{n-1}$ can be determined uniquely from the $\widetilde{f}(b)$.

Theorem 7. *The matrices M_n and N_n have nonzero determinants.*

Proof (Proof Sketch). We order the indices in both dimensions lexicographically, with most significant position on the right. For both types of matrices, we think of the rows (the as) as being divided into three segments:

1. The rows indexed by $a=0a'0$ with $a'\neq 0^{n-2}$;
2. The row indexed by $a=0^{n-1}1$; and
3. The rows indexed by $a=0a'1$ with $a'\neq 0^{n-2}$.

For M_n, we think of the columns (the bs) as being divided into three segments:

1. The columns indexed by $b=b'0$ with $\mathrm{wt}(b')$ even and $b'\neq 0^{n-1}$;
2. The column indexed by $b=10^{n-2}1$; and
3. The columns indexed by $b=b'1$ with $\mathrm{wt}(b')$ odd and $b'\neq 10^{n-2}$.

Let $\langle 1\rangle_n$ denote the $2^n\times 2^n$ matrix all of whose entries are 1. Following these decompositions of the indices, we can decompose M_n into blocks as follows.

1. If $a=0a'0$ with $a'\neq 0^{n-2}$ and $b=b'0$ with $b'\neq 0^{n-1}$ and $\mathrm{wt}(b')$ even, then $[0a'\cdot b']_2=[a\cdot b]_2$. Thus the upper left hand block of M_n equals M_{n-1}.
2. If $a=0a'1$ with $a'\neq 0^{n-2}$ and $b=b'0$ with $b'\neq 0^{n-1}$ and $\mathrm{wt}(b)$ even, then $[0a'\cdot b']_2=[a\cdot b]_2$. Thus the lower left hand block of M_n equals M_{n-1}.
3. If $a=0a'0$ with $a'\neq 0^{n-2}$ and $b=b'1$ with $b'\neq 10^{n-2}$ and $\mathrm{wt}(b')$ odd, then $[0a'\cdot b']_2=[a\cdot b]_2$. Thus the upper right hand block of M_n equals N_{n-1}.
4. If $a=0a'1$ with $a'\neq 0^{n-2}$ and $b=b'1$ with $b'\neq 10^{n-2}$ and $\mathrm{wt}(b')$ odd, then $[0a'\cdot b']_2=1-[a\cdot b]_2$. Thus the lower right hand block of M_n equals $\langle 1\rangle_{n-1}-N_{n-1}$.

5. If $a = 0^{n-1}1$, then the row indexed by a is $0^{2^{n-1}-1}1^{2^{n-1}}$.
6. If $b = 10^{n-2}1$, then the column indexed by b is $0^{2^{n-1}-1}1^{2^{n-1}}$.

We can summarize this by saying

$$M_n = \begin{bmatrix} & & 0 & & \\ & M_{n-1} & \vdots & N_{n-1} & \\ & & 0 & & \\ 0 & \cdots & 0\,1\,1 & \cdots & 1 \\ & & 1 & & \\ & M_{n-1} & \vdots & \langle 1\rangle_{n-1} - N_{n-1} & \\ & & 1 & & \end{bmatrix}$$

By subtracting the first block of rows from the last block of rows, then subtracting the row indexed by $a = 0^{n-1}1$ from each of the last block of rows, we have

$$\det(M_n) = \det \begin{bmatrix} & & 0 & & \\ & M_{n-1} & \vdots & N_{n-1} & \\ & & 0 & & \\ 0 & \cdots & 0\,1\,1 & \cdots & 1 \\ & & 0 & & \\ & 0 & \vdots & -2N_{n-1} & \\ & & 0 & & \end{bmatrix} = 2^{2^{n-1}-1} \det(M_{n-1}) \det(N_{n-1}). \tag{10}$$

A similar argument shows that

$$\det(N_n) = 2^{2^{n-1}-1} \det(M_{n-1}) \det(N_{n-1}). \tag{11}$$

Finally, we see that M_2 and N_2 are 1×1 matrices whose single entries are 1, hence whose determinants are 1. It follows that the determinant of M_n and N_n are nonzero as claimed. □

Corollary 8. *The values of $u(a)$ and $v(a)$ for $a \in U_n - \{0^n\}$ are uniquely determined by the $\widetilde{f}(b)$. This in turn uniquely determines the values of the $f(a)$ for $a \neq 0^n, 1^n$.*

Proof. The first statement follows from Theorem 7. Since $f(a), f(a+1^n) \in \{0, 1\}$, from a table of possible values of $f(a)$, $f(a+1^n)$, $u(a)$, and $v(a)$ we see that $f(a)$ and $f(a + 1^n)$ are uniquely determined by any valid value of $u(a)$ and $v(a)$. □

Having determined the $f(a)$ with $a \neq 0^n, 1^n$, we are left with two equations in the unknowns $f(0^n)$ and $f(1^n)$. From equation (5) with $b = 0^n$ we have $f(0^n) + f(1^n) = x$ for some $x \in \mathbb{Q}$, and from equation (7) with $b = 10^{n-1}$ we have $f(1^n) - f(0^n)f(1^n) = y$ for some $y \in \mathbb{Q}$. The values x and y are uniquely determined by the $\widetilde{f}(b)$.

Again, from a table of possible values of $f(0^n)$, $f(1^n)$, x, and y it follows that $f(0^n)$ and $f(1^n)$ are uniquely determined by any valid value of x and y. We have proved the following theorem.

Theorem 9. *Every Boolean function on V_n is uniquely determined by its arithmetic Walsh transform.*

Embedded in this proof is a method of computing the function f from its arithmetic Walsh transform. It is, however, more complicated than the situation for classical Walsh transforms where one simply computes essentially the Walsh transform of the Walsh transform. We do not know of such an idempotency law for the arithmetic Walsh transform.

4 Expected Arithmetic Walsh Transform

Recall that for a Boolean function f, the expectation of the classical Walsh coefficients of f is $(-1)^{f(0)}$ and the second moment is 2^n (independent of f). The picture is quite different in the arithmetic case.

Let

$$H(f) = \sum_{a \in V_n} f(a),$$

the Hamming weight of f, and let

$$Q(f) = \sum_{a \in U_n} f(a)f(a+1^n) = \frac{1}{2} \sum_{a \in V_n} f(a)f(a+1^n),$$

the number of diagonals on which f is a constant 1.

Lemma 10. *If f is a Boolean function on n variables, then*

$$\sum_{a \in V_n} f(a)f(a+1^n) \sum_{b \cdot 1^n = 0} [a \cdot b]_2 = 2^{n-1}Q(f) - 2^{n-1}f(0^n)f(1^n),$$

$$\sum_{a \in V_n} (f(a) - f(a+1^n))) \sum_{b \cdot 1^n = 1} [a \cdot b]_2 = 2^{n-1}(f(1^n) - f(0^n)),$$

Proof. For any $a \in V_n$, let

$$S_a = \sum_{b \cdot 1^n = 0} [a \cdot b]_2 \quad \text{and} \quad T_a = \sum_{b \cdot 1^n = 1} [a \cdot b]_2.$$

If $a = 0^n$ or $a = 1^n$, then $S_a = 0$. Otherwise 1^n and a are linearly independent modulo 2. Thus $\sum_{b \cdot 1^n = 0} [a \cdot b]_2 = 2^{n-2}$, so

$$\sum_{a \in V_n} f(a)f(a+1^n) \sum_{b \cdot 1^n = 0} [a \cdot b]_2 = 2^{n-1}Q(f) - 2^{n-1}f(0^n)f(1^n).$$

Similarly, if $a = 0^n$, then $T_a = 0$. If $a = 1^n$, then $T_a = 2^{n-1}$. Otherwise $T_a = 2^{n-2}$. Since $\sum_{a \in V_n} (f(a) - f(a+1^n))) = 0$, we have

$$\sum_{a \in V_n} (f(a) - f(a+1^n)) \sum_{b \cdot 1^n = 0} [a \cdot b]_2 = 2^{n-1}(f(1^n) - f(0^n)).$$

□

Theorem 11. *Let f be a Boolean function on n variables. The expected arithmetic Walsh transform of f is*

$$E[\widetilde{f}] = 2^{n-1} - \frac{H(f) + f(0^n) - f(1^n)}{2} - f(0^n)f(1^n).$$

Proof. We have

$$E[\widetilde{f}] = \frac{1}{2^n}\sum_{b\in V_n}\widetilde{f}(b) = \frac{1}{2^n}\left(\sum_{b\cdot 1^n=0}\widetilde{f}(b) + \sum_{b\cdot 1^n=1}\widetilde{f}(b)\right).$$

We use equations (5) and (7) and Lemma 10 to compute these two sums separately. For the first sum we have

$$\begin{aligned}\sum_{b\cdot 1^n=0}\widetilde{f}(b) &= \sum_{b\cdot 1^n=0}\left(2^n - 2\sum_{a\in V_n} f(a) + 2\sum_{a\in V_n} f(a)f(a+1^n)[a\cdot b]_2\right)\\ &= 2^{2n-1} - 2^n H(f) + 2^n Q(f) - 2^n f(0^n)f(1^n)\end{aligned}$$

by Lemma 10.

Similarly, for the second sum we have

$$\sum_{b\cdot 1^n=1}\widetilde{f}(b) = 2^{n-1}H(f) - 2^n Q(f) + 2^{n-1}(f(1^n) - f(0^n)),$$

again by Lemma 10. It follows that

$$E[\widetilde{f}] = 2^{n-1} - \frac{H(f) + f(0^n) - f(1^n)}{2} - f(0^n)f(1^n),$$

as claimed. □

5 Arithmetic Walsh Transforms of Linear Functions

In this section we make use of the analysis in Sect. 2 to completely describe the arithmetic correlations of linear functions. That is, of Boolean functions $f(a) = \mathbf{T}_c(a) = [a\cdot c]_2$, $a, c \in V_n$.

If $c = 0^n$, then f is identically zero. By Theorem 5,

$$\widetilde{\mathbf{T}}_{0^n}(b) = \begin{cases} 2^n & \text{if } b\cdot 1^n = 0\\ 0 & \text{if } b\cdot 1^n = 1.\end{cases}$$

For the remainder of the section we assume that $c \neq 0^n$. By equation (5), if $b\cdot 1^n = 0$, then

$$\begin{aligned}\widetilde{\mathbf{T}}_c(b) &= 2^n - 2\sum_{a\in V_n}[a\cdot c]_2 + 2\sum_{a\in V_n}[a\cdot c]_2[(a+1^n)\cdot c]_2[a\cdot b]_2\\ &= 2\sum_{a\in V_n}[a\cdot c]_2[(a+1^n)\cdot c]_2[a\cdot b]_2. \qquad (12)\end{aligned}$$

By equation (7), if $b \cdot 1^n = 1$, then

$$\widetilde{\mathbf{T}}_c(b) = \sum_{a \in V_n} [(a + 1^n) \cdot c]_2 (1 - [a \cdot c]_2) + ([a \cdot c]_2 - [(a + 1^n) \cdot c]_2)[a \cdot b]_2). \quad (13)$$

We treat these equations separately. First suppose that $b \cdot 1^n = 0$. If $b = 0^n$, then $\widetilde{\mathbf{T}}_c(b) = 0$. If $b \neq 0^n$ and $c \cdot 1^n = 0$, then

$$\widetilde{\mathbf{T}}_c(b) = 2 \sum_{a \in V_n} [a \cdot c]_2 [a \cdot c]_2 [a \cdot b]_2 = 2 \sum_{a \in V_n} [a \cdot c]_2 [a \cdot b]_2$$
$$= \begin{cases} 2 \sum_{a \in V_n} [a \cdot c]_2 = 2^n \text{ if } b = c \\ 2 \cdot 2^{n-2} = 2^{n-1} \quad \text{if } b \neq c. \end{cases}$$

(The last line holds because $[a \cdot c]_2 [a \cdot b]_2 = 1$ on the intersection of two hyperplanes and is 0 everywhere else.) The last case occurs for $2^{n-1} - 2$ values of b for each such c. If $c \cdot 1^n = 1$, then

$$\widetilde{\mathbf{T}}_c(b) = 2 \sum_{a \in V_n} [a \cdot c]_2 (1 - [a \cdot c]_2)[a \cdot b]_2 = 0,$$

since if $x \in \{0, 1\}$, then $x(1 - x) = 0$. This occurs for 2^{n-1} values of b for each such c.

Now suppose that $b \cdot 1^n = 1$. If $c \cdot 1^n = 0$, then

$$\widetilde{\mathbf{T}}_c(b) = \sum_{a \in V_n} [a \cdot c]_2 (1 - [a \cdot c]_2) + ([a \cdot c]_2 - [a \cdot c]_2)[a \cdot b]_2) = 0.$$

This occurs for 2^{n-1} values of b for each such c. If $c \cdot 1^n = 1$, then

$$\widetilde{\mathbf{T}}_c(b) = \sum_{a \in V_n} (1 - [a \cdot c]_2)^2 + (2[a \cdot c]_2 - 1)[a \cdot b]_2)$$
$$= \begin{cases} 2^{n-1} + \sum_{a \in V_n} 2[a \cdot c]_2^2 - [a \cdot c]_2 = 2^n & \text{if } b = c \\ 2^{n-1} + \sum_{a \in V_n} 2[a \cdot c]_2 [a \cdot b]_2 - [a \cdot b]_2 = 2^{n-1} \text{ if } b \neq c. \end{cases}$$

The second case occurs for $2^{n-1} - 1$ values of b for each such c. Now we fix c and describe the distribution of values of $\widetilde{\mathbf{T}}_c(b)$.

Theorem 12. *Let $c \in V_n$. If $c = 0^n$, then the arithmetic Walsh transform of $\mathbf{T}_c$ has values 0, which occurs 2^{n-1} times, and 2^n, which occurs 2^{n-1} times. If $c \cdot 1^n = 0$ and $c \neq 0^n$, then the arithmetic Walsh transform of $\mathbf{T}_c$ has values 0, which occurs $2^{n-1} + 1$ times, 2^{n-1}, which occurs $2^{n-1} - 2$ times, and 2^n, which occurs once. If $c \cdot 1^n = 1$, then the arithmetic Walsh transform of $\mathbf{T}_c$ has values 0, which occurs 2^{n-1} times, 2^{n-1}, which occurs $2^{n-1} - 1$ times, and 2^n, which occurs once.*

Similarly, for affine functions we have the following theorem.

Theorem 13. *Let $c \in V_n$. If $c = 0^n$, then the arithmetic Walsh transform of $1 - \mathbf{S}_c$ has values 0, which occurs 2^{n-1} times, and -2^n, which occurs 2^{n-1} times. If $c \cdot 1^n = 0$ and $c \neq 0^n$, then the arithmetic Walsh transform of $1 - \mathbf{S}_c$ has values 0, which occurs $2^{n-1} + 2$ times and 2^{n-1}, which occurs $2^{n-1} - 2$ times. If $c \cdot 1^n = 1$, then the arithmetic Walsh transform of $1 - \mathbf{S}_c$ has values 0, which occurs $2^{n-1} + 1$ times and 2^{n-1}, which occurs $2^{n-1} - 1$ times.*

6 Conclusions

We have defined a new arithmetic (or with-carry) version of the Walsh transform of a Boolean function, and we have explored some of its basic properties: invertibility of the transform, its average behavior, and its value on linear functions.

Many questions remain. In the case of classical Walsh transforms, the second moment plays a critical role through Parseval's identity, and gives rise to the notion of bent functions. In the arithmetic case we can show that the second moment is much more complicated. This leaves open the problem of defining arithmetically bent functions. We also mention that the methods used here can be used to define arithmetic versions of the cross-correlation of Boolean functions. We shall explore these and other issues in future work.

In the classical case the Walsh transform can be interpreted as telling us how close a given function is to a linear function, and this gives the Walsh transform significance in cryptography. In the arithmetic case it remains to be seen whether there is cryptographic significance. We can try to relate it to some notion of with-carry distance to linear functions, but this leads to messier definitions. For example, in one sense there are nonlinear functions whose with-carry distance to linear functions is zero. We leave this issue and the broader issue of applications of the arithmetic Walsh transform as open questions.

References

1. Cusick, T., Stanica, P.: Cryptographic Boolean Functions and Applications. Academic Press, San Diego (2009)
2. Gauss, C.F.: Disquisitiones Arithmeticae (1801); reprinted in English translation by Yale Univ. Press, New Haven (1966)
3. Goresky, M., Klapper, A.: Arithmetic Cross-Correlations of FCSR Sequences. IEEE Trans. Info. Theory 43, 1342–1346 (1997)
4. Klapper, A., Goresky, M.: Feedback Shift Registers, Combiners with Memory, and 2-Adic Span. Journal of Cryptology 10, 111–147 (1997)
5. Koblitz, N.: p-Adic Numbers, p-Adic Analysis, and Zeta Functions. Springer, New York (1984)

Clock-Controlled FCSR Sequence with Large Linear Complexity

Zhen Pan, Wei Su, and Xiaohu Tang*

Key Laboratory of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, Sichuan, 610031, P.R. of China
zpan5@163.com, suwei060166@yahoo.com.cn, xhutang@ieee.org

Abstract. In this paper, we investigate the stop-and-go clock-controlled generator based on FCSR. The output sequence is proven to have large linear complexity. Further, the experimental results show that most of the output sequences also have almost optimal 2-adic complexity.

Keywords: FCSR, clock-controlled sequence, linear complexity, 2-adic complexity.

1 Introduction

Linear feedback shift registers (LFSR) have been widely used in keystream generators as basic building blocks because of their good statistical properties and the easy implementation. But LFSR cannot be used directly due to the well-known Berlekamp-Massey algorithm [11], which can easily recovers an LFSR if it has low linear complexity.

One general technique for destroying the low linear complexity inherent in LFSR is by combining the output of several LFSR in nonlinear ways, such as nonlinear combination generators, nonlinear filter generators and clock-controlled generators [12,13]. In the first two generators, all the component LFSR are clocked regularly. Whereas in the clock-controlled generator, the outputs of some LFSR control the clocking of other LFSR, which can resist the attacks based on the regular motion of LFSR [5]. The stop-and-go generator is the simplest clock-controlled generator with many good properties, such as easy hardware implementation and large linear complexity etc.

In 1994, Klapper and Goresky proposed a new type of feedback register called Feedback with Carry Shift Register (FCSR) [8]. An FCSR is a feedback shift register together with a small amount of auxiliary memory. It turns out that sequences generated by an FCSR share many of the important properties enjoyed by LFSR sequences. In general, FCSR sequences have larger linear complexity. But they are vulnerable to another kind of measure: the 2-adic complexity [4]. Hence, FCSR cannot be used directly in keystream generators as well.

* This work was supported by the Foundation for the Author of National Excellent Doctoral Dissertation of PR China (FANEDD) under Grants 200341.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 229–239, 2010.

In 2005, Arnault *et al.* firstly proposed a linear filter generator based on FCSR with Galois representation [1]. As a result, a hardware implementation called F-FCSR-Hv2 passed all the evaluations and then was chosen as one of the four candidates in the final phase of eSTREAM [2]. But unfortunately, it was broken in 2008 [7]. Very recently, they presented a new generator using ring representation FCSR (i.e., F-FCSR-Hv3) which totally resist previous attacks [3]. To explore more possibilities of the application FSCR in keystream generators, the objective of this paper is to introduce the stop-and-go generator based on FCSR for generating sequences with large linear complexity, and breaking the 2-adic structure of FCSR. The output sequence is proven to have (1) large period; (2) half period complementary property; (3) and large linear complexity. In addition, it was shown to possess high 2-adic complexity by experimental results.

The remainder of this paper is organized as follows. Section 2 gives some definitions and results of FCSR sequence with half period complementary property and large linear complexity. Section 3 introduces the basic arrangement of the stop-and-go generator. Section 4 determines the period of the output sequences of the stop-and-go generator based on FCSR. Its linear complexity and 2-adic complexity are considered as well. Section 5 concludes the paper.

2 FCSR Sequence with Half Period Complementary Property and Its Linear Complexity

Let $\underline{a} = (a_0, a_1, a_2, \cdots)$ be a binary sequence. If there exist two integers $N > 0$ and $j \geq 0$ satisfy

$$a_i = a_{i+N}, \quad \text{for } i \geq j, \tag{1}$$

$\underline{a}$ is said to be *eventually periodic* with period N, and *periodic* if $j = 0$. The minimum N satisfying (1) is called *the least period*. Straightforwardly, if T is a period of the sequence $\underline{a}$ then $N|T$.

2.1 Linear Complexity

It is well-known that any periodic sequence can be generated by an LFSR. Let $\underline{a} = (a_0, a_1, a_2, \cdots)$ be a periodic binary sequence. Then, there must be a linear recursive relation such that

$$a_{n+k} = \bigoplus_{i=0}^{n-1} c_i a_{k+i}, \quad k = 0, 1, \cdots, \tag{2}$$

where $c_i \in \mathbb{F}_2$ and $\oplus$ denotes the addition modulo 2. The polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ is called the *characteristic polynomial* of $\underline{a}$.

Among all the characteristic polynomials of $\underline{a}$, the monic polynomial of the lowest degree is said to be the *minimal polynomial* of $\underline{a}$. If $f(x)$ is a characteristic polynomial of periodic sequence $\underline{a}$, then the minimal polynomial of $\underline{a}$, say $g(x)$, divides $f(x)$.

Definition 1. *The linear complexity of an infinite periodic binary sequence* $\underline{a}$*, denoted as* $L(\underline{a})$*, is defined by the degree of its minimal polynomial.*

In the following, we discuss the minimal polynomials and the periods of sequences in terms of the polynomial ring $\mathbb{F}_2[x]$.

Definition 2 ([10]). *Let* $f \in \mathbb{F}_2[x]$ *be a nonzero polynomial. If* $f(0) \neq 0$*, then the least positive integer* e *for which* $f(x)$ *divides* $x^e - 1$ *is called the order of* f *and denoted by* $\mathrm{ord}(f) = \mathrm{ord}(f(x))$*. If* $f(0) = 0$*, then* $f(x) = x^h g(x)$*, where* $h \in \mathbb{N}$ *and* $g \in \mathbb{F}_2[x]$ *with* $g(0) \neq 0$ *are uniquely determined;* $\mathrm{ord}(f)$ *is then defined to be* $\mathrm{ord}(g)$*.*

The order of the polynomial f is sometimes also called the *period* of f because of the following lemma.

Lemma 1 ([10]). *Let* $f(x) \in \mathbb{F}_2[x]$ *be the minimal polynomial of periodic sequence* $\underline{s}$ *and* N *is the least period of sequence* $\underline{s}$*, then* $N = \mathrm{ord}(f(x))$*.*

The order of a polynomial f can be characterized in the following lemmas depending on whether it is irreducible or not.

Lemma 2 ([10]). *Let* $f(x) \in \mathbb{F}_2[x]$ *be an irreducible polynomial of degree* m *and with* $f(0) \neq 0$*. Then* $\mathrm{ord}(f)$ *is equal to the order of any root of* f *in the multiplicative group* $\mathbb{F}_{2^m}^*$*.*

Lemma 3 ([10]). *Let* $f \in \mathbb{F}_2[x]$ *be a polynomial of positive degree and with* $f(0) \neq 0$*. Let* $f = f_1^{b_1} \cdots f_k^{b_k}$*, where* $b_1, \cdots, b_k \in \mathbb{N}$*, and* $f_1, \cdots, f_k$ *are distinct irreducible polynomials in* $\mathbb{F}_2[x]$*, be the canonical factorization of* f *in* $\mathbb{F}_2[x]$*. Then* $\mathrm{ord}(f) = 2^t e$*, where* t *is the smallest integer with* $2^t \geq \max\{b_1, \cdots, b_k\}$ *and* e *is the least common multiple of* $\mathrm{ord}(f_1), \cdots, \mathrm{ord}(f_k)$*.*

Finally, we conclude this section by directly stating the relation between the decomposition of a sequence $\underline{c}$ and the decomposition of its characteristic polynomial without proof for saving space.

Lemma 4. *Let* $f(x)$ *be a characteristic polynomial of sequence* $\underline{c} = (c_0, c_1, c_2, \cdots)$*. If* $f(x) = f_1(x) \cdot f_2(x) \cdots f_k(x)$ *where* $f_1(x), f_2(x), \cdots, f_k(x)$ *are pairwise relatively prime, then there exist sequences* $\underline{a}_1, \underline{a}_2, \cdots, \underline{a}_k$*, such that* $\underline{c} = \underline{a}_1 \oplus \underline{a}_2 \oplus \cdots \oplus \underline{a}_k$ *and* $f_i(x)$ *is a characteristic polynomial of sequence* $\underline{a}_i$*,* $1 \leq i \leq k$*.*

2.2 FCSR Sequence with Half Period Complementary Property

It was showed in [9] that every eventually periodic sequence is an FCSR sequence, and vise versa. An FCSR is a feedback shift register together with a small amount of auxiliary memory [6,8,9]. The structure of an r-stage FCSR is depicted in Figure 1, where $m_{n-1} \in \mathbb{Z}$, $a_i, q_j \in \{0, 1\}$, $n-r \leq i \leq n-1$, and $1 \leq j \leq r$. If the contents of the register at any given time $n-1$ are $(a_{n-1}, a_{n-2}, \cdots, a_{n-r+1}, a_{n-r})$ and the memory is m_{n-1}. Then the operation of the shift register at the n-th clock time is defined as follows:

1. Take an integer sum $\delta_n = \sum_{k=1}^{r} q_k a_{n-k} + m_{n-1}$;
2. Shift the contents one step to the right, while outputting the rightmost bit a_{n-r};
3. Put $a_n = \delta_n (\text{mod } 2)$ into the leftmost cell of the shift register;
4. Replace the memory integer m_n with $m_n = (\delta_n - a_n)/2$.

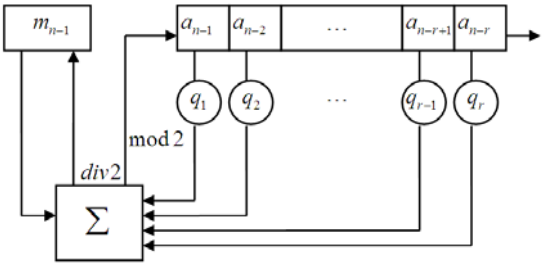


Fig. 1. Feedback with Carry Shift Register

The r taps $q_1, q_2, \cdots, q_r$ on the cells of an r-stage FCSR define *connection integer*

$$q = q_r 2^r + q_{r-1} 2^{r-1} + \cdots + q_1 2 - 1.$$

If a periodic sequence $\underline{a} = (a_0, a_1, a_2, \cdots)$ is generated by an FCSR with connection integer q. Then, there exists $A \in \mathbb{Z}_q$ such that for all $i = 0, 1, 2, \cdots$, $a_i = (A \cdot \gamma^i \,(\text{mod } q))(\text{mod } 2)$ where $\gamma = 2^{-1} \in \mathbb{Z}_q$. Obviously, $\underline{a}$ can achieve its maximum possible least period $N = q - 1$ if and only if the connection integer q is a prime and 2 is a primitive root modulo q. Such sequence $\underline{a}$ is called *l-sequence* [9], and its connection integer q is said to be a *2-prime*.

For simplicity, in this paper the connection integer q of FCSR is always assumed to be 2-prime. Thus, the FCSR sequence is an l-sequence with the least period $N = q - 1$.

Similarly to the run property of m-sequence, l-sequence also has good partial period distribution.

Lemma 5 ([9]). *Let $\underline{a} = (a_0, a_1, a_2, \cdots)$ be an l-sequence generated by an FCSR with connection integer q. If $2^n < q \leq 2^{n+1}$ is 2-prime, then every subsequence with length less than or equal to n can be found in $\underline{a}$.*

In addition, l-sequence has an interesting property called half period complementarity.

Definition 3. *Let $\underline{a} = (a_0, a_1, a_2, \cdots)$ be a periodic sequence with period N where N is an even integer. Then $\underline{a}$ is said to be half period complementary if*

$$a_i = a_{i+N/2} \oplus 1, \quad i \geq 0. \tag{3}$$

Lemma 6 ([9]). *Let $\underline{a} = (a_0, a_1, a_2, \cdots)$ be an l-sequence. Then $\underline{a}$ is half period complementary.*

If sequence $\underline{a}$ has half period complementary property, we have the following result concerning its characteristic polynomial.

Lemma 7 ([14]). *Let binary sequence $\underline{a}$ of period $N = 2r$ have half period complementary property, then*

$$f(x) = 1 + x + x^r + x^{r+1} = (1 + x)(1 + x^r)$$

is a characteristic polynomial of sequence $\underline{a}$.

2.3 Cyclotomic Polynomial

As shown in Lemma 7, we are able to determine the lower bound of minimal polynomial's degree of sequence $\underline{a}$ if we can factorize the polynomial $1 + x^r$. To do so, we need to introduce the cyclotomic polynomial.

Definition 4 ([10]). *Let m be a positive odd integer and ζ a primitive m-th root of unity over $\mathbb{F}_2$. Then the polynomial*

$$Q_m(x) = \prod_{s=1,\gcd(s,m)=1}^{m} (x - \zeta^s) \tag{4}$$

is called the m-th cyclotomic polynomial over $\mathbb{F}_2$.

According to the theory of cyclotomic polynomial [10],

$$1 + x^r = \prod_{m|r} Q_m(x). \tag{5}$$

Then, the characteristic polynomial $f(x)$ of sequence $\underline{a}$ can be rewritten as

$$f(x) = (1 + x)^2 \prod_{m|r, m\neq 1} Q_m(x).$$

Before further factorizing $f(x)$, we define the order of 2 modulo m.

Definition 5 ([10]). *If an integer d is the least positive integer such that $2^d \equiv 1 \pmod{m}$, then d is called the order of 2 modulo m, denoted as $d = \mathrm{ord}_m(2)$.*

Lemma 8 ([10]). *If m is a positive odd integer, then the m-th cyclotomic polynomial over $\mathbb{F}_2$ can be factorized as*

$$Q_m(x) = \prod_{i=1}^{\phi(m)/d} r_i(x)$$

where $r_i(x)$ is a monic irreducible polynomial of the same degree $d = \mathrm{ord}_m(2)$.

Obviously, $Q_m(x)$ is irreducible in $\mathbb{F}_2$ if and only if 2 is a primitive root modulo m, i.e. $\mathrm{ord}_m(2) = \phi(m)$. Applying Lemmas 2 and 3 to (4), we always have the following corollary.

Corollary 1. *The order of the m-th cyclotomic polynomial $Q_m(x)$ is m, i.e., $\mathrm{ord}(Q_m(x)) = m$.*

3 The Basic Arrangement of Stop-and-Go Generator

A stop-and-go generator consists of a controlling register CR and a generating register GR, see Figure 2. Let $\underline{a} = (a_0, a_1, a_2, \cdots)$ and $\underline{b} = (b_0, b_1, b_2, \cdots)$ be the CR sequence and GR sequence respectively. Let $\underline{u} = (u_0, u_1, u_2, \cdots)$ be the output sequence of the stop-and-go generator.

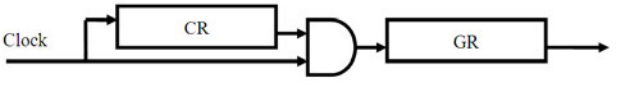


Fig. 2. Stop-and-Go Generator

The stop-and-go generator works as follows. After the output u_{t-1} has been taken from GR in the clock-controlled arrangement, the control register generates a binary member a_t, and then GR is stepped by a_t steps before producing the next output u_t. Finally, CR is stepped in regularly to produce the next value a_{t+1}. Mathematically,

$$u_t = b_{\sum_{k=0}^{t} a_k}, \quad \text{for } t \geq 0. \tag{6}$$

Considering that the least period of the sequence $\underline{a}$ is N_1, we rewrite (6) as

$$u_{i+jN_1} = b_{jS+\sigma(i)}, \quad 0 \leq i < N_1, \ j \geq 0, \tag{7}$$

where

$$\sigma(t) = \sum_{k=0}^{t} a_k, \tag{8}$$

and

$$S = \sum_{k=0}^{N_1-1} a_k. \tag{9}$$

The following lemmas describe some properties of the sequence $\underline{u}$.

Lemma 9 ([5]). *For the stop-and-go generator, the least period of the CR sequence $\underline{a}$ is N_1, and the least period of the GR sequence $\underline{b}$ is N_2. If S is relatively prime to N_2, where S is defined by (9), then the least period of clock-controlled sequence $\underline{u}$ is N_1N_2.*

Lemma 10. *Let sequences $\underline{a}$ and $\underline{b}$ respectively be sequences of the least period $N_1 = 2p_1$ and $N_2 = 2p_2$ with half period complementary property. If p_1 is relatively prime to $2p_2$, then the least period of sequence $\underline{u}$ is N_1N_2 and $\underline{u}$ also has half period complementary property.*

Proof. Since $\underline{a}$ is a sequence of the least period $N_1 = 2p_1$ with half period complementary property, one immediately has $S = p_1$. It follows from Lemma 9 that the least period of sequence $\underline{u}$ is $N_1N_2 = 4p_1p_2$.

Given an integer $t = i + jN_1 \geq 0$, $0 \leq i < N_1$ and $j \geq 0$. According to (7),

$$u_t = u_{i+jN_1} = b_{jp_1+\sigma(i)},$$
$$u_{t+2p_1p_2} = u_{i+jN_1+p_2N_1} = b_{jp_1+p_2p_1+\sigma(i)}.$$

Since the least period of $\underline{b}$ is $N_2 = 2p_2$ and $\gcd(p_1, 2p_2) = 1$, one has

$$b_{jp_1+p_2p_1+\sigma(i)} = b_{jp_1+\sigma(i)+p_2}$$

whereas, $b_{jp_1+\sigma(i)+p_2} = b_{jp_1+\sigma(i)} \oplus 1$ by the half period complementary property of $\underline{b}$, which indicates that $\underline{u}$ has half period complementary property. □

4 Stop-and-Go Generator Based on FCSR

The stop-and-go generator based on FCSR is depicted in Figure 3. Let the connection integers of FCSR1 and FCSR2 are $q_1 = 2p_1 + 1$ and $q_2 = 2p_2 + 1$, respectively. Throughout this section, q_1 and q_2 are always assumed to be *strong 2-prime* with $q_1 \neq q_2$.

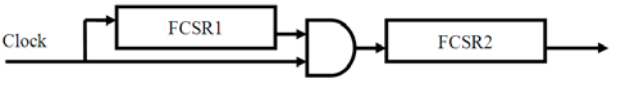


Fig. 3. Stop-and-Go Generator Based on FCSR

Definition 6 ([14]). *If $q(= 2p + 1)$ is a 2-prime and p is also 2-prime, then q is called strong 2-prime.*

Let $\underline{a}$ and $\underline{b}$ be the CR sequence and GR sequence, which are generated by FCSR1 and FCSR2, respectively. Let $\underline{u}$ be the output sequence of the stop-and-go generator. Since $q_1 = 2p_1 + 1$ and $q_2 = 2p_2 + 1$ are both strong 2-primes, $\underline{a}$ and $\underline{b}$ are l-sequences with least periods $2p_1$ and $2p_2$, respectively.

4.1 Period

Theorem 1. *Let $\underline{u}$ be the stop-and-go clock-controlled sequence generated by Figure 3, then $\underline{u}$ is a half period complementary sequence with the least period $4p_1p_2$.*

Proof. By Lemma 6, the two l-sequences $\underline{a}$ and $\underline{b}$ have half period complementary property. Then, the conclusions immediately follow from Lemmas 9 and 10. □

4.2 Linear Complexity

Theorem 2. *Let $\underline{u}$ be the stop-and-go clock-controlled sequence generated by Figure 3, then*

$$L(\underline{u}) \geq \mathrm{lcm}(p_1 - 1, p_2 - 1) + 3.$$

Proof. According to Lemma 7 and (5), $\underline{u}$ can be generated by the following polynomial

$$\begin{aligned} f(x) &= (1+x)(1+x^{p_1p_2})^2 = (1+x)(\textstyle\prod_{d|p_1p_2} Q_d(x))^2 \\ &= (1+x)^3 Q_{p_1}^2(x) Q_{p_2}^2(x) Q_{p_1p_2}^2(x), \end{aligned}$$

where $Q_{p_1p_2}(x) = \prod_{i=1}^{\phi(p_1p_2)/m} r_i(x)$ with $r_i(x)$s are monic irreducible polynomials of degree $m = \mathrm{ord}_{p_1p_2}(2)$ by Lemma 8. Since p_1 and p_2 are 2-primes with $p_1 \neq p_2$, one has $m = \mathrm{lcm}(p_1 - 1, p_2 - 1)$ from the Chinese Remainder Theorem.

Let $g(x)$ be the minimal polynomial of sequence $\underline{u}$, then $g(x)|f(x)$. In the sequel, we will prove that $g(x)$ is divisible by $(1+x)^3 r_i(x)$ for some i in two steps.

(I) $(1+x)^3 | g(x)$.

If $(1+x)^3$ is not a divisor of $g(x)$, then $\mathrm{ord}(g) \leq 2p_1p_2$ by Lemma 3 and Corollary 1. Applying Lemma 1, one has the period of $\underline{u}$ is equal to $\mathrm{ord}(g) \leq 2p_1p_2$, a contradiction.

(II) $r_i(x)|g(x)$ for some i.

If $r_i(x)$ is not a divisor of $g(x)$, for any $1 \leq i \leq \phi(p_1p_2)/m$, then $g(x)$ is of the form

$$g(x) = (1+x)^3 \cdot Q_{p_1}^i(x) \cdot Q_{p_2}^j(x), \qquad 1 \leq i, j \leq 2, \tag{10}$$

in which $i \neq 0$ and $j \neq 0$. Otherwise, one has $\mathrm{ord}(g) \leq 4p_2$ (resp. $\mathrm{ord}(g) \leq 4p_1$) from Lemma 3.

By Lemma 4, the sequence $\underline{u}$ can be decomposed as

$$\underline{u} = \underline{\alpha} \oplus \underline{\beta} \oplus \underline{\gamma}, \tag{11}$$

where $\underline{\alpha}$ is generated by $Q_{p_1}^i(x)$ with period ip_1, $\underline{\beta}$ is generated by $Q_{p_2}^j(x)$ with period jp_2, and $\underline{\gamma}$ is generated by $(1+x)^3$ with period 4 and satisfies the following rules

- $\gamma_{t+3} = \gamma_t \oplus \gamma_{t+1} \oplus \gamma_{t+2}$, for all $t \geq 0$, since $(1+x)^3$ is the minimal polynomial of $\underline{\gamma}$;
- $\gamma_{t+2} = \gamma_t \oplus 1$, for all $t \geq 0$, since $\underline{u}$ has half period complementary property and

$$\begin{aligned} u_t \oplus u_{t+2p_1p_2} &= \alpha_t \oplus \beta_t \oplus \gamma_t \oplus \alpha_{t+2p_1p_2} \oplus \beta_{t+2p_1p_2} \oplus \gamma_{t+2p_1p_2} \\ &= \alpha_t \oplus \beta_t \oplus \gamma_t \oplus \alpha_t \oplus \beta_t \oplus \gamma_{t+2} \\ &= \gamma_t \oplus \gamma_{t+2}. \end{aligned}$$

Since q_1 is a strong 2-prime, one has $q_1 \geq 7$. According to Lemma 5, sequence $\underline{a}$ must contain the subsequence "00", i.e. there exists an integer $k \geq 0$ such that $a_{k+1} = a_{k+2} = 0$. Subsisting them into (8), we have $\sigma(k) = \sigma(k+1) = \sigma(k+2)$. It then follows from (7) that $u_{t\cdot 2p_1+k} = u_{t\cdot 2p_1+k+1} = u_{t\cdot 2p_1+k+2}$, for all $t \geq 0$.

By means of (11), $u_{t\cdot 2p_1+k}$ and $u_{t\cdot 2p_1+k+1}$ can be expressed as

$$\begin{aligned} u_{t\cdot 2p_1+k} &= \alpha_{t\cdot 2p_1+k} \oplus \beta_{t\cdot 2p_1+k} \oplus \gamma_{t\cdot 2p_1+k} \\ &= \alpha_k \oplus \beta_{t\cdot 2p_1+k} \oplus \gamma_{t\cdot 2p_1+k}, \\ u_{t\cdot 2p_1+k+1} &= \alpha_{t\cdot 2p_1+k+1} \oplus \beta_{t\cdot 2p_1+k+1} \oplus \gamma_{t\cdot 2p_1+k+1} \\ &= \alpha_{k+1} \oplus \beta_{t\cdot 2p_1+k+1} \oplus \gamma_{t\cdot 2p_1+k+1}. \end{aligned}$$

Then, we can get

$$\beta_{t\cdot 2p_1+k} \oplus \beta_{t\cdot 2p_1+k+1} = \alpha_k \oplus \alpha_{k+1} \oplus \gamma_{t\cdot 2p_1+k} \oplus \gamma_{t\cdot 2p_1+k+1}.$$

Further from the property of $\underline{\gamma}$ derived above, we have

$$\gamma_{(t+1)\cdot 2p_1+k} \oplus \gamma_{(t+1)\cdot 2p_1+k+1} = \gamma_{t\cdot 2p_1+k+2} \oplus \gamma_{t\cdot 2p_1+k+3} = \gamma_{t\cdot 2p_1+k} \oplus \gamma_{t\cdot 2p_1+k+1},$$

Hence,

$$\beta_{(t+1)\cdot 2p_1+k} \oplus \beta_{(t+1)\cdot 2p_1+k+1} = \beta_{t\cdot 2p_1+k} \oplus \beta_{t\cdot 2p_1+k+1}. \tag{12}$$

By the same argument on $u_{t\cdot 2p_1+k+1} = u_{t\cdot 2p_1+k+2}$, we have

$$\beta_{(t+1)\cdot 2p_1+k+1} \oplus \beta_{(t+1)\cdot 2p_1+k+2} = \beta_{t\cdot 2p_1+k+1} \oplus \beta_{t\cdot 2p_1+k+2}. \tag{13}$$

Since $\gcd(p_2, p_1) = 1$, $\{t \cdot 2p_1\}$ and $\{t \cdot 2p_1 + 1\}$ enumerate all the even values and all odd values from 0 to $2p_2 - 1$ respectively by mode $2p_2$ when t ranges from 0 to $p_2 - 1$. Then, (12) and (13) give that for all $0 \leq t < p_2$,

$$\begin{aligned} \beta_{2t+k} \oplus \beta_{2t+k+1} &= \beta_{2t+k+2} \oplus \beta_{2t+k+3}, \\ \beta_{2t+k+1} \oplus \beta_{2t+k+2} &= \beta_{2t+k+3} \oplus \beta_{2t+k+4}, \end{aligned}$$

which result in $\beta_{2t+k} = \beta_{2t+k+4}$ and $\beta_{2t+k+1} = \beta_{2t+k+5}$ for all $0 \leq t < p_2$. That is, the period of $\underline{\beta}$ is 4, which contradicts the assumption.

Combining (I) and (II), we conclude that $g(x)$ is divisible by $(1+x)^3 r_i(x)$ for some $1 \leq i \leq \phi(p_1 p_2)/m$. Then,

$$L(\underline{u}) = \deg(g(x)) \geq m + 3 = \mathrm{lcm}(p_1 - 1, p_2 - 1) + 3. \qquad \square$$

When we choose $\gcd(p_1 - 1, p_2 - 2) = 2$, the lower bound of linear complexity is $(p_1 - 1)(p_2 - 1)/2 + 3$. The ratio of the lower bound to the length of sequence is approximately equal to 1/8. While in the stop-and-go generator based on LFSR, the ratio is $n/(2^n - 1)$ where n is the stage of the component LFSR [5]. So in terms of this ratio, clocked-control generator based on FCSR is much better than that based on LFSR.

4.3 2-Adic Complexity

Definition 7 ([9]). *Let $\underline{a}$ be binary periodic sequence, and q is the least connection integer of $\underline{a}$, then, the 2-adic complexity of $\underline{a}$ is defined as $log_2(q)$.*

Theorem 3. *Let $\underline{a}$ be binary periodic sequence with half period complementary property, $2n$ be the period of $\underline{a}$, q be the least connection integer of $\underline{a}$. Then, we have $q \leq (2^n + 1)$.*

Proof. The conclusion is obvious since the sequence $\underline{a}$ can be generated by an FCSR with the connection integer $q = 2^n + 1$ and initial states $(a_t, a_{t+1}, \cdots, a_{t+n-1})$. □

To test the 2-adic complexity of our clock-controlled FCSR sequences, firstly we generated l-sequence with prime connection integer $10 < q < 1200$. Secondly choosing two of them, we generated all the stop-and-go sequences with length less than 12000, and calculate their 2-adic complexities. The ratios of 2-adic complexity to the period of the sequence are shown in Figure 4. By Theorem 3, the ration should be not more than $\frac{\log_2(2^n+1)}{2n} \approx 0.5$. So, we see that most of the sequences achieve almost the optimal 2-adic complexity, i.e., $q \approx 2^n + 1$.

Based on the experimental results, we expect that clock-controlled FSCR sequence can resist 2-adic analysis because clock-controlled structure destroys the algebra structure over the 2-adic numbers.

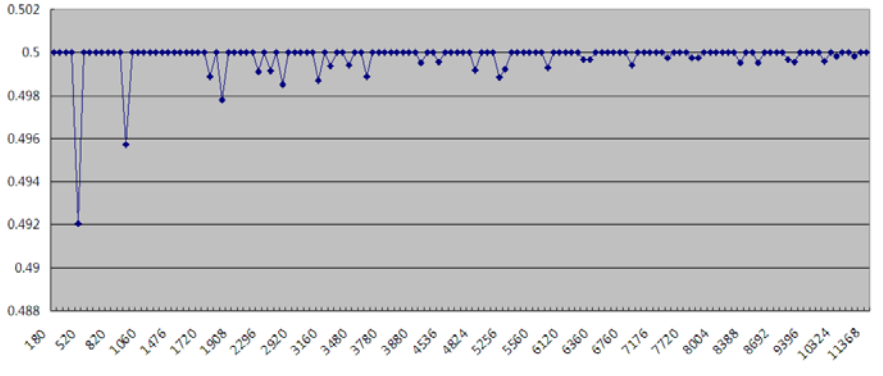


Fig. 4. Ratio of 2-adic Complexity to Period

5 Conclusions

In this paper, we introduce the stop-and-go generator based on FCSR. For the FCSR with connection integer being strong 2-prime, we determine the period of the ouput sequence. The linear complexity and the 2-adic complexity are also considered. The experimental results show that most of the output sequences also have almost the optimal 2-adic complexity. Thus we believe that the clock-controlled FSCR sequences can resist 2-adic analysis.

References

1. Arnault, F., Berger, T.P.: F-FCSR: Design of a new class of stream ciphers. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 83–97. Springer, Heidelberg (2005)
2. Arnault, F., Berger, T.P., Lauradoux, C.: Update on F-FCSR stream cipher. In: ECRYPT - Network of Excellence in Cryptology (Call for stream Cipher Primitives - Phase 2 2006) (2006), http://www.ecrypt.eu.org/stream/
3. Arnault, F., Berger, T.P., Lauradoux, C., Minier, M., Pousse, B.: A new approach for FCSRs. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 433–448. Springer, Heidelberg (2009)
4. De Weger, B.M.M.: Approximation lattices of p-adic numbers. Journal of Number Theory 24, 70–88 (1986)
5. Gollmann, D., Chambers, W.G.: Clock-controlled shift registers: a review. IEEE Journal on Selected Areas in Communications 7(4), 525–533 (1989)
6. Goresky, M., Kalapper, A.: Feedback register based on ramified extensions of the 2-adic number. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 215–222. Springer, Heidelberg (1995)
7. Hell, M., Johansson, T.: Breaking the F-FCSR-H stream cipher in real time. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 557–569. Springer, Heidelberg (2008)
8. Klapper, A., Goresky, M.: 2-adic shift register. In: Fast Software Encryption 2nd International Workshop. LNCS, vol. 809, pp. 174–178. Springer, Berlin (1994)
9. Klapper, A., Goresky, M.: Feedback shift registers, 2-adic span and combiners with memory. Journal of Cryptology 10(2), 111–147 (1997)
10. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge Univ. Press, Cambridge (1986)
11. Massey, J.L.: Shift-register synthesis and BCH decoding. IEEE Transactions on Information Theory 15(1), 122–127 (1969)
12. Rueppel, R.: Anaysis and design of stream ciphers. Springer, Heidelberg (1986)
13. Rueppel, R., Staffelbach, O.: Products of linear recurring sequences with maximum complexity. IEEE Transactions on Information Theory 33(1), 124–131 (1987)
14. Seo, C., Lee, S., Sung, Y., Han, K., Kim, S.: A lower bound on the linear span of FCSR. IEEE Transactions on Information Theory 46(2), 691–693 (2000)

Vectorial Conception of FCSR

Abdelaziz Marjane[1] and Boufeldja Allailou[2]

[1] LAGA, UMR CNRS 7539, Université Paris 13, Villetaneuse, France
marjane@math.univ-paris13.fr
[2] LAGA, UMR CNRS 7539, Université Paris 8, Saint-Denis, France
allailou@math.univ-paris13.fr

Abstract. In this paper, we investigate the structure of FCSR made by Goresky and Klapper. Using a vectorial construction of the objects and of the register, we extend the analysis of FCSRs. We call these registers vectorial FCSRs or VFCSRs. We obtain similar results to those of analysis of FCSRs and of d-FCSRs generating binary sequences or p-ary sequences. In fact, the AFSRs built over finite fields $\mathbb{F}_{p^n}$ with $n \geq 2$ suffer from an very difficult and formal analysis. But if you analyze these registers with a vectorial structure, you can decompose the output sequence into a vector of binary sequences or p-ary sequences. This method allows us to obtain very easily the period, the behavior of memory with interval optimized , the maximal period, the existence of l-sequences and the calculations become explicit and easily implementable. At the end of this paper, we implement the quadratic case ($\mathbb{F}_{2^2}$ case) and present the conclusions about pseudorandom properties of quadratic l-sequences which are tested by NIST STS package. In conclusion, VFCSRs are easy to implement in software and hardware and have excellent pseudorandomn property.

1 Introduction

In 1993, Goresky and Klapper ([1] and [2]) have introduced a new sequences generator named FCSR. They have developped many results about FCSR sequences over $\mathbb{F}_2$. With the correspondence between rational numbers and eventually periodic binary sequences, they prove that the output sequence $(a_i)_i$ is periodic and its 2-adic development $\sum_{i=0}^{i=+\infty} a_i 2^i$ corresponds to a rational number $\frac{p}{q} \in \mathbb{Q}$ where $q = \sum_{i=1}^{i=r} q_i 2^i - 1$ is an odd positive integer called the connection integer and q_i are connection coefficients (see Fig. 2). Suppose that $\frac{p}{q}$ is irreducible, then the period of the sequence is $ord_q(2)$. The output sequence has an exponential representation, $a_i = (A2^{-i}) \pmod q \pmod 2$ for all i. The period is maximal if q is prime which 2 is a primitive root modulo q. A sequence of such period is called an l-sequence. These sequences verify distributional properties very good like the balance property. Furthermore, they give a rational approximation algorithm similar to Berlekamp-Massey algorithm. Finally, the arithmetic cross correlation between two first decimations of an l-sequence is either zero or equal to the period. In 1994, Klapper [3] has extended these FCSRs to any

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 240–252, 2010.

finite field. In order to construct FCSR over a finite field, he takes a principal domain R with valuation such that the ideal of the valuation πR generated by π is maximal and $R/\pi R$ is a finite field. He corresponds the output sequence $(a_i)_i$ with its π-adic development $\sum_{i=0}^{i=+\infty} a_i \pi^i$ in the completion R_π of R at the valuation. For example, to obtain $\mathbb{F}_{2^n}$, he takes $R = \mathbb{Z}[\beta]$ and $\pi = 2$ where $2R$ is a prime ideal and the reduction of β modulo 2 is a root of a primitive polynomial of degree n over $\mathbb{F}_2$(note that in this general case R is not necessarily a principal domain but just an order of a Dedekind domain). Then we have $\mathbb{Z}[\beta]/(2) = \mathbb{F}_{2^n}$. Klapper analyzes these FCSRs and shows that the 2-adic development is equal to $\frac{p}{q}$ which is a rational in $\mathbb{Q}(\beta)$ the fraction field of $\mathbb{Z}[\beta]$. q is always the connection integer. In this general setting the analyzis of these registers is more difficult. To conclude his work, Klapper give an algorithm to answer the inverse question which is how to construct the initial loading of an FCSR over $\mathbb{F}_{2^n}$ whose output sequence coincides with the 2-adic expansion of $\frac{p}{q}$? Finally in [3] Klapper generalizes the 2-adic rational approximation algorithm with very restrictive conditions. In the same year, Goresky and Klapper [4] have introduced a new design of FCSR called d-FCSR based on totally ramified extensions of $\mathbb{Z}_2$ of degree d. To construct d-FCSR, they take $R = \mathbb{Z}[\sqrt[d]{2}]$ an order of a Dedekind domain and $\pi = \sqrt[d]{2}$. The output sequence corresponds to the π-adic expansion of $\frac{p}{q} \in \mathbb{Q}(\sqrt[d]{2})$ where $q = \sum_{i=1}^{i=r} q_i \pi^i - 1 \in \mathbb{Z}[\sqrt[d]{2}]$. Furthermore they give the exponential representation of d-FCSR which is $a_i = A \sqrt[d]{2}^{-i} \pmod{q} \pmod{\sqrt[d]{2}}$. So the maximal period is $T = |R/(q) - 0|$ and they define l-sequences for d-FCSRs. In 2002 [5], they present many results about periodicity and correlation of d-FCSR. We consider mainly that they use the norm of q and obtain $\frac{p}{q} \in \frac{1}{N(q)}\mathbb{Z}[\sqrt[d]{2}]$. This fact is very important because $N(q)$ is in $\mathbb{Q}$ and thus simplifies the analysis. The maximal period becomes $N(q) - 1$. We emphasize that it's very important because using the norm, we can analyze these registers over integer and not over elements in $\mathbb{Z}[\pi]$. We use this norm in this paper in order to reduce computations on abstract algebraic structures to computations on vectorial structures over $\mathbb{Z}$. In 1999, Klapper and Xu [6] have presented a generalization of FCSR and LFSR called AFSR. Algebraic FSR are constructed over an integral and commutative ring R and they consider an element $\pi \in R$. We assume that $R/\pi R$ is a finite field. The construction is the same as that of FCSR. Also, if we take $R = \mathbb{F}_{2^n}[x]$ and $\pi = x$ where x is an indeterminate, we obtain an LFSR. As far as, if we take $R = \mathbb{Z}$ and $\pi = p$ with p prime, you have simple FCSR. If we take $R = \mathbb{Z}[\sqrt[d]{2}]$ and $\pi = \sqrt[d]{2}$, we have the case of d-FCSR. This construction generalizes all FSR over an algebraic structure. Any such π defines a topology on R. For analysis, they consider the completion of R for the π-adic topology. If R is noetherian, this completion is simply the set of power series $\sum_{i=0}^{i=+\infty} a_i \pi^i$. For analysis, we have a correspondance between this set of power series and the set of sequences over $R/\pi R$. Furthermore, the most important results are that the output sequence is the π-adic expansion of $\frac{p}{q}$ which is in the fraction field of R and $q = \sum_{i=1}^{i=r} q_i \pi^i - 1$ is the connection integer. Under special conditions, the output sequence has an exponential representation

modulo q modulo π. Moreover, in this case, the period is the order of π modulo q. Finally, they give a rational approximation algorithm for AFSR using the norm of q and an interleaving of several sequences over subrings. Goresky, Klapper and Xu use only these concepts for d-FCSR and for rational approximation algorithm to AFSR. All these results about algebraic FSR and their properties are described in an excellent book [7]. However in this paper, we repeat and develop this analysis of FCSR over finite fields $\mathbb{F}_{2^n}$ with $n \geq 2$ but through a vectorial contruction that produces results much more significant as the determination of the period, the behavior of memory, the existence of l-sequences, the implementation, the properties of distribution etc... Furthermore we consider the output sequences as vectors of binary sequences or p-ary sequences, and thus we obtain results as strong as those Goresky and Klapper get to the FCSR and d-FCSR since generally AFSRs have an underlying algebraic structure difficult to analyze. So we present a new design called vectorial FCSR. We develop especially the quadratic case.

2 Definitions and Analysis

2.1 Formalism

We keep the scheme of the FCSR built by Goresky and Klapper. However, we must redefine the space in which we calculate. The field $\mathbb{F}_{2^n}$ can be seen as a vector space over $\mathbb{F}_2$ of dimension n. Indeed, we can take an irreducible polynomial P over $\mathbb{F}_2$ and we construct $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$. First, we must choose an arbitrary irreducible polynomial. This polynomial defines the operations of the register. Secondly, to describe our calculations in a vectorial way to implement them, you have to put an arbitrary basis. We choose the canonical basis $\mathcal{B} = \left\{1, \bar{X}, \ldots, \bar{X}^{n-1}\right\}$ where $\overline{X}$ is the class of X in $\mathbb{F}_2[X]/(P)$. Then we take a lift of P in $\mathbb{Z}[X]$, in this case P itself because it is irreducible in $\mathbb{Z}[X]$, and we obtain the ring $\mathbb{Z}[X]/(P)$ which is a free $\mathbb{Z}$-module of rank n. With these notations, we define the vectorial FCSR.

Definition 1. *A vectorial feedback with carry shift register over* $(\mathbb{F}_2, P, \mathcal{B})$ *of length* r *with coefficient* $q_1, \ldots, q_r \in \mathbb{F}_2[X]/(P)$ *is an automaton or sequence generator whose state is an element* $s = (a_0, \ldots, a_{r-1}, m_{r-1})$ *where* $a_i \in \mathbb{F}_2[X]/(P)$ *and* $m_{r-1} \in \mathbb{Z}[X]/(P)$. *We take the canonical lift of the collection of* a_i *and* q_i *in* $\mathbb{Z}[X]/(P)$ *and compute the element* $\sigma_r = \sum_{i=1}^{i=r} q_i a_{r-i} + m_{r-1}$ *and* $a_r = \sigma_r \pmod 2$ *where* $\pmod 2$ *applies coordinates by coordinates following the basis* $\mathcal{B}$. *Take the canonical lift of* a_r *in* $\mathbb{Z}[X]/(P)$ *and compute* $m_r = \frac{\sigma_r - a_r}{2}$. *The feedback function is* $f(s) = (a_1, \ldots, a_{r-1}, a_r, m_r)$ *and the output function is* $g(x_0, x_1, \ldots, x_{r-1}, z) = x_0$. *The FCSR generates an infinite output sequence* $\underline{a} = (g(s), g(f(s)), g(f^2(s)), \ldots) = (a_0, a_1, a_2, \ldots)$. s *is called initial state,* $q_1, \ldots, q_r$ *are called the coefficients of the recurrence and the infinite sequence* $(m_{r-1}, m_r, \ldots)$ *is called memory values.*

2.2 Calculus over $(\mathbb{F}_2, P, \mathcal{B})$

We write all elements in the basis $\mathcal{B}$.

$$\begin{array}{l} i \in \mathbb{N},\ a_i = \sum\limits_{j=0}^{j=n-1} a_j^i \bar{X}^j;\ a_j^i \in \mathbb{F}_2,\ \ 1 \le i \le r,\ q_i = \sum\limits_{j=0}^{j=n-1} q_j^i \bar{X}^j;\ q_j^i \in \mathbb{F}_2, \\ i \ge r-1,\ m_i = \sum\limits_{j=0}^{j=n-1} m_j^i \bar{X}^j;\ m_j^i \in \mathbb{Z} \ \text{ and } \ i \ge r,\ \sigma_i = \sum\limits_{j=0}^{j=n-1} \sigma_j^i \bar{X}^j;\ \sigma_j^i \in \mathbb{Z}. \end{array} \tag{1}$$

In calculating σ, we find a polynomial expression in $\bar{X}$ of degree $2n-2$ thus we must eliminate the degree greater than $n-1$ to obtain the coordinates for σ in the basis $\mathcal{B}$. For this, we must express the power of $\bar{X}$ in terms of $\mathcal{B}$ with the polynomial P. So we set

$$j \ge n, \quad \bar{X}^j = \sum_{t=0}^{t=n-1} b_t^j \bar{X}^t\ ;\ b_t^j \in \mathbb{F}_2.$$

We get the coordinates of σ and of the output sequence in the basis $\mathcal{B}$, $z \ge r$,

$$\sigma_z = \sum_{t=0}^{t=n-1} \Big[\sum_{k=0}^{k=t} \sum_{i=1}^{i=r} (q_k^i a_{t-k}^{z-i}) + \sum_{j=n}^{j=2n-2} (b_t^j \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} (q_k^i a_{j-k}^{z-i})) + m_t^{z-1} \Big] \bar{X}^t$$

$$a_t^z = \Big[\sum_{k=0}^{k=t} \sum_{i=1}^{i=r} (q_k^i a_{t-k}^{z-i}) + \sum_{j=n}^{j=2n-2} (b_t^j \sum_{k=j-n+1}^{k=n-1} \sum_{i=1}^{i=r} (q_k^i a_{j-k}^{z-i})) + m_t^{z-1} \Big] \pmod 2 \tag{2}$$

2.3 Analysis of VFCSRs over $(\mathbb{F}_2, P, \mathcal{B})$

The output sequence corresponds to n binary sequences.

$$\underline{a} = (a_i)_{i \in \mathbb{N}} = \sum_{j=0}^{j=n-1} (a_j^i)_{i \in \mathbb{N}} \bar{X}^j = \sum_{j=0}^{j=n-1} \underline{a}_j \bar{X}^j \tag{3}$$

Following Goresky and Klapper's correspondance, to each $\underline{a}_j$, we associate its 2-adic development and we obtain a 2-adic vector $\beta = (\beta_t)_{t=0}^{t=n-1}$ associated to $\underline{a}$

$$\begin{array}{l} {\mathbb{F}_2}^{\mathbb{N}} \to {\mathbb{Z}_2}^n \\ \quad \underline{a} \mapsto \Big(\sum\limits_{z \in \mathbb{N}} a_t^z 2^z \Big)_{t=0}^{t=n-1}. \end{array} \tag{4}$$

Definition 2. *We set* $\tilde{q}_i = \sum\limits_{j=1}^{j=r} q_i^j 2^j$ *for all* $0 \le i \le n-1$ *and we call* $(\tilde{q}_i)_{0 \le i \le n-1}$ *the connection vector for the VFCSR over* $(\mathbb{F}_2, P, \mathcal{B})$.

Using 2, we obtain a linear system with integer coefficients

$$\left\{ \beta_t - \sum_{j=n}^{j=2n-2} \sum_{k+l=j}^{0\leq k,l\leq n-1} (b_t^j \tilde{q}_k \beta_l) - \sum_{k+l=t} \tilde{q}_k \beta_l = \tilde{p}_t \right\}_{t=0}^{t=n-1}$$

where we leave to the readers to determine the expression of $\tilde{p}_t$. This system can be written in matrix form with a matrix whose diagonal is odd and the other entries are even. So this matrix denoted M and called *the connection matrix of the VFCSR over* $(\mathbb{F}_2, P, \mathcal{B})$ is invertible, its determinant is odd and we have (Comat is the comatrice)

$$\beta = \frac{1}{|\det(M)|} \mathtt{sgn}(\det M) \mathtt{Comat}(M)(\tilde{p}_t)_{0\leq t\leq n-1} \tag{5}$$

Theorem 1. *Consider a VFCSR over* $(\mathbb{F}_2, P, \mathcal{B})$ *of length* r *with connection vector* $(\tilde{q}_0, \ldots, \tilde{q}_{n-1})$ *and connection matrix* M*. For all sequences* $\underline{a}$ *generated by this VFCSR, the associated 2-adic vector* β *is in* $\frac{1}{|\det M|}\mathbb{Z}^n$ *and* $|\det M|$ *is positive and odd.*

Notice that to generate a sequence with VFCSR returns to generate n binary sequences with the same FCSR over $\mathbb{F}_2$ whose connection integer is $|\det M|$ and therefore a size much larger than the VFCSR (see Table 4).

2.4 Norm and Analysis with Respect to an Another Basis

The norm $N(x)$ of an element x in $\mathbb{Q}[X]/(P)$ is the determinant of the linear transformation defined as the multiplication by x. We have a special element $q = \sum_{i=1}^{i=r} q_i 2^i - 1 \in \mathbb{Z}[X]/(P)$ and $N(q) \in \mathbb{Z}$.

Proposition 1. *The connection matrix* M *is the matrix in the canonical basis* $\mathcal{B}$ *of the linear transformation defined as the multiplication by* $-q$*. The determinant of* M *is the norm of* $-q$*.*

Whatever the basis chosen for $\mathbb{Q}[X]/(P)$, the norm does not change, because we replace M by an equivalent matrix. If we construct and analyze the VFCSR over an another basis $\mathcal{B}'$, we obtain the same results with respect to $\mathcal{B}'$: all sequences generated by this VFCSR on $(\mathbb{F}_2, P, \mathcal{B}')$ are associated to a 2-adic vector in $\frac{1}{N(q)}\mathbb{Z}$. So *we can define FCSR over finite fields on the pair* $(\mathbb{F}_2, P)$ *and we call* q *the connection integer of the FCSR* and we have $q = (\tilde{q}_0, \ldots, \tilde{q}_{n-1}) - (1, 0, ..., 0)$ in the basis $\mathcal{B}$.

2.5 Periodicity and *l*-Sequences

In this section, $\mathcal{B}$ is not necessarily the canonical basis. Also we consider the equations 1, 2, 3, 4 and 5 with respect to $\mathcal{B}$.

Proposition 2. *The sequence* $\underline{a}$ *is periodic if and only if* $\underline{a}_j$ *is periodic for all* $0 \leq j \leq n-1$. *The period of* $\underline{a}$ *is the lcm of the periods of* $\underline{a}_j$ *where* $0 \leq j \leq n-1$.

According to the theory of 2-adic number, $\underline{a}$ is periodic if and only if $\beta \in \mathbb{Q}^n$. Hence the following corollary:

Corollary 1. *All sequences generated by vectorial FCSR over* $(\mathbb{F}_2, P, \mathcal{B})$ *are eventually periodic. The output sequence is periodic if and only if* $-1 \leq \beta_t \leq 0$ *for all* $0 \leq t \leq n-1$.

Proposition 3. *Let* $\beta = (\frac{\tilde{r}_t}{\tilde{q}})_{t=0}^{t=n-1}$ *be the vector associated to the output sequence* $\underline{a}$ *of the VFCSR. If exists* t *such that* $\tilde{r}_t \notin \tilde{q}\mathbb{Z}$, *then*

$$\mathtt{per}(\underline{a}) = \mathtt{lcm}_{0 \leq t \leq n-1} \left\{ \mathtt{ord}_{\frac{\tilde{q}}{\gcd(\tilde{q}, \tilde{r}_t)}}(2); \tilde{r}_t \notin \tilde{q}\mathbb{Z} \right\}$$

otherwise $\mathtt{per}(\underline{a}) = 1$.

Here $\tilde{q} = |\det(M)| = |N(q)|$. The period is always less than $\tilde{q} - 1$. This upper limit is reached if $\tilde{q}$ is a prime number whose 2 is a primitive root modulo $\tilde{q}$ and if there exists a numerator that is not a multiple of $\tilde{q}$. $\tilde{q}$ being plus or minus the determinant of the connection matrix, so it is an integer represented by an n-form. So we must look for such numbers, if they exist then we can extend the notion of l-sequences to VFCSR.

Definition 3. *Let a VFCSR with connection matrix* M. *Suppose that* $\tilde{q} = |\det M|$ *is prime and 2 is a primitive root modulo* $\tilde{q}$. *A nontrivial output sequence (ie not with period 1) is called vectorial* l*-sequence if the period is* $\tilde{q} - 1$.

We note that the maximal period of VFCSR sequences is $|N(q)| - 1$. So we can define l-sequence in another way: let an FCSR over a finite fields on $(\mathbb{F}_2, P)$. Suppose that q is the connection integer and $|N(q)|$ is prime with 2 a primitive root modulo $|N(q)|$. *A nontrivial output sequence (ie not with period 1) is called* l*-sequence over* $(\mathbb{F}_2, P)$ *if the period is* $|N(q)| - 1$. We note that each nontrivial binary sequence $\underline{a}_j$ of a vectorial l-sequence can be viewed as a binary l-sequence. So they check all the results of Goresky and Klapper on l-sequences such as distributional properties (balanced property, complementarity of the half periods...).

2.6 Vectorial Exponential Representation

In this section, $\mathcal{B}$ is not necessarily the canonical basis. We can reformulate the following theorem in a more intrinsic way by replacing $\det(M)$ by $N(q)$.

Theorem 2. *Let* $\underline{a}$ *be a sequence generated by a VFCSR over* $(\mathbb{F}_2, P, \mathcal{B})$ *of connection matrix* M. *Then there are integers* $(s_t)_{t=0}^{t=n-1}$ *such that*

$$\forall i \in \mathbb{N}, \quad a_i = \left(2^{-i} \sum_{t=0}^{t=n-1} (s_t \bar{X}^t)\right) \pmod{|\det M|} \pmod 2$$

2.7 Vectorial Memory Requirements

We place ourselves in the canonical basis $\mathcal{B}$, and we define $w_i = \sum_{j=1}^{j=r} q_i^j$ for all $0 \leq i \leq n-1$. Using 2, it also defines special constants

$$K_t = \sum_{k=0}^{k=t} w_k + \sum_{j=n}^{j=2n-2} b_t^j \sum_{k+l=j}^{0\leq k,l\leq n-1} w_k.$$

Proposition 4. *For $0 \leq i \leq n-1$, if $m_i^{r-1} \in [0, K_i[$, then the next memory remain in $[0, K_i[$. If $m_i^{r-1} = K_i$, then the next memory monotonically decreases to $[0, K_i[$ after at most r steps. If $m_i^{r-1} > K_i$, then the next memory monotonically decreases to $[0, K_i[$ after at most $[\log_2(m_i^{r-1} - K_i)] + r$ steps. If $m_i^{r-1} < 0$, then the next memory monotonically increases to $[0, K_i[$ after at most $[\log_2 |m_i^{r-1}|] + r + 1$ steps.*

For example, for VFCSR over $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$, we find $K_0 = w_0 + w_1$ and $K_1 = w_0 + 2w_1$. For VFCSR over $(\mathbb{F}_2, X^3 - X - 1, \mathcal{B})$, we have $K_0 = w_0 + w_1 + w_2$, $K_1 = w_0 + 2w_1 + 2w_2$ and $K_2 = w_0 + w_1 + 2w_2$. If we replace $\mathcal{B}$ by $\mathcal{B}' = \{\mu_0, \ldots, \mu_{n-1}\}$, there is a general method to determine the constants K_i' on this basis: we compute the vectorial coordinates of $\sum_{i=1}^{i=r} q_i(\mu_0 + \ldots + \mu_{n-1})$ on $\mathcal{B}'$.

$$\sum_{i=1}^{i=r} q_i(\mu_0 + \ldots + \mu_{n-1}) = K_0'\mu_0 + \ldots + K_{n-1}'\mu_{n-1}$$

2.8 Initial Loading

In this section, we answer the reverse question: Let $\beta = (\frac{\tilde{r}_0}{\tilde{s}_0}, \ldots, \frac{\tilde{r}_{n-1}}{\tilde{s}_{n-1}})$ a rational vector whose denominators are all odd, how do we determine a VFCSR and initial loading whose output sequence coincides with the 2-adic expansion vector of β. If a VFCSR generates β, it must be constructed over $(\mathbb{F}_2, P, \mathcal{B})$ with P an irreducible polynomial of degree n and $\mathcal{B}$ the canonical basis. Let start with an irreductible polynomial P of degree n. In other words, we seek an VFCSR over $(\mathbb{F}_2, P, \mathcal{B})$ size r with connection vector $(\tilde{q}_0, \ldots, \tilde{q}_{n-1})$ and an initial state $(a_0, \ldots, a_{r-1}, m_{r-1})$. All these unknowns satisfy an equation of the form 5. In order to solve this equation, use the following procedure:

1. Compute $\tilde{q} = \texttt{lcm}\{\tilde{s}_0, \ldots, \tilde{s}_{n-1}\}$ and now we have $\beta = (\frac{\tilde{r}_0}{\tilde{q}}, \ldots, \frac{\tilde{s}_{n-1}}{\tilde{q}})$.
2. $(\mathbb{F}_2, P, \mathcal{B})$ determines the form of the connection matrix M and so we have a n-form $\det M$ noted $f(\tilde{q}_0 - 1, \tilde{q}_1, \ldots, \tilde{q}_{n-1})$. We must solve the equation $f(\tilde{q}_0 - 1, \tilde{q}_1, \ldots, \tilde{q}_{n-1}) = \tilde{q}$ where connection vector (definition 2) is the unknown.
3. Compute $r = \max\{[\log_2(\tilde{q}_i)]; 0 \leq i \leq n-1\}$. Now we have the size of the VFCSR.
4. Write the 2-adic expansion vector of connection vector like definition 2 and we deduce connection coefficient $q_1, \ldots, q_r$.

5. Compute $a_i^0 + a_i^1 2 + \ldots + q_i^{r-1} 2^{r-1}$ the first r bits in the 2-adic expansion for $\frac{\tilde{r}_i}{\tilde{q}}$ (for all $0 \leq i \leq n-1$).
6. With all its data inputs into the equation 5, it remains to determine the memory. The memory m_t^{r-1} appears in 5 only in the expression of $\tilde{p}_t$ for all $0 \leq t \leq n-1$. It is an integral linear system $n \times n$ with n indeterminates.

2.9 First Cases

In this part we will present the first cases, $n = 1, 2, 3$. Firstly, if $n = 1$, it is an binary FCSR. The case $n = 2$ is special because to build our vectorial FCSR, there is a single irreducible polynomial of degree 2 on $\mathbb{F}_2$: $X^2 - X - 1$ modulo 2. For $n = 3$, we have two polynomials $X^3 - X - 1$ and $X^3 - X^2 - 1$ modulo 2. VFCSRs models for quadratic and cubic cases are given in Table 1.

Table 1. Theoritical models for FCSRs and VFCSRs

	Quadratic Case	Cubic Case
VFCSR	$(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$	$(\mathbb{F}_2, X^3 - X - 1, \mathcal{B})$
Connection integer	$u = \widetilde{q}_0 - 1$ and $v = \widetilde{q}_1$	$u = \widetilde{q}_0 - 1$, $v = \widetilde{q}_1$ and $w = \widetilde{q}_2$
Connection Matrix	$\mathcal{M} = \begin{pmatrix} u & v \\ -v & -u-v \end{pmatrix}$	$\begin{pmatrix} -u & -w & -v \\ -v & -v-w & -v-w \\ -w & -v & -u-w \end{pmatrix}$
Form f determinant	$u^2 + uv - v^2$	$-u^3 - v^3 - w^3 + 3uvw$ $+uv^2 - uw^2 - 2u^2w + vw^2$
l-Sequences	$\widetilde{q} = f(u,v)$ odd prime 2 primitive root modulo $\widetilde{q}$	$\widetilde{q} = f(u,v)$ odd prime 2 primitive root modulo $\widetilde{q}$
$\widetilde{q} = 11$	$(u,v) = (3,2)$	$(u,v,w) = (-1,2,0)$
59	$(7,2)$	$(-1,2,4)$
101	$(9,4)$	$(5,4,2)$
701	$(27,28)$	$(9,2,0)$

3 Investigation of VFCSRs

3.1 Quadratic Case

We analyse the quadratic case of VFCSRs (see Table1). From Equations 2 and 3, operations are defined as follows:

1. Form integers σ_1^z and σ_0^z, as follows

$$\sigma_1^z = \sum_{i=1}^{i=r} \left(q_1^i a_1^{z-i} + q_1^i a_0^{z-i} + q_0^i a_1^{z-i} \right) + m_1^{z-1}, \forall z \geq r \tag{6}$$

$$\sigma_0^z = \sum_{i=1}^{i=r} \left(q_1^i a_1^{z-i} + q_0^i a_0^{z-i} \right) + m_0^{z-1}$$

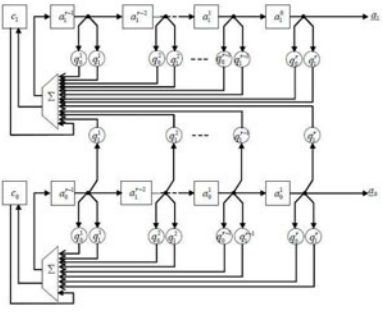


Fig. 1. VFCSR representation for a triplet (q, u, v)

2. Shift the content of the first element register and the second element register on step to the right, while outputing the rightmost bits a_1^{z-i} and a_1^{z-i} as shown in Fig. 1.
3. Put $a_1^{z-i} = \sigma_1^z \pmod 2$ and $a_0^{z-i} = \sigma_0^z \pmod 2$, $\forall z \geq r$.
4. Replace memorys integer as below: $m_1^z = \frac{\sigma_1^z - a_1^z}{2}$ and $m_0^z = \frac{\sigma_0^z - a_0^z}{2}$.

3.2 Parameters Research

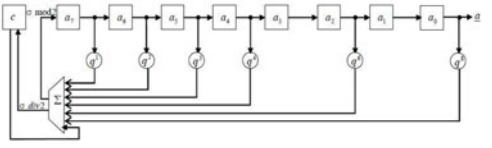
Research parameters for VFCSR is a fundamental task, due to the fact that in this case which is different from FCSRs; parameter connection is not only a prime number but a triplet system of parameters $(\widetilde{q}, u, v)$ as defined by the following equation where, $\widetilde{q}$ is an odd prime number and 2 is primitive root modulo $\widetilde{q}$, u is an odd number and v even number.

$$\widetilde{q} = u^2 + u.v - v^2 \tag{7}$$

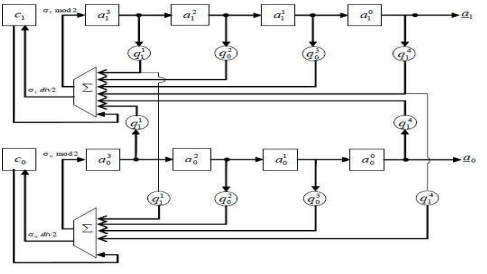
In Table 4, the results from simulation allow us to conclude on the behavior of VFCSRs based on triple $(\widetilde{q}, u, v)$:

- For a fixed u in a triplet $(\widetilde{q}, u, v)$ we see that the periode $(\widetilde{q} - 1)$ with $u > v$ is higher than that where $u < v$.
- For certain integer connection $\widetilde{q}$, there is more than a couple (u, v) which satisfies the equation 7.
- The number of cells $(2l_{\max})$ used to represent VFCSRs when $u > v$ is less than or equal to the number of cells representing FCSRs.
- The number of cells $(2l_{\max})$ used to represent VFCSRs when $u < v$ is greater than or equal to the number of cells representing FCSRs.
- Number of cells representing VFSCR is $2 \times l_{(u,v)}$, where $l_{(u,v)} = \max length(u, v)$.

We give an example of vectorial l-sequence. We take an VFCSR over $(\mathbb{F}_2, X^2 - X - 1, \mathcal{B})$ size $r = 2$ with connection coefficient $q_1 = 1$ and $q_2 = \bar{X}$. We load initial state $(a_0, a_1, m_1) = (1, \bar{X} + 1, 3 - 4\bar{X})$. The length of the pre-period is 6 and the period is 10. The connection vector is $(\tilde{q}_0, \tilde{q}_1) = (4, 2)$. $\tilde{q}$ is equal to



(a)



(b)

Fig. 2. (a) FCSR representation for connexion integer 349, (b) VFCSR representation for triplet (349,17,12)

$(4-1)^2+(4-1).2+2^2=11$. We verify the proposition 4. Finally, we have five 0's and five 1's in one period. The halves of a period are complementary. The output sequence and memory is in vectorial representation:

a_0^i	1	1	1	1	0	1	1	0	1	0	0	0	1	0	1	1	1	0	1		
a_1^i	0	1	0	1	0	1	0	1	1	1	0	1	0	0	0	1	0	1	1	1	
m_0^{i+1}	3	2	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	1	1	
m_1^{i+1}	−4	−1	0	1	1	1	1	1	1	2	1	1	1	1	0	1	1	1	1	2	

where Fig. 2 shows representation for the two conceptions of FCSRs and VFCSRs. For this example, connection integer for FCSR is $q = 349$, where for the VFCSR is as defined above by 7; $(\widetilde{q}, u, v) = (349, 17, 12)$.

3.3 Testing on Pseudorandom Property of VFCSR Sequences

In order to test pseudorandom property of sequences generated by VFCSR, in the quadratic case, with different stage and compare the testing results with those for FCSR in [8], we have taken several triplets $(\widetilde{q}, u, v)$ with differents magnitudes (see Table 4) with the case where $u > v$ and $u < v$. All tests have been investigated by package NIST (National Institute of Standardization and Technology) STS [9], which is a special package designed to test the sequences generated by sequences generators. These tests are useful in detecting deviations of a binary sequence from randomness [10]. This package consists of 15 differents statistical tests, which allow accepting (or rejecting) the hypothesis about randomness of the testing sequence. Nist framework, like many tests, is based

Table 2. Results statistical tests 1-4 on some triplets (q̃, u, v)

$\widetilde{q}$ (u,v)	Seq	Test 1		Test 2		Test 3		Test 4	
		P-value	Task	P-value	Task	P-value	Task	P-value	Task
829	a0	0.972294	Succ	0.972260	Succ	0.498961	Succ	0.874766	Succ
(35,34)	a1	0.972294	Succ	0.972260	Succ	0.498961	Succ	0.654567	Succ
1259	a0	0.977516	Succ	0.932602	Succ	0.498961	Succ	0.317535	Succ
(35,44)	a1	0.977516	Succ	0.932602	Succ	0.498961	Succ	0.472308	Succ
2389	a0	0.983677	Succ	0.983670	Succ	0.498961	Succ	0.353726	Succ
(85,28)	a1	0.983677	Succ	0.983670	Succ	0.498961	Succ	0.571931	Succ
3581	a0	0.986667	Succ	0.986664	Succ	0.527464	Succ	0.856311	Succ
(85,124)	a1	0.986667	Succ	0.986664	Succ	0.527464	Succ	0.949487	Succ
7621	a0	0.990860	Succ	0.990859	Succ	0.498961	Succ	0.653463	Succ
(89,86)	a1	0.990860	Succ	0.990859	Succ	0.512361	Succ	0.580758	Succ
8179	a0	0.991178	Succ	0.973536	Succ	0.511447	Succ	0.891599	Succ
(98,124)	a1	0.991178	Succ	0.973536	Succ	0.498961	Succ	0.865508	Succ
8821	a0	0.991505	Succ	0.991504	Succ	0.498961	Succ	0.806508	Succ
(95,84)	a1	0.991505	Succ	0.991504	Succ	0.498961	Succ	0.806508	Succ
9949	a0	0.992001	Succ	0.992000	Succ	0.478444	Succ	0.521477	Succ
(95,108)	a1	0.992001	Succ	0.992000	Succ	0.468205	Succ	0.917313	Succ

Table 3. Statistical Tests

Statistical Tests	**Deffect detected**	**Length**
1-Frequency	Larger than expected deviation from the theoretical distribution of zeroes and ones, too many ones or zeroes	≥ 100
2-Serial	Non-uniform distribution of m-length words.	≥ 100
3-Cumulative Sums	Too many zeroes or ones at the bigining of the sequence	≥ 100
4-Run	Large (small) test statistic indicates that the oscillation	≥ 100
	in the bitstream is too fast (too slow).	
5-Matrix Rank	Deviation of the rank distribution from a corresponding	≥ 38912
	random sequence, due to periodicity	
6-DFT	Periodic featurs	≥ 1000
7-Maurer	Compressibility (regularity)	≥ 387840

on hypothesis testing. Testing result is $P-value \in [0,1]$. If $P-value \geq 0.01$ The tested sequence is considered to be random (accepted) and the bigger the $P-value$ is, the better pseudorandom property the tested sequence has.

Table 2 show results testing on sequences $\underline{a}_0$ and $\underline{a}_1$ for some triplets listed in Table 4. Tests selected for this group are those that require at least a subsequence of size 100 bits; test 1 to 4 as listed in Table 3. It is observed that the two sequences generated by the VFCSR have passed the four tests since all $P-value > 0.01$. That mean that the two sequences have perfect balance and good uniform distribution.

Table 4. Some triplets and their length.

Some results														
$l_{\widetilde{q}}$	$\widetilde{q}$	$l_{(u,v)}$	u	v	$l_{\widetilde{q}}$	$\widetilde{q}$	$l_{(u,v)}$	u	v	$l_{\widetilde{q}}$	$\widetilde{q}$	$l_{(u,v)}$	u	v
4	11	2	3	2	16	101419	8	331	354	18	411491	9	639	634
4	11	5	31	50	16	109891	8	331	330	18	424451	9	651	650
10	1259	5	35	34	16	115259	8	339	338	18	428339	9	657	662
9	829	5	35	44	16	103451	8	339	370	18	443771	9	657	638
13	8821	6	85	28	16	112181	8	351	380	18	467171	9	683	682
11	2389	6	85	124	16	121421	8	351	332	18	481619	9	675	634
12	8179	6	89	86	17	132499	8	373	390	18	502499	9	689	646
11	3581	6	89	124	17	157141	8	373	316	20	1164589	9	1001	204
13	9949	6	95	84	18	389219	9	637	662	20	3932741	10	2001	2036
12	7621	6	95	108	18	395429	9	651	692					

As shown in Fig.3-a, the two sequences for connection integer from $\widetilde{q} = 101419$ to $\widetilde{q} = 157141$ as defined in table4, have passed the Matrix Rank. In Fig.3-b where the Maurer Test is performed for connection integer $\widetilde{q} = 389219$ to $\widetilde{q} = 502499$, in order to mesure the compressibility of sequences, it's appears that test was passed and the sequence should be considered as random. While in Fig.3-c, for DFT Test applicated on VFCSR with integer connection triplet $(\widetilde{q}, u, v) = (1164589, 1001, 204)$, it is observed that as the size of subsequence increases (by step of 20000 *bits*) the

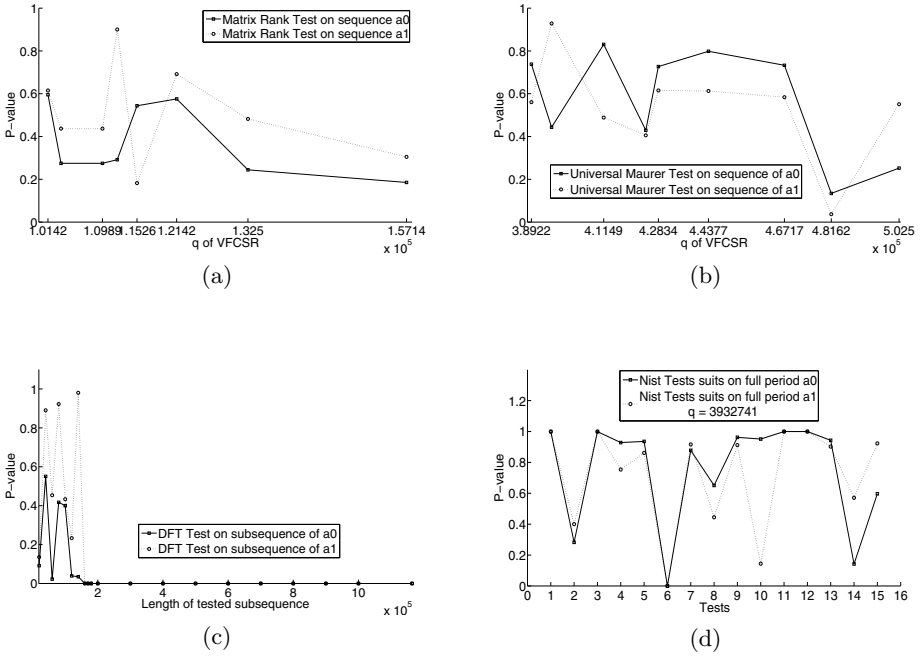


Fig. 3. Testing results of: (a) Matrix Rank Test, (b) Universal Maurer Test, (c) DFT Test and (d) all NIST Tests

test results decreases to 0 when their length exceeds one ninth of the period. The reason for the decrease of $P - value$ is that l-sequence generated by VFCSR begin to show repetition when the subsequence becomes long.

Fig.3-d represent results for all statistical Tests in the Nist suite applicated on a VFCSR whith integer connection triplet $(3932741, 2001, 2036)$, on the curve, tests are presented from 1 to 15 as deffined in [10]-p.201. All tests are passed successfuly wich conclude on the good randomness propertys of VFCSR on $\mathbb{F}_{2^2}$.

4 Conclusion and Open Problems

The construction of VFCSR depends on the choice of the prime fields $\mathbb{F}_p$, the polynomial P and the basis $\mathcal{B}$ but the main results of analysis don't depend to the basis. Most of the fundamental results of this paper are true for p odd prime. We have a limited choice of irreducible polynomials of degree n in $\mathbb{F}_p$. There is therefore a finite number of ways to build a VFCSR for p and n fixed. The form of P affects the difficulty of calculations from the register. We must therefore look for simple forms of P as trinomial. For example, for every p prime, $X^p - X - 1$ is irreducible in $\mathbb{F}_p$. Illustrated numerical experiments conducted utilizing NIST Statistical Tests Suite, confirm the good propertys of the VFCSRs.

References

1. Goresky, M., Klapper, A.: Feedback shift registers, combiners with memory, and 2-adic span. Journal of Cryptology 10, 111–147 (1997)
2. Goresky, M., Klapper, A.: 2-adic shift registers. In: Anderson, R. (ed.) FSE 1993. LNCS, vol. 809, pp. 174–178. Springer, Heidelberg (1994)
3. Klapper, A.: Feedback with Carry Shift Registers over Finite Fields (extended abstract). In: FSE 1994, pp. 170–178 (1994)
4. Goresky, M., Klapper, A.: Feedback Registers Based on Ramified Extensions of the 2-Adic Numbers (Extended Abstract). In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 215–222. Springer, Heidelberg (1995)
5. Goresky, M., Klapper, A.: Periodicity and Correlation Properties of d-FCSR Sequences. Des. Codes Cryptography 33(2), 123–148 (2004)
6. Klapper, A., Xu, J.: Algebraic Feedback Shift Registers. Theor. Comput. Sci. 226(1-2), 61–92 (1999)
7. Goresky, M., Klapper, A.: Algebraic Shift Register Sequences (2009), http://www.cs.uky.edu/~klapper/algebraic.html
8. Zheng, Y., Tang, X., He, D., Xu, L.: Investigation on pseudorandom properties of FCSR sequence. In: Proc. IEEE International Conference on Communications, Circuits and Systems, vol. I, pp. 66–70 (2005)
9. http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.0.zip
10. http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf
11. Arnault, F., Berger, T.P.: Design and Properties of a New Pseudorandom Generator Based on a Filtered FCSR Automaton. IEEE Transaction on Computers 54(11), 1374–1383 (2005)
12. Berger, T., Arnault, F., Lauradoux, C.: Description of F-FCSR-8 and F-FCSR-H stream ciphers. In: SKEW - Symmetric Key Encryption Workshop, An ECRYPT STVL event, Aarhus, Danemark (May 2005)

Fourier Duals of Björck Sequences

Branislav M. Popović

Huawei Technologies Sweden AB,
Box 54, 164 94 Kista, Sweden
branislav.popovic@huawei.com

Abstract. Closed-form expressions for the Fourier duals of Björck sequences are derived. Based on these expressions, the definition of Björck sequences of prime lengths $N \equiv 3 \pmod 4$ is extended to include additional, previously unknown Constant Amplitude Zero Autocorrelation (CAZAC) sequences.

Keywords: Sequences, DFT, Fourier dual, CAZAC, Björck.

1 Introduction

The Constant Amplitude Zero (periodic) Autocorrelation (CAZAC) polyphase sequences have been extensively used in communications [1,2] and radars [3]. A lesser known family of CAZAC sequences is the family of Björck sequences [3,4]. The potential applications of these sequences in frequency domain raise the interest in the properties of their Fourier duals.

In Section 2 the basic mathematical definitions are stated. In Section 3 the Fourier duals of Björck sequences are derived. The Section 4 summarizes the paper.

2 Definitions

The periodic cross-correlation $R_{xy}(p)$ of two sequences $\{x(k)\}$ and $\{y(k)\}$, $k = 0, 1, \ldots, N-1$, is defined as

$$R_{xy}(p) = \sum_{k=0}^{N-1} x^*(k)y(k+p) \tag{1}$$

where $p = 0, 1, \ldots, N-1$ is the cyclic delay and '*' denotes complex conjugate. The periodic autocorrelation $R_{xx}(p)$ of sequence $\{x(k)\}$ is defined by (1) when $\{y(k)\}$=$\{x(k)\}$. The $R_{xx}(p)$ is *ideal* when $R_{xx}(p) = 0$ for any $p \not\equiv 0 \pmod N$. If the sequence with ideal periodic autocorrelation has constant amplitude, it is called a CAZAC sequence.

The Discrete Fourier Transform (DFT) $\{X(n)\}$, $n = 0, 1, \ldots, N-1$, of a sequence $\{x(k)\}$, $k = 0, 1, \ldots, N-1$, is defined as

$$X(n) = \sum_{k=0}^{N-1} x(k)W_N^{nk} \tag{2}$$

$$W_N = e^{-j2\pi/N} \ , \ j = \sqrt{-1} \ , \ N \text{ is any positive integer .}$$

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 253–258, 2010.

The Fourier dual of a sequence $\{x(k)\}$ is its DFT sequence $\{X(n)\}$ normalized by $\sqrt{N}$.

Vector of DFT coefficients of any sequence of symbols of constant amplitude has the ideal period autocorrelation, but only a CAZAC sequence has its DFT coefficients of constant amplitude. It can be shown that the necessary and sufficient condition for a sequence to be the CAZAC sequence is that its DFT coefficients have constant amplitude. Thus, if a CAZAC sequence of length N has the symbols of unit amplitude, according to Parseval's theorem the corresponding DFT coefficients have the amplitudes equal to $\sqrt{N}$. Hence the Fourier dual of a unit amplitude CAZAC sequence is also a unit amplitude CAZAC sequence.

A Björck sequence $\{x(k)\}$ can be defined only for prime lengths $N > 2$. For prime lengths $N \equiv 1 \pmod 4$, the Björck sequences are defined as

$$x(k) = e^{j\theta\left(\frac{k}{N}\right)}, \quad k = 0, 1, \ldots, N-1 \tag{3}$$
$$\theta = \cos^{-1}\left(\frac{1}{1+\sqrt{N}}\right)$$

where $\left(\frac{k}{N}\right)$ is the Legendre symbol, defined for any integer k and any odd prime N, as

$$\left(\frac{k}{N}\right) = \begin{cases} 0, & \text{if } k \equiv 0 \pmod N \\ +1, & \text{if } k \not\equiv 0 \pmod N \text{ is a square} \pmod N \\ -1, & \text{if } k \not\equiv 0 \pmod N \text{ is not a square} \pmod N \end{cases} \tag{4}$$

For prime lengths $N \equiv 3 \pmod 4$, the Björck sequences are defined as

$$x(k) = \begin{cases} e^{j\phi}, & \text{if } \left(\frac{k}{N}\right) = -1, \quad k = 0, 1, \ldots, N-1 \\ 1, & \text{otherwise} \end{cases} \tag{5}$$
$$\phi = \cos^{-1}\left(\frac{1-N}{1+N}\right) .$$

The binary-to-biphase (BTB) alphabet transform similar to (5), given by

$$x(k) = BTB\,[b(k)] = e^{j\phi}, \text{ if } b(k) = -1$$

has been defined in [5], to produce a biphase CAZAC sequence from a binary pseudo-noise sequence $\{b(k)\}$, whose alphabet is $\{+1, -1\}$ and periodic autocorrelation $R_{bb}(p) = -1$ for any $p \not\equiv 0 \pmod N$, $N \equiv 3 \pmod 4$. The same transform has been used in [6] to obtain a CAZAC sequence from a binary Hadamard cyclic difference set sequence.

In Section 3 we derive an extended definition of Björck sequences for prime $N \equiv 3 \pmod 4$ by including the Fourier dual of (5). This extended definition is given by

$$z(k) = \begin{cases} 1 \text{ or } e^{j\phi}, & k = 0 \\ e^{j\frac{\phi}{2}\left[1-\left(\frac{k}{N}\right)\right]}, & k = 1, 2, \ldots, N-1 \end{cases} \tag{6}$$

$$\phi = \cos^{-1}\left(\frac{1-N}{1+N}\right), \quad N \equiv 3 \pmod 4 .$$

An equivalent extended definition of Björck sequences can be obtained if the BTB transform is applied on the pair of binary pseudo-noise Legendre sequences of the same length. Such a pair of binary sequences is defined through a bipolar ternary Legendre sequence of a prime length $N \equiv 3 \pmod 4$, whose Legendre symbol $\left(\frac{0}{N}\right)$ is replaced either by $+1$ or -1 [7].

3 Fourier Duals

For a Björck sequence of prime length $N \equiv 1 \pmod 4$, the DFT $\{X(n)\}$, $n > 0$, can be obtained from (2) and (3) as

$$\begin{aligned} X(n) &= 1 + \sum_{k=1}^{N-1} \left[\cos\theta + j\left(\frac{k}{N}\right)\sin\theta\right] e^{-j\frac{2\pi}{N}nk} \\ &= 1 - \cos\theta + j\left(\frac{n}{N}\right)\sin\theta \sum_{k=1}^{N-1}\left(\frac{nk}{N}\right) e^{-j\frac{2\pi}{N}nk} \\ &= \sqrt{N}\cos\theta + G^*(1,N)j\left(\frac{n}{N}\right)\sin\theta \end{aligned} \tag{7}$$

where $G^*(u,N)$ is the complex-conjugate of the Gauss sum [8]

$$G(u,N) = \sum_{l=0}^{N-1}\left(\frac{l}{N}\right) W_N^{-ul} = \begin{cases} \left(\frac{u}{N}\right)\sqrt{N}, & \text{if } N \equiv 1 \pmod 4 \\ \left(\frac{u}{N}\right) j\sqrt{N}, & \text{if } N \equiv 3 \pmod 4 \end{cases} \tag{8}$$

where u is a positive integer such that $(u,N) = 1$.

From (7) and (8) we obtain

$$\begin{aligned} X(n) &= \sqrt{N} e^{j\theta\left(\frac{n}{N}\right)} \\ &= \sqrt{N} x(n), \ n > 0 . \end{aligned} \tag{9}$$

For $n = 0$ we have

$$\begin{aligned} X(0) &= 1 + (N-1)\cos\theta + j\sin\theta \sum_{k=1}^{N-1}\left(\frac{k}{N}\right) \\ &= 1 + (N-1)\frac{1}{1+\sqrt{N}} \\ &= \sqrt{N} \\ &= \sqrt{N} x(0) . \end{aligned} \tag{10}$$

By (9) and (10) we have shown that the Fourier dual of a Björck sequence of prime length $N \equiv 1 \pmod 4$ is equal to the sequence itself.

To calculate the DFT of Björck sequences of prime lengths $N \equiv 3 \pmod 4$, we shall re-formulate the original definition (5) as

$$x(k) = \begin{cases} 1, & k = 0 \\ e^{j\frac{\phi}{2}\left[1-\left(\frac{k}{N}\right)\right]}, & k = 1, 2, \ldots, N-1 \, . \end{cases} \tag{11}$$

From (2) and (11) it follows that $\{X(n)\}$, $n > 0$, is given by

$$\begin{aligned} X(n) &= 1 + e^{j\frac{\phi}{2}} \sum_{k=1}^{N-1} \left[\cos\frac{\phi}{2} - j\left(\frac{k}{N}\right)\sin\frac{\phi}{2}\right] e^{-j\frac{2\pi}{N}nk} \\ &= 1 - e^{j\frac{\phi}{2}} \left[\cos\frac{\phi}{2} + j\left(\frac{n}{N}\right)\sin\frac{\phi}{2}\, G^*(1,N)\right] \\ &= e^{j\frac{\phi}{2}} \left[-j\sin\frac{\phi}{2} - \sqrt{N}\left(\frac{n}{N}\right)\sin\frac{\phi}{2}\right] \, . \end{aligned} \tag{12}$$

From the definition of ϕ it follows that

$$\sin\frac{\phi}{2} = \pm\sqrt{\frac{1-\cos\phi}{2}} = \pm\frac{\sqrt{N}}{\sqrt{1+N}} = \sqrt{N}\cos\frac{\phi}{2} \tag{13}$$

so from (12) and (13) we obtain

$$\begin{aligned} X(n) &= \sqrt{N}(-j)e^{j\frac{\phi}{2}} \left[\cos\frac{\phi}{2} - j\left(\frac{n}{N}\right)\sin\frac{\phi}{2}\right] \\ &= \sqrt{N}(-j)x(n), \; n > 0 \, . \end{aligned} \tag{14}$$

For $n = 0$ we have

$$\begin{aligned} X(0) &= 1 + e^{j\frac{\phi}{2}} \left[(N-1)\cos\frac{\phi}{2} - j\sin\frac{\phi}{2}\sum_{k=1}^{N-1}\left(\frac{k}{N}\right)\right] \\ &= 1 + (N-1)\left(\cos^2\frac{\phi}{2} + j\sin\frac{\phi}{2}\cos\frac{\phi}{2}\right) \\ &= \frac{2N}{1+N} - j\sqrt{N}\frac{1-N}{1+N} \\ &= \sqrt{N}\,(\sin\phi - j\cos\phi) \\ &= \sqrt{N}(-j)e^{j\phi} \, . \end{aligned} \tag{15}$$

By (14) and (15) we have shown that the Fourier dual of a Björck sequence of prime length $N \equiv 3 \pmod 4$ is equal to a scaled version of another CAZAC sequence $\{y(k)\}$, where $\{y(k)\}$ is obtained by replacing the first element of the original sequence $\{x(k)\}$ with the symbol $e^{j\phi}$, i.e.

$$y(k) = \begin{cases} e^{j\phi}, & k = 0 \\ e^{j\frac{\phi}{2}\left[1-\left(\frac{k}{N}\right)\right]}, & k = 1, 2, \ldots, N-1 \, . \end{cases} \tag{16}$$

The sequence $\{y(k)\}$ is included in the extended definition of the Björck sequences (6) as it cannot be obtained from the sequence $\{x(k)\}$ through any combination of the transforms which preserve the ideal periodic autocorrelation function. For example, the complex conjugation, the inversion, or the multiplication with linear complex exponential function, applied to the the sequence $\{x(k)\}$, would produce a new sequence alphabet which is different from the one common to the sequences $\{x(k)\}$ and $\{y(k)\}$. Similarly, as the number of repetitions of any of the two symbols from the common alphabet is not the same in $\{x(k)\}$ and $\{y(k)\}$, the sequence $\{y(k)\}$ obviously cannot be obtained neither by reversion nor by a cyclic shift of the sequence $\{x(k)\}$.

The Fourier dual of the sequence $\{y(k)\}$ can be obtained in a similar manner as for the sequence $\{x(k)\}$. Thus we have

$$\begin{aligned} Y(n) &= e^{j\phi} - e^{j\frac{\phi}{2}} \left[\cos\frac{\phi}{2} + j\left(\frac{n}{N}\right) \sin\frac{\phi}{2} \, G^*(1, N) \right] \\ &= e^{j\frac{\phi}{2}} \left[j \sin\frac{\phi}{2} - \sqrt{N}\left(\frac{n}{N}\right) \sin\frac{\phi}{2} \right] \\ &= \sqrt{N} \, j \, e^{j\frac{\phi}{2}\left[1+\left(\frac{n}{N}\right)\right]} \\ &= \sqrt{N} \, j \, e^{j\phi} \, y^*(n), \; n > 0 \, . \end{aligned} \tag{17}$$

$$\begin{aligned} Y(0) &= e^{j\phi} + (N-1)\left(\cos^2\frac{\phi}{2} + j \sin\frac{\phi}{2} \cos\frac{\phi}{2} \right) \\ &= \sqrt{N} \, j \\ &= \sqrt{N} \, j \, e^{j\phi} \, y^*(0) \, . \end{aligned} \tag{18}$$

By (17) and (18) we have shown that the Fourier dual of the modified Björck sequence $\{y(k)\}$ of prime length $N \equiv 3 \pmod 4$ is equal to a scaled complex conjugated version of the sequence itself.

4 Conclusions

The recent extensive frequency domain applications of the Constant Amplitude Zero (periodic) Autocorrelation (CAZAC) sequences, particularly on the uplink of LTE cellular communication system, raise the interest in the Fourier duals of CAZAC sequences. The Fourier duals of a lesser known family of CAZAC sequences, called Björck sequences, are derived in this paper.

It has been shown that the Björck sequences of prime lengths $N \equiv 1 \pmod 4$ are self-dual, while those of the prime lengths $N \equiv 3 \pmod 4$ are not. Based on these results, the definition of Björck sequences of prime lengths $N \equiv 3 \pmod 4$ is extended to include the corresponding Fourier duals.

References

1. Sesia, S., Toufik, I., Baker, M. (eds.): LTE - The UMTS Long Term Evolution: from Theory to Practice. John Wiley & Sons Ltd., Chichester (2009)
2. Popovic, B.M.: Efficient DFT of Zadoff-Chu sequences. Electronics Letters 46(7) (April 1, 2010)
3. Benedetto, J.J., Konstantinidis, I., Rangaswamy, M.: Phase-Coded Waveforms and Their Design. IEEE Signal Processing Magazine 22 (January 2009)
4. Björck, G.: Functions of modulus 1 on Zn whose Fourier transforms have constant modulus, and "cyclic n-roots". In: Byrnes, J.S., Byrnes, J.F. (eds.) Recent Advances in Fourier Analysis and Its Applications. NATO-ASI Series C, vol. 315, pp. 131–140. Kluwer Academic Publishers, Dordrecht (1990)
5. Bömer, L., Antweiler, M.: Binary and Biphase Sequences and Arrays with Low Periodic Autocorrelation Sidelobes. In: IEEE ICASSP Conference, Albuquerque, pp. 1663–1666 (1990)
6. Golomb, S.W.: Two-Valued Sequences with Perfect Periodic Autocorrelation. IEEE Trans. on Aerospace and Electronic Systems 28(2), 383–386 (1992)
7. Gottesman, S.R., Grieve, P.G., Golomb, S.W.: A Class of Pseudonoise-Like Pulse Compression Codes. IEEE Trans. on Aerospace and Electronic Systems 28(2), 355–362 (1992)
8. Berndt, B.C., Evans, R.J., Williams, K.S.: Gauss and Jacobi sums. John Wiley & Sons Inc., New York (1998)

New Constructions of Complete Non-cyclic Hadamard Matrices, Related Function Families and LCZ Sequences

Krystal Guo and Guang Gong

Department of Combinatorics and Optimizations
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
{kguo,ggong}@uwaterloo.ca

Abstract. A Hadamard matrix is said to be completely non-cyclic (CNC) if there are no two rows (or two columns) that are shift equivalent in its reduced form. In this paper, we present three new constructions of CNC Hadamard matrices. We give a primary construction using a flipping operation on the submatrices of the reduced form of a Hadamard matrix. We show that, up to some restrictions, the Kronecker product preserves the CNC property of Hadamard matrices and use this fact to give two secondary constructions of Hadamard matrices. The applications to construct low correlation zone sequences are provided.

Keywords: Hadamard matrices, completely non-cyclic type, low correlation zone sequences, shift-distinctness.

1 Introduction and the Basic Definitions

Low correlation zone sequences (LCZ) signal sets have important applications in quasi-synchronous code division multiple access (CDMA) applications, proposed in 1992 [3]. There has been considerable work towards constructions of these sequences. The first construction of LCZ set, given in [11] in 1998, produces a LCZ signal set whose size is not maximized. Following this approach, many different constructions have been proposed, including approaches in [12,9,13,8,10,16,1]. In 2007, Gong, Golomb, and Song [5] describe a general approach to the construction of LCZ sequences using sequences with subfield decompositions. Constructions of this type of LCZ signal sets with maximum size are in one-to-one correspondence with constructions of completely non-cyclic Hadamard matrices.

In this paper, we will show three new constructions of such Hadamard matrices. The first and third new constructions generalize two known constructions in [8] and with improved results. The second construction is the Kronecker product of matrices, which we show to preserve the completely non-cyclic property, under some conditions.

We now introduce basic concepts and definitions which will be used throughout the paper.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 259–269, 2010.

A. Basic Concepts about Sequences. Let p be a prime number, $\mathbb{F}_p$ denote a finite field with p elements, and $\mathbf{a} = \{a_i\}$ be a sequence over $\mathbb{F}_p$, of period N. The shift operator is defined by $L(\mathbf{a}) := (a_1, a_2, \cdots)$. So, $L^r(\mathbf{a}) = (a_r, a_{r+1}, \cdots)$. For two sequences, $\mathbf{a}$ and $\mathbf{b}$, if $\mathbf{b} = L^r(\mathbf{a})$, then $\mathbf{a}$ and $\mathbf{b}$ are called *shift equivalent*, denoted $\mathbf{a} \sim \mathbf{b}$. Otherwise, we say that $\mathbf{a}$ and $\mathbf{b}$ are *shift distinct* and write $\mathbf{a} \nsim \mathbf{b}$. If the elements of $\mathbf{a}$ satisfies the linear recursive relation: $a_{r+k} = \sum_{i=0}^{r-1} c_i a_{i+k}, k \in \mathbb{Z}$, where $c_i \in \mathbb{F}_p$ and $t(x) = x^r - \sum_{i=0}^{r-1} c_i x^i$ is the polynomial with the smallest degree which recursively generates $\mathbf{a}$, then the degree of $t(x)$ is called the *linear span* of $\mathbf{a}$, denoted $l(\mathbf{a})$.

When $N \,|\, p^n - 1$, we can associate the sequence $\mathbf{a}$ with a function $f(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ such that $a_i = f(\alpha^i), i \in \mathbb{Z}$, where α is an element in $\mathbb{F}_{p^n}$ with order N. Then $\mathbf{a}$ is called an *evaluation* of $f(x)$. In this paper, we assume that $f(0) = 0$. We say that $\mathbf{a}$ is *balanced* if $|N_a - N_b| \leq 1$ for any $a, b \in \mathbb{F}_p$ where $N_x = |\{a_i = x \,|\, 0 \leq i < N\}|$. Let $\omega = e^{2\pi i/p}$ be a primitive pth root of unity. The *periodic crosscorrelation* of $\mathbf{a}$ and $\mathbf{b}$ is defined by $C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} \omega^{b_{i+\tau} - a_i}$, $0 \leq \tau \leq N-1$ where the indices are computed modulo $N-1$. If $\mathbf{b} = \mathbf{a}$, we write $C_{\mathbf{a},\mathbf{b}}(\tau)$ as $C_{\mathbf{a}}(\tau)$ and call it the *autocorrelation* of $\mathbf{a}$. If $\mathbf{a}$ is balanced and $C_{\mathbf{a}}(\tau) = \begin{cases} N, & \tau \equiv 0 \pmod{N} \\ -1, & \tau \not\equiv 0 \pmod{N}, \end{cases}$ then we say that $\mathbf{a}$ has an *(ideal) 2-level autocorrelation function.*

B. Hadamard Matrices and CNC Hadamard Matrices. A *Hadamard matrix* of order n is a $n \times n$ matrix H with entries in $\{1, -1\}$, such that $HH^T = H^T H = nI_n$, where I_n is the n by n identity matrix. By applying elementary "Hadamard-preserving" operations, the matrix H can always be transformed into a special form in which all entries in the first row and the first column are equal to 1, see [2,4]. Without loss of generality, all the Hadamard matrices in this paper will be assumed to be in this form. The *reduced form* of H, denoted H^- is the matrix obtained from H by deleting the first row and the first column. A Hadamard matrix is said to be *completely non-cyclic (CNC) with respect to row (or column) shifts* if any two rows (respectively columns) in the reduced form of H are shift distinct.

One can see that, up to cyclic shifts, there is a unique sequence of length 3 consisting of two -1's and one 1. This implies that there is no CNC Hadamard matrix of order 4. By a similar enumeration, there are five shift-distinct sequences of length 7 consisting of four -1's and three 1's, which implies that there is no CNC Hadamard matrix of order 8. The smallest value of q for which there exists a CNC Hadamard matrix of order 2^q is 4.

A *generalized Hadamard matrix* is a matrix $H = (h_{ij})_{v \times v}$ where $h_{ij} = \omega^{s_{ij}}, s_{ij} \in \mathbb{F}_p$ of order v such that $HH^* = vI_v$, where H^* is the conjugate transpose of H and ω is a primitive pth root of unity. Reduced form and the CNC property are analogously defined for generalized Hadamard matrices.

C. Equivalent Problem. A *low correlation zone signal set with parameters* (N, r, δ, d) is a set $\mathcal{K}$ consisting of r shift-distinct sequences over $\mathbb{F}_p$ with period N which satisfies that $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq \delta$ for all τ such that $|\tau| < d$, when $\mathbf{a}, \mathbf{b} \in \mathcal{K}$,

and $\tau \neq 0$, when $\mathbf{a} = \mathbf{b}$. It has been shown in the literature [13,8,5], that a construction of an LCZ signal set with the parameters $(q^m - 1, q - 1, -1, d)$ where $d = (q^m - 1)/(q - 1)$ $(q = p^n)$ is equivalent to a construction of a family of functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, denoted as S, satisfying the following three conditions:

(a) Each function in S is balanced,
(b) The sum of any two functions in S is also balanced, and
(c) Any two sequences obtained from the functions in S by evaluation are shift distinct.

The number of functions in S, denoted $|S|$, cannot exceed $q - 1$. Gong, Golomb and Song [5] point out that a construction of S with maximal size is equivalent to a construction of a CNC Hadamard matrix of order q. In the literature, there are only three known constructions for the CNC Hadamard matrices of order q, of which the first two appear in [8] and one of them also appears in [13] as a somehow equivalent case, and the third in [5].

See [4] for further background on the theory of sequences and known constructions of 2-level autocorrelation sequences (see Chapters 8-9).

The rest of the paper is organized as follows. In Section 2, we present a new primary construction for CNC Hadamard matrices of order $q = p^n$ based on 2-level autocrrelation sequences over F_p and the flipping operator. In Section 3, we assert, under some restrictions, that Kronecker products of CNC Hadamard matrices are again CNC Hadamard matrices. In Section 4, we give a construction using the Kronecker product and 2-level autocorrelation sequences. Section 5 provides the related functions and LCZ signal sets, and Section 6 includes concluding remarks. [6] is a full version of this paper.

2 A Primary Construction of CNC Hadamard Matrices Using Flipping Operator

In this section, we present a new primary construction for CNC generalized Hadamard matrices of order $q = p^n$, where p is a prime. We assume that $N = p^n - 1$. For a given 2-level autocorrelation sequence $\mathbf{a} = (a_0, \cdots, a_{N-1})$ over $\mathbb{F}_p$, we may construct a circular matrix $C(\mathbf{a}) = (a_{ij})$ where $a_{ij} = a_{i+j}$. Let $b_i = \omega^{a_i}$, where ω is a primitive pth root of unity. Then we have the circular matrix $C(\mathbf{b})$, also written symbolically as $C(\mathbf{b}) = \omega^{C(\mathbf{a})}$. Let $H(\mathbf{a}) = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & \omega^{C(\mathbf{a})} \end{pmatrix}$. Then $H(\mathbf{a})$ is a Hadamard matrix if $p = 2$ and a generalized Hadamard matrix otherwise. We will give a construction of CNC Hadamard matrices by applying the flipping operation on the submatrices of $C(\mathbf{a})$.

Let $\mathbf{x} = (x_0, x_1, \cdots, x_{k-1})$ and R_k be the back diagonal identity matrix of order k, i.e., the entries of the back diagonal is equal to 1, and the other entries are zeros. Then $\mathbf{x}R_k = (x_{k-1}, \cdots, x_1, x_0)$, R_k is referred to as a *flipping operator*. Note that the flipping operation does not change the Hadamard property.

Construction 1. Let $\mathbf{e} = (e_0, e_1, \cdots, e_{2h-1})$ be a positive integer sequence satisfying that $\sum_{i=0}^{2h-1} e_i = N, e_i > 0$. We denote the first e_0 columns in $C(\mathbf{a})$ as

an $N \times e_0$ submatrix A_0, the second e_1 columns in $C(\mathbf{a})$ as an $N \times e_1$ submatrix A_1, and so on. Then $C(\mathbf{a}) = (A_0, A_1, \cdots, A_{2h-1})$. Let

$$E(\mathbf{a}) = \left(A_0, A_1 R_{e_1}, A_2, A_3 R_{e_3}, \cdots, A_{2h-2}, A_{2h-1} R_{e_{2h-1}}\right).$$

Note that $E(\mathbf{a})$ is resulted from $C(\mathbf{a})$ by flipping h blocks of the columns. Let $H^- = \omega^{E(\mathbf{a})}$. Then

$$H = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^{\mathbf{T}} & \omega^{E(\mathbf{a})} \end{pmatrix} \tag{1}$$

is again a Hadamard matrix.

Theorem 1. *Assume that $l(\mathbf{a}) < \frac{N}{2(4h)}$ where h is a positive integer and $l(\mathbf{a}) < e_i < N - l(\mathbf{a})$. Then any two row vectors in $\omega^{E(\mathbf{a})}$ (equivalently in $E(\mathbf{a})$) are shift distinct. Thus H, defined in (1), is a CNC Hadamard matrix.*

In order to prove Theorem 1, we need some basic properties of the linear spans of sequences and their corresponding reciprocal sequences, which are summarized below.

Property 1. Assume that $\mathbf{a} = \{a_i\}$ is a sequence over $\mathbb{F}_p$ with period N. Let $\mathbf{b} = \{b_i\}$ be the reciprocal sequence of $\mathbf{a}$, i.e., $b_0 = a_0$ and $b_i = a_{N-i}, 0 < i < N$.

(a) $l(\mathbf{a}) = l(\mathbf{b})$.
(b) $l(\mathbf{x} + L^\tau(\mathbf{x})) \le l(\mathbf{x})$ where $\mathbf{x} \in \{\mathbf{a}, \mathbf{b}\}$.
(c) $l(\mathbf{a} + L^\tau(\mathbf{b})) \le l(\mathbf{a}) + l(\mathbf{b}) \le 2\max\{l(\mathbf{a}), l(\mathbf{b})\}$.
(d) Maximum length of the runs of zeros in $\mathbf{a}$ is upper bounded by $l(\mathbf{a}) - 1$, i.e., there are at most $l(\mathbf{a}) - 1$ consecutive zeros in $\mathbf{a}$.
(e) $\mathbf{b} = L^{N-1}(\mathbf{a}R_N)$. Thus $l(\mathbf{a}R_N) = l(\mathbf{a})$.

Proof of Theorem 1. We only need to prove the row distinctness of $H^- = \omega^{E(\mathbf{a})}$, which is equivalent to the row shift-distinctness of $E(\mathbf{a})$. If there are two row vectors in $E(\mathbf{a})$, say $\mathbf{u}, \mathbf{v}$ which are shift equivalent, i.e., there is $r \ge 0$ such that $\mathbf{u} = L^r\mathbf{v}$, then $\mathbf{u} - L^r\mathbf{v} = \mathbf{0}$. According to the construction, we can consider their respective index sets of $\mathbf{u}$ and $\mathbf{v}$, each having $2h$ separating lines (including the last end point) at $\sum_{j=0}^{i} e_j$, $i = 0, \cdots, 2h-1$ and at $\sum_{j=0}^{i}(e_j + r)$, $i = 0, \cdots, 2h-1$ (recall that the index is reduced by modulo N). Note that the multi-set $Q = \{e_i, e_i + r \mid 0 \le i < 2h\}$ has at most $4h$ different elements. Therefore, $\mathbf{u} - L^r\mathbf{v}$ can be divided into at most $4h$ blocks, each of which consists of consecutive elements of one of the three types of the sequences in Table 1 where $R = R_N$, the flipping operator defined at the beginning of this section. Their respective linear spans are determined by Property 1 where we exclude the cases that the sequences are zero sequences in the first two cases in Table 1. Therefore, according to Property 1, the sequences of Types 1 and 2 have at most $l(\mathbf{a}) - 1$ consecutive zeros and the sequences of Type 3 have at most $2l(\mathbf{a}) - 1$ consecutive zeros.

Case 1: $|Q| = 4h$ and each block has the equal length, which is equal to $\frac{N}{4h}$. This is possible only when $\frac{N}{4h}$ is an integer. In this case, a block in $\mathbf{u} - L^r\mathbf{v}$

Table 1. Types of the full sequences containing the segments of $\mathbf{u} - L^r\mathbf{v}$

		Type	Linear Span
$\mathbf{a} \pm L^i(\mathbf{a})$	$0 \le i < N$	1	$l(\mathbf{a})$
$\mathbf{a}R \pm L^j(\mathbf{a}R)$	$0 \le j < N$	2	$l(\mathbf{a})$
$\mathbf{a} \pm L^k(\mathbf{a}R)$	$0 \le k < N$	3	$\le 2l(\mathbf{a})$

gives $\frac{N}{4h}$ consecutive zeros. Since $l(\mathbf{a}) < \frac{N}{8h}$, we have $2l(\mathbf{a}) - 1 < \frac{N}{4h}$, which is a contradiction.

Case 2: Each block does not have the equal length. According to the pigeon hole principle, there is at least one block with length $> \frac{N}{4h}$. Hence, this block gives more than $\frac{N}{4h}$ consecutive zeros, which is a contradiction, since there are at most $2l(\mathbf{a}) - 1$ consecutive zeros where $2l(\mathbf{a}) - 1 < \frac{N}{4h}$. □

If $h = 1$, then we can have a more refined result shown below by carefully examining patterns appeared in $\mathbf{u} - L^r\mathbf{v}$ in the proof of Theorem 1.

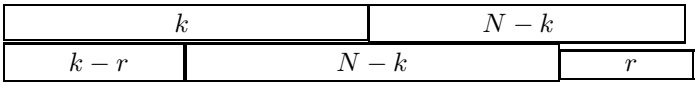
Theorem 2. *With the same notation as in Theorem 1, we assume that* $l(\mathbf{a}) < \frac{N}{4}$, $h = 1$, $\mathbf{e} = (e_0, e_1)$, *and* $3l(\mathbf{a}) < e_0 < N - 3l(\mathbf{a})$. *Then* H *is a CNC Hadamard matrix.*

Proof. We proceed as in the proof of Theorem 1 until we divide into the two cases.

We now write $e_0 = k$, so that $e_1 = N - k$. Without loss of generality, we can assume that $\mathbf{u}$ is the sequence from the first row of $E(\mathbf{a})$, and $\mathbf{v}$ is the tth row of $E(\mathbf{a})$. Since the case $k < N/2$ or $N - k < N/2$ can be processed similarly, we may assume that $t < k < N/2$.

Configuration 1: $r = k$. There are three sections which are overlapped with lengths k, $(N-k)-k$, and k added up to N. Since $k > 3l(\mathbf{a})$, then the block with length k has k consecutive zeros in $\mathbf{u} - L^r(\mathbf{v})$. On the other hand, any block in $\mathbf{u} - L^r(\mathbf{v})$ is a block in a sequence with the linear span at most $2l(\mathbf{a})$. Thus, it has at most $2l(\mathbf{a})$ consecutive zeros, which is a contradiction, since $2l(\mathbf{a}) < 3l(\mathbf{a}) < k$.

Configuration 2: $0 < r < k$ or $k < r < N - 1$. The proof of the latter case can be proceeded in the same way as the former case, so we omit it. For $0 < r < k$, we also could have $r < N-k$ or $r \ge N-k$. We will only show the case $r < N-k$ and the proof for $r \ge N - k$ is similar. Then we have four blocks with the following lengths configuration:



In details, we have the following pattern.

$$\begin{array}{rcl} \mathbf{u} & = & a_0 \ \cdots \ a_{k-1-r} \,\|\, a_{k-r} \ \cdots \ a_{k-1} \,\|\, a_{N-1} \ \cdots \ a_{k+r} \,\|\, a_{k+r-1} \ \cdots \ a_k \\ L^r(\mathbf{v}) & = & a_{t+r} \ \cdots \ a_{t+k-1} \,\|\, a_{t-1} \ \cdots \ a_{t-r} \,\|\, a_{t-1-r} \ \cdots \ a_{t+k} \,\|\, a_t \ \cdots \ a_{t+r-1} \end{array}$$

Thus the four blocks of $\mathbf{u} - L^r(\mathbf{v})$ has the following length patterns according to Table 1 in the proof of Theorem 1.

Segment	Type	Length
1	1	$k-r$
3	2	$N-k-r$
2, 4	3	r

(Note. For a different range of r, the only difference is that those blocks correspond to their respective types of sequences in a different order.)

The average length is $N/4$. The case that $N-k-r = r = k = N/4$ is possible only when $\frac{N}{4}$ is an integer. In this case, the first block gives $N/4$ consecutive zeros of Type 1 sequences with linear span $l(\mathbf{a})$. According to Property 1-(d), it has at most $l(\mathbf{a}) - 1$ consecutive zeros. From the assumption that $l(\mathbf{a}) < N/4$, we have $l(\mathbf{a}) - 1 < N/4$, which is a contradiction. Thus, we only need to consider the case that not all the blocks have the same length. According to Property 2 below we have $\mathbf{u} \nsim \mathbf{v}$.

Thus H is a CNC Hadamard matrix. □

Property 2. With the same notation in the proof of Theorem 2, let that $\mathbf{u}$ be the sequence from the first row of $E(\mathbf{a})$, and $\mathbf{v}$, the tth row of $E(\mathbf{a})$, $k < N/2$. If the lengths of the corresponding blocks in $\mathbf{u} = L^r(\mathbf{v})$ are $k-r$, r, $N-k-r$, and r respectively, which are not equal, then $\mathbf{u} \nsim \mathbf{v}$.

The proof of Property 2 is omitted here due to the lack of space. The reader is referring to the full version of this work [6].

Remark 1. The construction given in [8] (Theorem 17) can be considered as a special case of Theorem 1 when $h = 1$. However, the result given by Theorem 2 is an improvement of that result; Theorem 17 of [8] requires that $l(\mathbf{a}) < N/6$ and, here, Theorem 2 only needs that $l(\mathbf{a}) < N/4$. This bound also answered the question, addressed in [8] (Theorem 17), about whether there exists a general class when $l(\mathbf{a}) \geq N/6$.

3 CNC Property of Kronecker Products

In this section, we discuss the Kronecker product of two CNC Hadamard matrices. We then provide a construction using the Kronecker product and 2-level autocorrelation sequences in the next section. For these two sections, we will proceed the binary case for simplicity. For general p, the results are similar to the binary case, so we omit here.

For matrices $A = (a_{ij})$ and B, the *Kronecker product* of A and B, denoted $A \otimes B$, is:

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots & a_{0,n-1}B \\ a_{10}B & a_{11}B & \cdots & a_{1,n-1}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0}B & a_{n-1,1}B & \cdots & a_{n-1,n-1}B \end{pmatrix}.$$

In this section, we denote by $\tilde{\mathbf{j}}_n$ the row vector of n alternating ± 1s; that is

$$\tilde{\mathbf{j}}_n := \left(1 \; -1 \; 1 \cdots \; (-1)^{n-1}\right).$$

We may omit the subscript when the dimension of the vector is implicit. Note that a CNC Hadamard matrix does not guarantee that any two rows of the matrix are shift distinct.

Theorem 3. (Construction 2) *If A and B are Hadamard matrices such that the following are true:*

i) for any two rows of A, $\mathbf{a} = (1, \mathbf{a}^-)$ and $\mathbf{a}' = (1, \mathbf{a}'^-)$, $\mathbf{a} \nsim \pm\mathbf{a}'$ and $\mathbf{a}^- \nsim \pm\mathbf{a}'^-$,
ii) for any two rows of B, $\mathbf{b} = (1, \mathbf{b}^-)$ and $\mathbf{b}' = (1, \mathbf{b}'^-)$, $\mathbf{b} \nsim \pm\mathbf{b}'$ and $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$,
iii) the orders of A and B are both greater than 3, and
iv) $\tilde{\mathbf{j}}$ is not a row in the reduced form of A or B,

then $A \otimes B$ is CNC Hadamard matrix and its rows are also shift distinct.

From the conditions i)-ii), we know that both A and B are CNC. Theorem 3 can be seen as a direct consequence of the following lemma. Since this lemma is technical and straightforward, we will omit the proof here. The proof of Theorem 3 is given in the full version of this work [6].

For a vector

$$\mathbf{x} = \left(x_0, x_1, \cdots, x_{d-1}\right)$$

of order d, let $\mathbf{x}^-$ denote $\mathbf{x}$ with the first entry removed;

$$\mathbf{x}^- = \left(x_1, x_2, \cdots, x_{d-1}\right).$$

Lemma 1. *If $\mathbf{a}, \mathbf{a}', \mathbf{b}$ and $\mathbf{b}'$ be row vectors such that the following are true:*

i) $\mathbf{a} \nsim \pm\mathbf{a}'$ and $\mathbf{a}^- \nsim \pm\mathbf{a}'^-$, and
ii) either $\mathbf{b} \nsim \pm\mathbf{b}'$ and $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$, or $\mathbf{b} = \mathbf{b}'$.

Then $\mathbf{a} \otimes \mathbf{b} \nsim \mathbf{a}' \otimes \mathbf{b}'$ and $(\mathbf{a} \otimes \mathbf{b})^- \nsim (\mathbf{a}' \otimes \mathbf{b}')^-$

4 A Secondary Construction from the Kronecker Product and 2-Level Autocorrelation Sequences

In this section, we show a construction for CNC Hadamard matrices using the Kronecker product and 2-level autocorrelation sequences.

Let $\mathbf{u}$ and $\mathbf{v}$ be two 2-level autocorrelation sequences over $\mathbb{F}_2$ of period $N = 2^n - 1$ (they may be equal). Recall that R_N the back diagonal identity matrix of order N. Thus $\mathbf{v}R_N = (v_{N-1}, \cdots, v_1, v_0)$ is also a 2-level autocorrelation

sequence, which is a shift of the reciprocal of $\mathbf{v}$ (see Property 1). For $p = 2$, recall the following notation

$$H(\mathbf{x}) = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & (-1)^{C(\mathbf{x})} \end{pmatrix}$$

where $C(\mathbf{x})$ is the circular matrix defined in Section 2.

Construction 3. Let I_k be the identity matrix of order k. Let

$$B = \begin{pmatrix} H(\mathbf{a}) & H(\mathbf{b}P) \\ H(\mathbf{a}) & -H(\mathbf{b}P) \end{pmatrix} \text{ where } \begin{cases} P = R_N & \text{for } \mathbf{a} \sim \mathbf{b} \\ P \in \{I_N, R_N\} & \text{for } \mathbf{a} \nsim \mathbf{b}. \end{cases}$$

Let A be a ± 1 matrix of order m. We define

$$H = A \otimes B.$$

Thus, B can be considered as the case that $A = (1)$ for $m = 1$.

Theorem 4. *Assume that either both* $\mathbf{a}$ *and* $\mathbf{b}$ *are shift-distinct quadratic sequences with* $P = I_N$ *or at least one of them is not a quadratic sequence with* $l(\mathbf{a}) + l(\mathbf{b}) < 2^{n-1} - 1$. *Then* B *is a CNC Hadamard matrices with order* 2^{n+1}, *and for two rows* $\mathbf{b}$ *and* $\mathbf{b}'$ *in* B, $\mathbf{b} \nsim \pm\mathbf{b}'$ *and* $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$.

In order to prove Theorem 4, we need some properties of the quadratic residue sequences summarized in the following property.

Property 3. (a) If $\mathbf{a}$ is a binary 2-level autocorrelation sequence, then $l(\mathbf{a}) \leq 2^{n-1} - 1$. The upper bound is achieved by a quadratic residue sequence.

(b) There are only two shift-distinct quadratic residue sequences with period $N = 2^n - 1$ where N is a prime and $N \equiv 3 \pmod{N}$, say $\mathbf{a}$ and $\mathbf{b}$. Note that $\mathbf{a}$ and $\mathbf{b}$ are reciprocal. Thus, $\mathbf{b}$ can obtained from $\mathbf{a}$ by two methods, i.e., $b_0 = a_0 = 1$, and $b_i = a_i + 1$ or $b_i = a_{N-i}, i = 1, \cdots, N-1$. The crosscorrelation of $\mathbf{a}$ and $\mathbf{b}$ is bounded by 3. Thus $\mathbf{a} + L^k(\mathbf{b})$ has maximum $2^{n-1} - 3$ zeros in one period.

Proof of Theorem 4. We first need to prove the CNC property of B. However, a proof can be given in a similar way as the proof for Theorems 1- 2 where the length of zero runs in the investigated sequences are bounded by Property 3, we omit it here (the reader can find the proof in the full version of this work). Thus, B is a CNC Hadamard matrix and for any two rows $\mathbf{b}^-$ and $\mathbf{b}'^-$ in B^-, $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$. Note that if there are two rows in B which are shift equivalent, then the overlapping patterns in those two rows have the length patterns by adding 1 or subtracting 1 in the case of the reduced form of B for which the zeros and their corresponding elements are excluded. Thus, a similar argument to prove the CNC property of B can be applied to this case. Thus, for two rows $\mathbf{b}$ and $\mathbf{b}'$ in B, $\mathbf{b} \nsim - \pm \mathbf{b}'$. □

Remark 2. In [8], it is proved that B is a CNC Hadamard by using $\mathbf{b}R_N$ where $\mathbf{a}$ and $\mathbf{b}$ could be the same, and the bound for the linear span is shown to be

$l(\mathbf{a}) + l(\mathbf{b}) + \max\{l(\mathbf{a}), l(\mathbf{b})\} \leq N \Longrightarrow l(\mathbf{a}) \leq N/3$ when $l(\mathbf{a}) = l(\mathbf{b})$. The result obtained in Theorem 4 is an improvement, since if $\mathbf{a} \nsim \mathbf{b}$, we could use both $\mathbf{b}$ and $\mathbf{b}R_N$, and the bound on the linear span is larger, i.e., $l(\mathbf{a}) \leq N/2$ when $l(\mathbf{a}) = l(\mathbf{b})$. Theorem 4 also shows that if both $\mathbf{a}$ and $\mathbf{b}$ are shift-distinct quadratic residue sequences with $P = I_N$, then the result is true without imposing any conditions on the linear span of the sequences.

Theorem 5. *With the notation in Construction 3, let A be a CNC Hadamard matrix of order $m > 1$ such that $\mathbf{u} \nsim \pm\mathbf{v}$ where $\mathbf{u}$ and $\mathbf{v}$ are any two rows from A. Then $H = A \otimes B$, as constructed in Construction 3, is a CNC Hadamard matrix with order $m2^{n+1}$.*

Proof. Let $\mathbf{e}$ and $\mathbf{d}$ be two different rows in B. From Theorem 4, $\mathbf{e} \nsim \pm\mathbf{d}$. From the construction of B in Construction 3, $\tilde{\mathbf{j}}$ is not a row in B. Thus for $m > 3$ both A and B satisfy the conditions in Theorem 3. Therefore, H is a CNC Hadamard matrix. Note that if $m = 3$, there are no Hadamard matrices [2].

For $m = 2$, we have $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. In this case, $H = A \otimes B = \begin{pmatrix} B & B \\ B & -B \end{pmatrix}$. For any two rows from H^-, if they are taken from the upper half of H^-, then they are shift distinct, since any two rows in B are shift distinct (similar arguments as that in the proof of Theorem 3). If one row from the upper half of H and the other from the lower half or both from then lower half then the argument can be proceeded similarly as the proofs Theorems 1-2, we omit it here due to the lack of space.

Thus H is a CNC Hadamard matrix. □

5 Related Functions and LCZ Signal Sets

Let $q = p^n$ and $H = (\omega^{a_{ij}})$ be a CNC Hadamard matrix of order q constructed using one of the constructions in Sections 2 and 3, where ω is a pth primitive root of unity α. Let α be a primitive element in $\mathbb{F}_q$. We construct a family of functions from $\mathbb{F}_q$ to $\mathbb{F}_p$ as follows. For each $i = 0, \cdots, q-1$, let $f_i(\alpha^j) = a_{ij}, 0 \leq j < q$ and $f_i(0) = 0$ (recall H is in the normal form). Then $S = \{f_i(x) \,|\, 1 \leq i < q\}$ is a set consisting of $q - 1$ functions which satisfy the three conditions listed in Section 1-C. In addition, S has maximum size.

Let $d = (q^m - 1)/(q - 1)$. According to the work in [5], we can construct LCZ signal sets with parameters $(q^m - 1, q - 1, 1, d)$ with maximum size as follows. A function $h(x)$, from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, is said to be *difference balanced* if for any $0 \neq \lambda \in \mathbb{F}_{q^m}$ and $a \in \mathbb{F}_q$, $h(x) - h(\lambda x) = a$ has q^{m-1} solutions in $\mathbb{F}_{q^m}$. We say that $h(x)$ is $\mathbb{F}_q$-*linear* if $h(ax) = ah(x)$. Let β a primitive element in $\mathbb{F}_{q^m}$, and $h(x)$ be a function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ with the difference balance property and $\mathbb{F}_q$-linear property. Let $g_i(x) = f_i(x) \circ h(x)$, for $1 \leq i < q$ and where $\circ$ is the composition operator. Then the evaluation of $g_i(x)$ at β, denoted as $\mathbf{a}_i$, is a 2-level autocorrelation sequence over $\mathbb{F}_p$ with period $q^m - 1$. The construction for 2-level autocorrelation sequences is referred to as *a subfield decomposition construction* in [4]. Hence $\mathcal{K} = \{\mathbf{a}_i \,|\, 1 \leq i < q\}$ is an LCZ set

with parameters $(q^m - 1, q - 1, 1, d)$. (Note. Here we replace the 2-tuple balance property for $h(x)$ in [5] by the difference balance and F_q-linear.) All LCZ signal sets corresponding to CNC Hadamard matrices constructed from Construction 1 for $h > 1$, Construction 2, Construction 3 for $m > 1$ and the case employing quadratic sequences for $m = 1$, are new. In the cases from Construction 1 for $h = 1$ and Construction 3 for $m = 1$ give LCZ signal sets with the improved results.

6 Concluding Remarks

In this work, we present three new constructions for CNC Hadamard matrices. The first construction is obtained by alternating the column blocks and the flipped column blocks in the circular matrix generated by a 2-level autocorrelation sequence over $\mathbb{F}_p$. Then we have showed that the Kronecker product of two CNC Hadamard matrices A and B is still a CNC Hadamard matrix provided that the row shift-distinctness also holds in those two CNC Hadamard matrices and the alternating vector is not a row vector of either A or B. The third construction is given by a combination of the Kronecker product and the circular matrices generated by 2-level autocorrelation sequences. The first and third construction contain two known constructions in [8] as special cases, but with improved bounds for the restrictions on the linear spans of 2-level autocorrelation sequences and new cases. Note that the third known construction for CNC Hadamard matrices in the literature is presented in [5], which is not any special case of the three constructions obtained in this work.

It is worth to point out that for the binary case, there are other constructions for Hadamard matrices which also give CNC Hadamard matrices. For example, the Hadamard matrices from the Turyn construction [14,15,7] are CNC Hadamard matrices. This can be easily seen from the construction from many examples, but work is needed to write out the proof. We currently work on that. In general, the orders of those Hadamard matrices are not powers of 2. Note that the motivation for the investigation of the CNC property is for the constructions of a set consisting of 2^n functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ which satisfies that each function in the set is balanced, the sum of any two function is balanced, and any two functions, considered as sequences with period $2^n - 1$, are shift distinct. If the order of a CNC Hadamard matrix is not 2^n, then its corresponding function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is not balanced. Thus, those types of CNC Hadamard matrices cannot be used in the construction of low correlation zone sequences with parameters $(q^m - 1, q - 1, 1, \frac{q^m-1}{q-1})$ where $q = 2^n$. However, the problem itself is interesting theoretically.

Acknowledgement

The work was conducted when the first author was supported by the NSERC Undergraduate Research Scholarship in Spring 2008. The work is supported by NSERC Discovery Grant.

References

1. Chung, J.H., Yang, K.C.: Design of m-ary low correlation zone sequence sets by interleaving. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 313–321. Springer, Heidelberg (2008)
2. Craigen, R.: Hadamard matrices and designs. In: Colbourn, C.J., Dinitz, J.H. (eds.) CRC Handbook of Combinatorial Designs, pp. 370–377. CRC Press, Boca Raton (1996)
3. De Gaudenzi, R., Elia, C., Viola, R.: Bandlimited quasi-synchronous cdma: A novel satellite access technique for mobile and personal communication systems. IEEE Journal on Selected Areas in Communications 10(2), 328–343 (1992)
4. Golomb, S.W., Gong, G.: Signal design for good correlation – for wireless communication, cryptography, and radar. Cambridge University Press, Cambridge (2005)
5. Gong, G., Golomb, S.W., Song, H.Y.: A note on low-correlation zone signal sets. IEEE Trans. Inform. Theory 53(7), 2575–2581 (2007)
6. Guo, K., Gong, G.: New constructions of complete non-cyclic hadamard matrices, related function families and lcz sequences. Technical Report, University of Waterloo, CACR 2010-14 (2010)
7. Holzmann, W.H., Kharaghani, H., Tayfeh-Rezaie, B.: Williamson matrices up to order 59. Des. Codes Cryptography 46(3), 343–352 (2008)
8. Jang, J.W., No, J.S., Chung, H.B., Tang, X.H.: New sets of optimal p-ary low-correlation zone sequences. IEEE Transactions on Information Theory 53(2), 815–821 (2007)
9. Kim, S.H., Jang, J.W., No, J.S., Chung, H.B.: New constructions of quaternary low correlation zone sequences. IEEE Transactions on Information Theory 51(4), 1469–1477 (2005)
10. Kim, Y.S., Jang, J.W., No, J.S., Chung, H.B.: New design of low-correlation zone sequence sets. IEEE Transactions on Information Theory 52(10), 4607–4616 (2006)
11. Long, B., Zhang, P., Hu, J.: A generalized qs-cdma system and the design of new spreading codes. IEEE Trans. Veh. Technol. 47(6), 1268–1275 (1998)
12. Tang, X.H., Fan, P.Z.: A class of pseudonoise sequences over gf(p) with low correlation zone. IEEE Transactions on Information Theory 47(4), 1644–1649 (2001)
13. Tang, X.H., Udaya, P.: New recursive construction of low correlation zone sequences. In: Proceedings of Second Int. Workshop Sequence Design and Its Applications to Communication, Shimonoseki, Japan, October 10-14 (2005)
14. Turyn, R.J.: An infinite class of williamson matrices. J. Comb. Theory, Ser. A 12(3), 319–321 (1972)
15. Turyn, R.J.: Hadamard matrices, baumert-hall units, four-symbol sequences, pulse compression, and surface wave encodings. J. Comb. Theory, Ser. A 16(3), 313–333 (1974)
16. Zhou, Z.C., Tang, X.H., Gong, G.: A new class of sequences with zero or low correlation zone based on interleaving technique. IEEE Trans. Inform. Theory 54(9), 4267–4273 (2008)

$\mathbb{Z}_4$-Nonlinearity of a Constructed Quaternary Cryptographic Functions Class

Zoubida Jadda[1,2] and Patrice Parraud[3]

[1] INSA de Rennes, IRMAR, F-35000, France
Zoubida.Jadda@insa-rennes.fr
[2] CNRS, UMR 6625, F-35000, France
[3] MACCLIA-CREC, Saint Cyr-Coëtquidan
patrice.parraud@st-cyr.terre-net.defense.gouv.fr

Abstract. New results on quaternary ($\mathbb{Z}_4 = \{0, 1, 2, 3\}$-valued) cryptographic functions are presented. We define and characterize completely the $\mathbb{Z}_4$-balancedness and the $\mathbb{Z}_4$-nonlinearity according the HAMMING metric and the LEE metric. In the particular case of quaternary Bent functions we show that the maximal nonlinearity of these functions is bounded for the HAMMING metric and we give the exact value of the maximal nonlinearity of these functions for the LEE metric. A general construction, based on Galois ring is detailed and applied to obtain a class of balanced and high nonlinearity quaternary cryptographic functions. We use Gray map to derive these constructed quaternary functions to obtain balanced boolean functions having high nonlinearity.

Keywords: quaternary functions, boolean functions, cryptographic functions, nonlinearity, balancedness, quaternary algebra, Gray map, Galois ring.

1 Introduction

Boolean ($\{0, 1\}$-valued) functions of length n used in pseudo-random generators of stream and blocks ciphers play an important role in their security ([7,1]). These functions are usually studied over the finite field of two elements $\mathbb{F}_2$. Finding boolean functions with optimal cryptographic properties as balancedness and high nonlinearity is still an open problem. The purpose of this paper is to present new results on quaternary ($\{0, 1, 2, 3\}$-valued) cryptographic functions. This work is motivated by the interest of studying quaternary objects and structures (see [8,12]). The usual metric used in $\mathbb{Z}_4$ is the LEE metric which allows to have an isometry from ($\mathbb{Z}_4^m$, LEE distance) to ($\mathbb{F}_2^{2m}$, HAMMING distance) with the Gray map. We begin by defining and characterizing exactly quaternary cryptographic functions of length m. Then, we formally describe balancedness and nonlinearity over $\mathbb{Z}_4$ according the HAMMING metric and the LEE metric. Quaternary Bent functions [19] (or more generaly q-ary Bent functions [3,9,10,11]) are defined by Walsh transform. For m-variables quaternary Bent functions we prove that the maximal nonlinearity is bounded between $3 \cdot 4^{m-1} - 2^{m-1}$ and

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 270–283, 2010.

$3 \cdot 4^{m-1} - 2^{m-2}$ under the HAMMING metric and we give conditions to reach the upper bound. We show the the exact value of the maximal nonlinearity of these functions under the LEE metric is $4^{m-1} - 2^{m+1}$. A general construction of quaternary cryptographic functions is detailed, using cyclotomic classes of the multiplicative group of a Galois ring R. We point out the fact that the balancedness and the nonlinearity of the obtained functions depend on the b_polynomial used to construct R and on the distribution of theses classes over R. We naturally apply this construction to a particular configuration in order to obtain a class of m-variables quaternary cryptographic functions which are balanced and have nonlinearity bounded between $3 \cdot 4^{m-1} - 2^m$ and $3 \cdot 4^{m-1} - 2^{m-1}$ for the HAMMING metric and bounded between $4^m - 2^{m+1}$ and $4^m - 2^m$ for the LEE metric. Using the Gray map with these obtained quaternary functions we present $2m-$variables balanced boolean functions with high nonlinearity. To avoid any confusion, a n-variables boolean function is denoted by f while a m-variables quaternary function is denoted by F .

2 Boolean Functions Basics

Let n be a natural integer and $\mathbb{F}_2^n$ the set of all n-tuples of elements in the finite field $\mathbb{F}_2 = \{0, 1\}$ with its sum denoted by $\oplus$. A n-variables boolean function f is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ which can be identified by its truth table $[f(0, \cdots, 0), \cdots, f(1, \cdots, 1)]$ of length 2^n. The support of f is defined by $supp(f) = \{u \in \mathbb{F}_2^n \mid f(u) \neq 0\}$ and the Hamming weight $w_H(f)$ of f by the size of its support. The Hamming distance between two n-variables boolean functions f and g is $d_H(f, g) = w_H(f \oplus g)$ where $\oplus$ denotes the addition on $\mathbb{F}_2$. The Walsh transform of a n-variables boolean function f is the complex mapping from $\mathbb{F}_2^n$ to $\mathbb{C}$ defined by $W_f(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{u \cdot v + f(v)}$ where $u \cdot v$ denotes the usual inner product in $\mathbb{F}_2^n$. A n-variables boolean function f is balanced if its truth table contains a equal number of 1's and 0's which means that $w_H(f) = 2^{n-1}$ or in spectral term $W_f(0) = 0$. The nonlinearity of a n-variables boolean function f is the minimum distance to all affine functions $nl_2(f) = \min_{g \ affine} d_H(f, g)$. Using the Walsh transform, the nonlinearity of f can be expressed by $nl_2(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)|$. Readers can refer to [5,6,16] for more detailed explanations of boolean functions cryptographic criteria. For every n-variables boolean function f, we have $nl_2(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. This bound is reached for Bent functions [17,14] which are characterised by $\forall u \in \mathbb{F}_2^n, \quad |W_f(u)| = 2^{\frac{n}{2}}$ for n even. A Bent function could not be balanced. Finding maximal nonlinearity boolean functions (see [13,15,18]) is an open problem.

3 Quaternary Cryptographic Functions

3.1 Quaternary Tools

Throughout this section i will denote the complex number such that $i^2 = -1$. Let $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ be the ring of integers modulo 4 which is

group-isomorphic to $\mathbb{U}_4 = \{\pm 1, \pm i\}$ the group of 4^{th} root of unity in $\mathbb{C}$ under the standard isomorphism $x \to i^x$. $\mathbb{Z}_4^m$ will represents the set of all $m-$tuples of elements in $\mathbb{Z}_4$ where m is a natural integer. The addition on $\mathbb{Z}_4$ (addition (mod 4)) will denoted by $+$. The LEE weights w_L of $0, 1, 2, 3$ in $\mathbb{Z}_4$ are $0, 1, 2, 1$ respectively and the LEE weight $w_L(u)$ of an element u of $\mathbb{Z}_4^m$ is the rationnal sum of the LEE weight of its components. The LEE distance $d_L(u, v)$ between two elements u and v in $\mathbb{Z}_4^m$ is $w_L(u + v)$.

Definition 1. *A m-variables quaternary function F is a function from $\mathbb{Z}_4^m$ to $\mathbb{Z}_4$ which can be identified by its truth table $[F(0, \cdots, 0), \cdots, F(3, \cdots, 3)]$ of length 4^m. Let us define $\mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$ as the set of all m-variables quaternary functions.*

The support of F is defined by $supp(F) = \{u \in \mathbb{Z}_4^m \mid F(u) \neq 0\}$. We define the relative support of F by $supp_j(F) = \{u \in \mathbb{Z}_4^m \mid F(u) = j\}$ for all j in $\mathbb{Z}_4$ and $\eta_j(F)$ its size. The HAMMING weight $w_H(F)$ of F is the size of its support and the HAMMING distance between two m-variables quaternary functions F and G is $d_H(F, G) = w_H(F - G)$. The LEE weight $w_L(F)$ of F is $\eta_1(F) + \eta_3(F) + 2\eta_2(F)$ and the LEE distance between two m-variables quaternary functions F and G is $d_L(F, G) = w_L(F - G)$. The Walsh transform of a m-variables quaternary function F is the complex mapping from $\mathbb{Z}_4^m$ to $\mathbb{C}$ defined by $W_F(u) = \sum_{v \in \mathbb{Z}_4^m} i^{u \cdot v + F(v)}$ where $u \cdot v$ denotes the usual inner product in $\mathbb{Z}_4^m$ (mod 4) . We define $W_F^2(u) = \sum_{v \in \mathbb{Z}_4^m} (-1)^{u \cdot v + F(v)}$ and $W_F^3(u) = \sum_{v \in \mathbb{Z}_4^m} (-i)^{u \cdot v + F(v)}$

3.2 Quaternary Balancedness and Nonlinearity

Definition 2 (Balancedness). *Let $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$.*

$$F \text{ is balanced } \iff \forall j \in \mathbb{Z}_4,\ \eta_j(F) = 4^{m-1}.$$

Let us give a balancedness characterisation of quaternary function.

Proposition 1. *Let $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$.*

$$F \text{ is balanced } \iff W_F(0) = W_F^2(0) = 0.$$

Proof. By definition we have $W_F(0) = \sum_{v \in \mathbb{Z}_4^m} i^{F(v)}$ and $W_F^2(0) = \sum_{v \in \mathbb{Z}_4^m} (-1)^{F(v)}$, then $W_F(0) = \eta_0(F) - \eta_2(F) + i(\eta_1(F) - \eta_3(f))$ and $W_F^2(0) = \eta_0(F) - \eta_1(F) + \eta_2(F) - \eta_3(F)$. These Two equalities give us 3 equations on η_j $(0 \leq j \leq 3)$ by extracting real and imaginary parts. Since $\sum_{j \in \mathbb{Z}_4} \eta_j(F) = 4^m$ we then obtain a system of 4 simultaneous equations in 4 unknowns that we solve. This finishes the proof. □

Similary to binary case, we define the nonlinearity of quaternary function.

Definition 3 (Nonlinearity). *Let $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$. The nonlinearity of F is defined by the minimum distance to all affine functions with*

$nl_4^H(F) = \min_{G\ affine} d_H(F,G)$ *under the* HAMMING *metric and with* $nl_4^L(F) = \min_{G\ affine} d_L(F,G)$ *under the* LEE *metric.*

Go on with a nonlinearity characterisation of quaternary function.

Proposition 2. *Let* $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$*. The nonlinearity of* F *under the* HAMMING *metric is completely characterised by*

$$\begin{aligned} nl_4^H(F) &= 3\cdot 4^{m-1} - \frac{1}{4}\max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\left\{2Re(i^b\,W_F(a)) + (-1)^b\,W_F^2(2a)\right\} \\ &= 3\cdot 4^{m-1} - \\ &\quad -\frac{1}{4}\max_{a\in\mathbb{Z}_4^m}\left\{2\mid Re(\,W_F(a))\mid + W_F^2(2a), 2\mid Im(\,W_F(a))\mid - W_F^2(2a)\right\} \end{aligned}$$

where $Re(z)$ *and* $Im(z)$ *denote respectively the real and imaginary part of the complex* z*.*

Proof. By Definition 3, we have

$$nl_4^L(F) = \min_{G\ affine} d_H(F,G) = \min_{G\ affine} w_H(F-G)$$

Let S be the function in $\mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$ such that $S(u) = F(u) + a\cdot u + b$ with a in $\mathbb{Z}_4^m$ and b in $\mathbb{Z}_4$.

$$\begin{aligned} nl_4^H(F) &= \min_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\{\eta_1(S) + \eta_2(S) + \eta_3(S)\} \\ &= 4^m - \max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\eta_0(S). \end{aligned}$$

Using the decomposition of $W_S(0)$, $W_S^2(0)$, $W_S^3(0)$ and the fact that $\eta_0(S) + \eta_1(S) + \eta_2(S) + \eta_3(S) = 4^m$ we obtain

$$\begin{aligned} \eta_0(S) &= \frac{1}{4}\left[4^m + W_S(0) + W_S^2(0) + W_S^3(0)\right] \\ &= \frac{1}{4}\left[4^m + \sum_{u\in\mathbb{Z}_4^m}\left(i^{F(u)+a\cdot u+b} + (-1)^{F(u)+a\cdot u+b} + (-i)^{F(u)+a\cdot u+b}\right)\right] \\ &= \frac{1}{4}\left[4^m + i^b\,W_F(a) + (-1)^b\,W_F^2(2a) + \overline{i^b\,W_F(a)}\right] \\ &= \frac{1}{4}\left[4^m + 2Re(i^b\,W_F(a)) + (-1)^b\,W_F^2(2a)\right]. \end{aligned}$$

The proof is completed, the second expression of $nl_4^H(F)$ is obvious using properties of complex numbers. □

Proposition 3. *Let* $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$*. The nonlinearity of* F *under the* LEE *metric is completely characterised by*

$$\begin{aligned} nl_4^L(F) &= 4^m - \max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4}\left\{Re(i^b\,W_F(a))\right\} \\ &= 4^m - \max_{a\in\mathbb{Z}_4^m}\{\mid Re(\,W_F(a))\mid, \mid Im(\,W_F(a))\mid\}. \end{aligned}$$

Proof. By Definition 3, we have

$$nl_4^L(F) = \min_{G\ affine} d_L(F,G) = \min_{G\ affine} w_L(F-G).$$

Let S be the function in $\mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$ such that $S(u) = F(u) + a \cdot u + b$ with a in $\mathbb{Z}_4^m$ and b in $\mathbb{Z}_4$.

$$nl_4^L(F) = \min_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4} \{\eta_1(S) + 2\eta_2(S) + \eta_3(S)\}.$$

Using the decomposition of $W_S(0)$ and $W_S^3(0)$ we have

$$W_S(0) + W_S^3(0) = 2(\eta_0(S) - \eta_2(S)).$$

Moreover

$$W_S(0) + W_S^3(0) = 2Re(i^b W_F(a)).$$

As $\sum_{j\in\mathbb{Z}_4} \eta_j(S) = 4^m$, we obtain

$$\eta_1(S) + 2\eta_2(S) + \eta_3(S) = 4^m + \eta_2(S) - \eta_0(S).$$

That is

$$\begin{aligned} nl_4^L(F) &= \min_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4} \{4^m + \eta_2(S) - \eta_0(S)\} \\ &= 4^m - \max_{a\in\mathbb{Z}_4^m, b\in\mathbb{Z}_4} \left\{Re(i^b W_F(a))\right\} \end{aligned}$$

which ends the proof of the first expression. The second expression of $nl_4^L(F)$ is obvious by properties of complex numbers. □

3.3 Quaternary Bent Functions Properties

Definition 4 (Quaternary Bent functions). *Let F be a m-variables quaternary function. F is Bent if and only if $|W_F(a)| = 2^m$, for any $a \in \mathbb{Z}_4^m$.*

Remark 1. A classical result gives $W_F(a) = \pm 2^m$ or $W_F(a) = \pm i 2^m$.

Let us now focus on the maximal nonlinearity of a m-variables quaternary Bent function F according to the Hamming metric and the Lee metric respectively as shown in Fig.1.

Theorem 1. *Let F be a m-variables Bent function.*

(1) $3 \cdot 4^{m-1} - 2^{m-1} \leq nl_4^H(F) \leq 3 \cdot 4^{m-1} - 2^{m-2}$.
(2) $nl_4^H(F) = 3 \cdot 4^{m-1} - 2^{m-2}$ *if and only if* $W_F^2(2a) = \pm 2^m$.

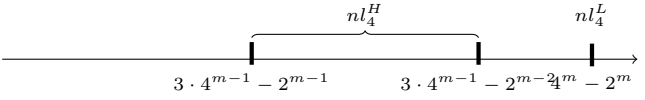


Fig. 1. Nonlinearity of Quaternary Bent function

Proof

(1): Proposition 2 gives

$$nl_4^H(F) = 3 \cdot 4^{m-1} - \\ -\frac{1}{4} \sup_{a \in \mathbb{Z}_4^m} \left\{ 2 \mid Re(W_F(a)) \mid + W_F^2(2a), 2 \mid Im(W_F(a)) \mid - W_F^2(2a) \right\}.$$

Let us write $nl_4^H(F) = 3 \cdot 4^{m-1} - \frac{1}{4}y$
where $y = \sup_{a \in \mathbb{Z}_4^m} \left\{ 2 \mid Re(W_F(a)) \mid + W_F^2(2a), 2 \mid Im(W_F(a)) \mid - W_F^2(2a) \right\}$
and $x = W_F^2(2a) = \sum_{u \in \mathbb{Z}_4^m} (-1)^{a.u} (-1)^{F(u)}$.
As F is bent, we use Remark 1 to distinguish two main cases in order to evaluate y (let c=2^{m+1}):

- $W_F(a) = \pm 2^m : y = Max\{c + x, -x\}$
- $W_F(a) = \pm i 2^m : y = Max\{x, c - x\}$

The geometric representation of y in terms of x (Fig. 2) shows that y ranges between 2^m and 2^{m+1} which achieves the proof.

(2): Let $nl_4^H(F) = 3 \cdot 4^{m-1} - 2^{m-2}$. If $W_F(a)$ is real then $2^m = \sup_{a \in \mathbb{Z}_4^m} \left\{ 2^{m+1} + W_F^2(2a), -W_F^2(2a) \right\}$. In this case $W_F^2(2a) < 0$ and $W_F^2(2a)$ is equal to -2^m or $2^{m+1} + W_F^2(2a) = 2^m$ that is $W_F^2(2a) = 2^m - 2^{m+1} = -2^m$. The case $W_F(a)$ is imaginary is similar. □

Theorem 2. *Let F be a m-variables Bent function.*

$$nl_4^L(F) = 4^m - 2^m.$$

Proof. Proposition 3 gives $nl_4^L(F) = 4^m - \max_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{ Re(i^b W_F(a)) \right\}$.
Using remark 1 we have $Re(i^b W_F(a)) = \pm 2^m$ which finishes the proof. □

4 Galois Rings and Cyclotomic Classes

In this section we give definitions and properties of the Galois ring $GR(4, m)$ without proofs. We refer the reader to [20] and [8] for further informations about Galois rings.

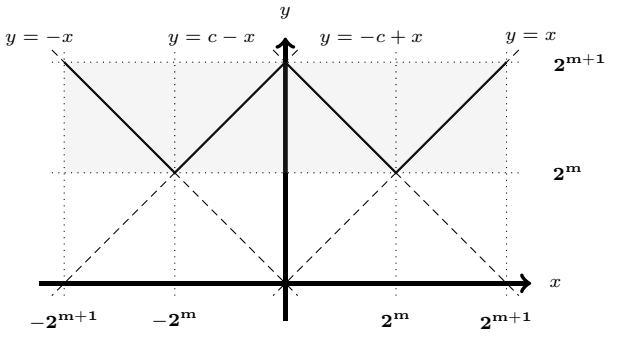


Fig. 2. y in terms of x

4.1 Galois Rings

As usual, $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ is the ring of integers modulo 4 and $\mathbb{F}_2$ the finite field with two elements. Let $\mu : \mathbb{Z}_4 \to \mathbb{F}_2$ be the mod-2 reduction map. We extend μ to $\mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ in the natural way. A monic polynomial $h(x)$ in $\mathbb{Z}_4[x]$ of degree m is said to be basic irreducible if $h_2(x) = \mu(h(x))$ is a monic irreducible primitive divisor of $x^{2^m-1} - 1$ in $\mathbb{F}_2[x]$ (Hensel lift). The Galois ring $R = GR(4, m)$ of 4^m elements is a Galois extension of order m of $\mathbb{Z}_4$ and is isomorphic to the factor ring $\mathbb{Z}_4[x]/(h(x))$ where $h(x)$ is a monic basic irreducible polynomial of degree m (b-polynomial). Let β be a root of $h(x)$ of order $2^m - 1$ ($\beta^{2^m-1} - 1 = 0$). Then R is the polynomial ring $\mathbb{Z}_4[\beta]$ where $\{1, \beta, \cdots, \beta^{m-1}\}$ is a basis of R over $\mathbb{Z}_4$. The Galois ring R is a local ring having a unique maximal ideal $D = 2R$ made up of the 2^m zero divisors. The residue class field $K = R/D$ is isomorphic to the finite field $\mathbb{F}_{2^m}$ under the canonical map $z \mapsto \bar{z}$ from R to K. The Teichmüller system $\mathcal{T} = \{0, 1, \beta, \cdots, \beta^{2^m-2}\}$ is the set of roots of $x^{2^m} - x$ in R and can be view as the set of representatives of K as $D = 2R = 2\mathcal{T}$. Let $\theta = \bar{\beta}$ be a primitive root of $h_2(x)$ in $\mathbb{F}_2[x]$, we can identify K with $\mathbb{F}_{2^m} = \overline{\mathcal{T}} = \{0, 1, \theta, \cdots, \theta^{2^m-2}\}$. The multiplicative group $R^\star = R \setminus D$ of R is a group of order $(2^m - 1)2^m$ which is the direct product $\mathcal{H} \times \mathcal{U}$ where $\mathcal{H}$ is the cyclic group of order $(2^m - 1)$ generated by β and $\mathcal{U}$ is the abelian group of principal units of R of order 2^m that is elements of the form $1 + 2z_0$ with z_0 in $\mathcal{T}$. There are two canonical ways to represent the 4^m elements of R, a multiplicative one and a additive one. In the multiplicative representation, every element z of R has a unique expansion $z = z_1 + 2z_2$ with z_1 and z_2 in $\mathcal{T}$.

4.2 Cyclotomic Classes

Let $R = GR(4, m)$ be the Galois ring of 4^m elements, $D = \{0, 2, 2\beta, \cdots, 2\beta^{2^m-2}\}$ the set of zero divisors with $\mid D \mid = 2^m$ and $R^\star = \{z_1(1 + 2z_0),\ z_0 \in \mathcal{T}, z_1 \in \mathcal{T} \setminus \{0\}\}$ the multiplicative group of R with $\mid R^\star \mid = 2^m(2^m - 1)$.

Definition 5. *Let m be a natural integer and $R = GR(4, m)$ be the Galois ring of 4^m elements and $R^\star$ its multiplicative group. The 2^m cyclotomic classes of order $2^m - 1$ of $R^\star$ are:*

$C_k = \{\beta^j + 2\beta^k,\ 0 \leq j \leq 2^m - 2\}$ *for any k such that $0 \leq k \leq 2^m - 2$ and* $C_{2^m-1} = \{\beta^j,\ 0 \leq j \leq 2^m - 2\}$.

5 Construction

Let $R = GR(4, m)$ be the Galois ring of 4^m elements and D the set of zero divisors of R. Let us consider the 2^m cyclotomic classes C_k of order $2^m - 1$ of $R^\star$ (see Proposition 5).

We construct the quaternary function F such that the function F takes the same value for each element of C_k.

We now compute formally the expressions of W_F and W_F^2 for this constructed function F. We have

$$\begin{cases} C_k & = \{\beta^j + 2\beta^k,\ 0 \leq j \leq 2^m - 2\},\ 0 \leq k \leq 2^m - 2 \\ \\ C_{2^m-1} & = \{\beta^j,\ 0 \leq j \leq 2^m - 2\} \end{cases}$$

with $\mid C_{k,\ 0 \leq k \leq 2^m-1} \mid = 2^m - 1$ and $D = \{0\} \cup \{2\beta^j,\ 0 \leq j \leq 2^m - 2\}$
Let a in $\mathbb{Z}_4^m$.

$$W_F(a) = \underbrace{\sum_{v \in D} i^{a \cdot v + F(v)}}_{S_D(a)} + \sum_{0 \leq k \leq 2^m - 2} \underbrace{\left(\sum_{v \in C_k} i^{a \cdot v + F(v)} \right)}_{S_{C_k}(a)} + \underbrace{\sum_{v \in C_{2^m-1}} i^{a \cdot v + F(v)}}_{S_{C_{2^m-1}}(a)}$$

$$W_F(a) = S_D(a) + \sum_{0 \leq k \leq 2^m - 2} S_{C_k}(a) + S_{C_{2^m-1}}(a) \tag{1}$$

As $D = \{0, 2, 2\beta, \cdots, 2\beta^{2^m-2}\}$ we have

$$S_D(a) = i^{F(0)} + \sum_{0 \leq k \leq 2^m - 2} (-1)^{a \cdot \beta^k} i^{F(2\beta^k)} \tag{2}$$

If $v \in C_k$ for $0 \leq k \leq 2^m - 2$ then $v = \beta^j + 2\beta^k$ with $0 \leq j \leq 2^m - 2$ and

$$S_{C_k}(a) = (-1)^{a \cdot \beta^k} \sum_{0 \leq j \leq 2^m - 2} i^{a \cdot \beta^j} i^{F(\beta^j + 2\beta^k)} \tag{3}$$

If $v \in C_{2^m-1}$ then $v = \beta^j$ for $0 \leq j \leq 2^m - 2$ and

$$S_{C_{2^m-1}}(a) = \sum_{0 \leq j \leq 2^m - 2} i^{a \cdot \beta^j} i^{F(\beta^j)} \tag{4}$$

In equations (2),(3) and (4), terms of the form $(-1)^{a \cdot \beta^k}$ and $i^{a \cdot \beta^j}$ show that $W_F(a)$ depends on the b_polynomial used to construct the Galois ring and terms

of the form $i^{F(2\beta^k)}$, $i^{F(\beta^j+2\beta^k)}$ and $i^{F(\beta^j)}$ show that $W_F(a)$ depends on the way that F takes value on the different cosets $C_{k,\ 0\leq k\leq 2^m-1}$ and D.

As the construction states that for a given class C_k, the function F takes the same value, if $v=\beta^j+2\beta^k\in C_k$ then let us define $F_k=F(v)=F(\beta^j+2\beta^k)$ which does not depend on j.

$$\begin{aligned} W_F(a) &= S_D(a)+\sum_{0\leq k\leq 2^m-2}\big((-1)^{a\cdot\beta^k}i^{F_k}\sum_{0\leq j\leq 2^m-2}i^{a\cdot\beta^j}\big)+i^{F_{2^m-1}}\sum_{0\leq j\leq 2^m-2}i^{a\cdot\beta^j}\\ &= S_D(a)+\big(\sum_{0\leq j\leq 2^m-2}i^{a\cdot\beta^j}\big)\big(\sum_{0\leq k\leq 2^m-2}(-1)^{a\cdot\beta^k}i^{F_k}+i^{F_{2^m-1}}\big)\end{aligned}$$

We have now to distinguish the case $a\in D$ from the case $a\notin D$.

$\underline{a\in D}$

Let $a=2\beta^l$ with $0\leq l\leq 2^m-2$ or $a=0$.

$$W_F(0)=\sum_{v\in D}i^{F(v)}+(2^m-1)\sum_{0\leq k\leq 2^m-1}i^{F_k} \tag{5}$$

$$W_F(a)=\sum_{v\in D}i^{F(v)}+\left(\sum_{0\leq j\leq 2^m-2}(-1)^{\beta^l\cdot\beta^j}\right)\left(\sum_{0\leq k\leq 2^m-1}i^{F_k}\right) \tag{6}$$

$\underline{a\notin D}$

Let $a=\beta^s+2\beta^l$ in C_l for $0\leq l\leq 2^m-2$ and for $l=2^m-1$ we have $a=\beta^s$ with $0\leq s\leq 2^m-2$.

Furthermore : $(-1)^{a\cdot\beta^k}=(-1)^{\beta^s\cdot\beta^k}$ and $i^{a\cdot\beta^j}=\begin{cases} i^{\beta^s\cdot\beta^j}(-1)^{\beta^l\cdot\beta^j}\\ i^{\beta^s\cdot\beta^j}\end{cases}$

That is

$$W_F(a)=S_D(s)+A(s,l)\left(B(s)+i^{F_{2^m-1}}\right) \tag{7}$$

where

$$S_D(s)=i^{F(0)}+\sum_{0\leq k\leq 2^m-2}(-1)^{\beta^s\cdot\beta^k}i^{F(2\beta^k)} \tag{8}$$

$$A(s,l)=\sum_{0\leq j\leq 2^m-2}(-1)^{\beta^l\cdot\beta^j}i^{\beta^s\cdot\beta^j} \tag{9}$$

$$B(s)=\sum_{0\leq k\leq 2^m-2}(-1)^{\beta^s\cdot\beta^k}i^{F_k} \tag{10}$$

$$A(s,\infty)=\sum_{0\leq j\leq 2^m-2}i^{\beta^s\cdot\beta^j} \tag{11}$$

We have that $S_D(s)$ and $B(s)$ do not depend on the class of a but only on values of F and $A(s,l)$ depends only on a but not on values of F. Moreover, we have

$$W_F^2(2a)=\sum_{v\in\mathbb{Z}_4^m}(-1)^{a.v}(-1)^{F(v)}=\sum_{v\in D}(-1)^{F(v)}+\sum_{0\leq k\leq 2^m-1}\left(\sum_{v\in C_k}(-1)^{a\cdot v+F(v)}\right)$$

As for the calculation of $W_F(a)$, we find that

$$W_F^2(2a) = \sum_{v \in D} (-1)^{F(v)} + \sum_{0 \le k \le 2^m - 1} (-1)^{F_k} \sum_{0 \le j \le 2^m - 2} (-1)^{a.\beta^j} \tag{12}$$

Equations (6) and (7) give the exact value of $W_F(a)$ and (12) the exact value of $W_F^2(2a)$ according to the detailed calculation done by equations (1)-(5) and (8)-(11).

Proposition 4 (Balancedness of F). *The balancedness of F depends on the way that F takes value on the different cosets C_k and D.*

Proof. $W_F(0) = \sum_{v \in \mathbb{Z}_4^m} i^{F(v)}$ and $W_F^2(0) = \sum_{v \in \mathbb{Z}_4^m} (-1)^{F(v)}$. □

Proposition 5 (Nonlinearity of F). *The nonlinearity of F under the* Hamming *and* Lee *metric depends on the choice of the b_polynomial and the way that F takes value according to u belongs to C_k or D.*

Proof. Using Proposition 2 and Proposition 3 and the above formal expressions of W_F and W_F^2, the result holds. □

We have seen that the nonlinearity of our quaternary function F depends on the chosen b_polynomial the distribution of F over the cyclotomic classes and C_k and D.

We now apply these results to a particular configuration in order to obtain a balanced quaternary function with high nonlinearity under the Hamming metric and Lee metric as shown in Fig. 3 and Fig. 4 respectively.

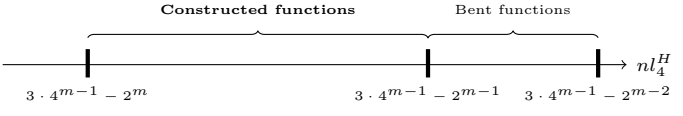


Fig. 3. Constructed Quaternary function nonlinearity nl_4^H

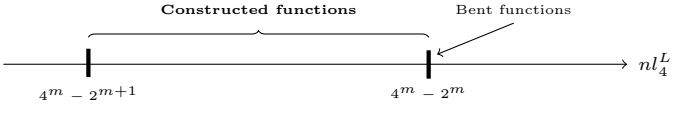


Fig. 4. Constructed Quaternary function nonlinearity nl_4^L

Proposition 6. *For k, $0 \le k \le 2^m - 2$ and for $\gamma \in \{0, 1, 2, 3\}$, we define $\delta_k = \gamma$ if $k \equiv \gamma \pmod 4$. With a suitable b_polynomial, we construct a m-variables quaternary function F as follows: $F(\beta^j + 2\beta^k) = F(2\beta^k) = \delta_k$ and $F(0) = 3$, for j, $0 \le j \le 2^m - 2$. This quaternary function is balanced and its nonlinearity under the* Hamming *metric satisfies $3 \cdot 4^{m-1} - 2^m \le nl_4^H(F) \le 3 \cdot 4^{m-1} - 2^{m-1}$ and its nonlinearity under the* Lee *metric satisfies $4^m - 2^{m+1} \le nl_4^L(F) \le 4^m - 2^m$.*

Proof. As we have 2^m classes of order 2^m-1 and $\mid D \mid = 2^m$ then by construction $\eta_0(F) = \eta_2(F) = \eta_1(F) = \eta_3(F) = 2^{2m-2}$ which proves that F is balanced.

By Proposition 2 the nonlinearity under the HAMMING metric of a m-variables quaternary function F is

$$nl_4^H(F) = 3 \cdot 4^{m-1} - \tfrac{1}{4} \sup_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{ 2Re(i^b W_F(a)) + (-1)^b W_F^2(2a) \right\}.$$

As F is balanced we have $W_F^2(2a) = 0$ by Equation (12) and then

$$nl_4^H(F) = 3 \cdot 4^{m-1} - \tfrac{1}{4} \max_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{ 2Re(i^b W_F(a)) \right\}.$$

But $\max\limits_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{ 2Re(i^b W_F(a)) \right\} = \max\limits_{a \in \mathbb{Z}_4^m} \{ 2 \mid Re(W_F(a)) \mid, 2 \mid Im(W_F(a)) \mid \}.$

Reasoning similarly to the proof of Theorem 1 with $x = W_F(a)$, the result holds.

By Proposition 3 the nonlinearity under the LEE metric of a m-variables quaternary function F is

$$nl_4^L(F) = 4^m - \max_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{ Re(i^b W_F(a)) \right\}$$

But $\max\limits_{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4} \left\{ Re(i^b W_F(a)) \right\} = \max\limits_{a \in \mathbb{Z}_4^m} \{ \mid Re(W_F(a)) \mid, \mid Im(W_F(a)) \mid \}$

Similarly as above the result holds. □

Numerical Results (Prop. 6)
Nonlinearity under the HAMMING metric $nl_4^H(F)$ and the LEE metric $nl_4^L(F)$ of constructed balanced quaternary m-variables functions F with Nbp the number of possible b_polynomials, Nbs the number of suitable b_polynomials and $B_1^H = 3 \cdot 4^{m-1} - 2^m$, $B_2^H = 3 \cdot 4^{m-1} - 2^{m-1}$, $B_1^L = 4^m - 2^{m+1}$ and $B_2^L = 4^m - 2^m$.

m	Nbp	Nbs	*suitable b_polynomial*	B_1^H	$\mathbf{nl_4^H(F)}$	B_2^H	B_1^L	$\mathbf{nl_4^L(F)}$	B_2^L
3	2	2	$x^3 + 2x^2 + x + 3$	40	**44**	44	48	**56**	56
4	2	2	$x^4 + 2x^2 + 3x + 1$	176	**180**	184	224	**232**	240
5	6	6	$x^5 + 3x^2 + 2x + 3$	736	**744**	752	960	**976**	992
6	6	2	$x^6 + x^5 + x^4 + 2x^2 + 3x + 1$	3008	**3032**	3040	3968	**4016**	4032
7	18	14	$x^7 + 2x^4 + x + 3$	12160	**12208**	12224	16128	**16224**	16256
8	16	2	$x^8 + 3x^5 + x^3 + 2x^2 + 3x + 1$	48896	**49008**	49024	65024	**65248**	65280
9	48	10	$x^9 + 2x^6 + 2x^5 + 3x^4 + x^3 + 3$	196096	**196288**	196352	261120	**261504**	261632

6 Derived Boolean Functions

Let $R = GR(4, m)$ be the Galois ring of 4^m elements and D the set of zero divisors of R. Let us consider the m-variables quaternary function F obtained with the construction which uses the 2^m cyclotomic classes of order $2^m - 1$ of $R^\star$. By taking the binary images of F under the Gray map, we obtain $n = 2m$-variables boolean functions which are balanced and having high nonlinearity.

Definition 6. *The Gray map ϕ is defined from $\mathbb{Z}_4$ to $\mathbb{F}_2 \times \mathbb{F}_2$ with $\phi(2q + r) = (q, q \oplus r)$. We also define Q from $\mathbb{Z}_4$ to $\mathbb{F}_2$ with $Q(2q + r) = q$.*

The Gray map is clearly a bijection from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$ and its inverse is defined by $\phi^{-1}(q,s) = 2q + (q \oplus s)$. Identifying $\mathbb{F}_2^m \times \mathbb{F}_2^m$ to $\mathbb{F}_2^{2m}$, we extend naturally ϕ to $\mathbb{Z}_4^m$ componentwise by $\phi_m(2q_0 + r_0, \cdots, 2q_{m-1} + r_{m-1}) = (q_0, \cdots, q_{n-1}, q_0 \oplus r_0, \cdots, q_{m-1} \oplus r_{m-1})$ and ϕ_m^{-1} to $\mathbb{F}_2^{2m}$ by $\phi_m^{-1}(q_0, \cdots, q_{n-1}, s_0, \cdots, s_{m-1}) = (2q_0 + q_0 \oplus s_0, \cdots, 2q_{m-1} + q_{m-1} \oplus s_{m-1})$.

Definition 7. *The $2m$-variables boolean function f derived by the Gray map is*

$$\begin{array}{rl} f : \mathbb{F}_2^{2m} & \to \mathbb{F}_2 \\ y & \mapsto Q(F(\phi_m^{-1}(y))) \end{array}$$

Numerical Results

Nonlinearity $nl_2(f)$ of obtained balanced n-variables boolean functions f with $n = 2m$ derived from the previous constructed balanced quaternary m-variables functions F compared with known values.

n	bnl^1	bnl^2	nl^1	nl^2	$\mathbf{nl_2(f)}$
6	12	10	22	24	**24**
8	58	70	94	112	**112**
10	260	366	390	478	**464**
12	1124	1700	1600		**1952**
14	4760	7382	6524		**8000**

bnl^1 Lobanov's lower bound
bnl^2 Carlet - Feng's ([4]) lower bound

nl^1 Best balanced exact Nonlinearity before
nl^2 Carlet-Feng's ([4]) exact Nonlinearity with optimal algebraic immunity

7 Numerical Example for $m = 3$ and $n = 6$

Let consider the Galois ring $R = GR(4,3)$ of 64 elements built with the b-polynomial $h(x) = x^3 + 2x^2 + x + 3$ (Sub Section 4.1).

The 8 cyclotomic classes of order 7 of $R^\star$ (Def.5) are :

$C_0 : \{3, \beta+2, \beta^2+2, \beta^3+2, \beta^4+2, \beta^5+2, \beta^6+2\}$
$C_1 : \{1+2\beta, 3\beta, \beta^2+2\beta, \beta^3+2\beta, \beta^4+2\beta, \beta^5+2\beta, \beta^6+2\beta\}$
$C_2 : \{1+2\beta^2, \beta+2\beta^2, \beta^2+2\beta^2, \beta^3+2\beta^2, \beta^4+2\beta^2, \beta^5+2\beta^2, \beta^6+2\beta^2\}$
$C_3 : \{1+2\beta^3, \beta+2\beta^3, \beta^2+2\beta^3, \beta^3+2\beta^3, \beta^4+2\beta^3, \beta^5+2\beta^3, \beta^6+2\beta^3\}$
$C_4 : \{1+2\beta^4, \beta+2\beta^4, \beta^2+2\beta^4, \beta^3+2\beta^4, \beta^4+2\beta^4, \beta^5+2\beta^4, \beta^6+2\beta^4\}$
$C_5 : \{1+2\beta^5, \beta+2\beta^5, \beta^2+2\beta^5, \beta^3+2\beta^5, \beta^4+2\beta^5, \beta^5+2\beta^5, \beta^6+2\beta^5\}$
$C_6 : \{1+2\beta^6, \beta+2\beta^6, \beta^2+2\beta^6, \beta^3+2\beta^6, \beta^4+2\beta^6, \beta^5+2\beta^6, \beta^6+2\beta^6\}$
$C_7 : \{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\}$

The obtained partitions applying the construction are (Prop.6) :

Let $E_j = \{u \in \mathbb{Z}_4^3, F(u) = j\}$, $j = 0, 1, 2, 3$.

$$\begin{array}{l} E_0 = C_0 \cup C_4 \cup \{2, 2\beta^4\} \\ E_1 = C_1 \cup C_5 \cup \{2\beta, 2\beta^5\} \\ E_2 = C_2 \cup C_6 \cup 2\{\beta^2, 2\beta^6\} \\ E_3 = C_3 \cup C_7 \cup \{2\beta^3, 0\} \end{array}.$$

The balanced constructed 3-variables quaternary function F is :

$F = 33223123110012003120031113022032002200213311321303211130301223 02$
with $nl_4^H(F) = 44$ and $nl_4^L(F) = 56$.

The balanced derived 6-variables boolean function f is :

$f = 11111011000001001010010001011011001100101100110101100010100111101$
with $nl_2(f) = 24$.

8 Conclusion

This paper presents new results on quaternary cryptographic functions, bringing out a new approach of functions used in the security of pseudo-random generators of stream and blocks ciphers. The main goal of this work, similarly motivated by the $\mathbb{Z}_4$ linearity paper [8], is to present an alternative to the open problem of finding optimal boolean functions. After defining quaternary functions and describing their $\mathbb{Z}_4$ balancedness and nonlinearity, under the Hamming metric and the Lee metric, we give results on the maximal nonlinearity of quaternary Bent functions. Using the algebraic structure of a Galois ring, we present a general construction of quaternary functions, pointing out necessary trade offs in order to obtain optimal cryptographic properties. In a natural way, we apply this construction with a particular configuration to get balanced and high nonlinearity quaternary functions. Faithful to our main objective, we take the image of our quaternary constructed functions under the Gray map to obtain balanced and high nonlinearity boolean functions. Other quaternary cryptographic properties, as correlation immunity, resiliency and algebraic immunity and the study of the relationship between binary and quaternary nonlinearity are actually in progress. $\mathbb{Z}_4$ codes, Galois Rings and Difference Sets over $\mathbb{Z}_4$ seems to offer great investments opportunities and reinforce our motivation to go on with this new kind of approach.

References

1. Canteaut, A., Trabbia, M.: Improved fast correlation attacks using parity-check equations of weight 4 and 5. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 573–588. Springer, Heidelberg (2000)
2. Carlet, C.: On Bent and highly nonlinear balanced/resilient functions and their algebraic immunities. In: Fossorier, M.P.C., Imai, H., Lin, S., Poli, A. (eds.) AAECC 2006. LNCS, vol. 3857, pp. 1–28. Springer, Heidelberg (2006)
3. Carlet, C., Dubuc, S.: On generalized Bent and $q-$ary perfect nonlinear functions. Finite Fields and Applications 1999, 81–94 (2001)
4. Carlet, C., Feng, K.: An infinite class of balanced functions with optimal algbreaic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 425–440. Springer, Heidelberg (2008)
5. Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345–359. Springer, Heidelberg (2003)
6. Courtois, N., Pieprzyk, J.: Cryptanalysis of block ciphers with over-defined systems of equations. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 267–287. Springer, Heidelberg (2002)

7. Ding, C., Xiao, G., Shan, W.: The stability theory of stream ciphers. In: Ding, C., Shan, W., Xiao, G. (eds.) The Stability Theory of Stream Ciphers. LNCS, vol. 561. Springer, Heidelberg (1991)
8. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes. IEEE Transactions on Information Theory 40(2), 301–319 (1994)
9. Hou, X.: $p-$ary and $q-$ary versions of certain results about Bent functions and resilient functions. Finite Fields and Applications 10, 566–582 (2004)
10. Hou, X.: $q-$ary Bent functions constructed from chain rings. Finite Fields and Applications 4, 55–61 (1998)
11. Hou, X.-D.: Bent functions, partial difference sets and quasi-Frobenius rings. Designs, Codes and Cryptography 20, 251–268 (2000)
12. Kumar, P.V., Hellesth, T., Calderbank, A.R., Hammons, A.R.: Large Families of Quaternary Sequences with Low Correlation. IEEE Transactions on Information Theory 42(2), 579–592 (1996)
13. Kavut, S., Maitra, S., Sarkar, S., Yücel, M.D.: Enumeration of 9-variables rotation symetric boolean functions having non-linearity > 240. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 266–279. Springer, Heidelberg (2006)
14. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized Bent Functions and Their Properties. Journal of Combinatirial Theory, Ser. A 1(40), 90–107 (1985)
15. Li, N., Qi, W.-F.: Construction and analysis of boolean functions of $2t+1$ variables with maximum algebraic immunity. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 84–98. Springer, Heidelberg (2006)
16. Meier, W., Pasalic, E., Carlet, C.: Algebraic attacks and decomposition of boolean functions. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 474–491. Springer, Heidelberg (2004)
17. Rothaus, O.S.: On Bent functions. Journal of Combinatorial Theory 20, 300–305 (1976)
18. Saber, Z., Uddin, M.F., Youssef, A.: On the Existence of $(9, 3, 5, 240)$ Resilient Functions. IEEE Transactions on Information Theory 52(5), 2269–2270 (2006)
19. Solé, P., Tokareva, N.: Connections between quaternary and binary Bent functions. Cryptology ePrint Archives (2009), http://www.eprint.iacr.org/2009/544
20. McDonald, B.R.: Finite Rings with Identity. Marcel Dekker Inc., New York (1974)

A Public Key Cryptosystem Based upon Euclidean Addition Chains

Fabien Herbaut[1] and Pascal Véron[2]

[1] Université du Sud Toulon-Var, IMATH, France
IUFM de Nice, Université de Nice
herbaut@unice.fr
[2] Université du Sud Toulon-Var, IMATH, France
veron@univ-tln.fr

Abstract. Addition chains are classical tools used to speed up exponentiation in cryptographic algorithms. In this paper we proposed to use a subset of addition chains, the Euclidean addition chains, in order to define a new public key cryptosystem.

1 Introduction

The problem of minimizing the number of operations to compute x^n has a long history which involves al-Kashi and started at least in India, where the binary representation of n was already considered 200 B.C .

It appeared that this problem is deeply connected to this of finding short addition chains leading to n as explained in [6]. The name *addition chain* seems to come from Sholz paper [11].

Definition 1. *An addition chain of length s computing an integer k is a sequence $u_0, u_1, \ldots, u_s$ of positive integers such that :*

1. $u_0 = 1$ *and* $u_s = k$,
2. $\forall i \in [1, s]$, $u_i = u_j + u_t$ *with* $0 \leqslant j, t < i$.

Example : $(1, 2, 3, 6, 12, 15, 24, 39)$ is an addition chain of length 8 computing the integer 39, since $2 = 1 + 1$, $3 = 2 + 1$, $6 = 3 + 3$, $12 = 6 + 6$, $15 = 12 + 3$, $24 = 12 + 12$, $39 = 24 + 15$.

The problem of computing $l(n)$, the shortest length s of such a sequence computing n, is of importance and has given raise to numerous papers in the last century. For example, one can quote the papers of Brauer [2] , Yao [13], and the survey of Subbarao [12]. Two problems seem to have played the role of a red thread. The first one is to give sharp upper bounds for $l(n)$. As for example, it is well known that

$$\log n + \log v(n) - 2.13 \leqslant l(n) \leqslant \lfloor \log n \rfloor + v(n) - 1$$

where $v(n)$ is the Hamming weight of n. The Sholz conjecture, namely $\forall n \in \mathbb{N}^*, l(2^n - 1) \leqslant n - 1 + l(n)$, also played an important role in the development of the theory of addition chains.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 284–297, 2010.

The second problem is to find efficient algorithms to compute short chains for a given integer n. Both problems are still considered difficult. For recent results, one can see [1].

There is one special class of addition chains which have been well studied : the Brauer chains or star chains. This class is introduced in [2].

Definition 2. *A star addition chain or Brauer chain is a particular addition chain where* $\forall i \in [1, s]$, $u_i = u_{i-1} + u_j$ *with* $0 \leqslant j < i$.

EXAMPLE : $(1, 2, 3, 5, 8, 13, 26, 39)$ is a star addition chain of length 8 computing the integer 39.

These chains are well fitted for computations. Indeed at each step, to compute u_i, the last term u_{i-1} (already in the accumulator) is used. Recently, Meloni [8] studied a subclass of star chains : the so called Euclidean addition chains.

Definition 3. *An Euclidean addition chain (EAC) computing an integer* k *is an addition chain which satisfies* $u_1 = 1, u_2 = 2, u_3 = u_2 + u_1$ *and* $\forall\ 3 \leq i \leq s - 1$, *if* $u_i = u_{i-1} + u_j$ *for some* $j < i-1$, *then* $u_{i+1} = u_i + u_{i-1}$ *(case 1) or* $u_{i+1} = u_i + u_j$ *(case 2).*

As an EAC is a strictly increasing sequence, case 1 will be called big step (we add the biggest of the two possible numbers to u_i) and case 2 small step (we add the smallest one).

EXAMPLE : $(1, 2, 3, 4, 7, 11, 18, 25, 32, 39)$ is an Euclidean addition chain of length 10 computing the integer 39.

In [8], Meloni showed how to use such a chain (with a specific point addition algorithm) to compute nP where P is a point on an elliptic curve. Euclidean addition chains are also used in [5].

Computing an EAC for an integer n is easy : choose an integer $g < n$ such that $(g, n) = 1$ and apply Euclidean algorithm to n and g (see §2). In this way, one can find the $\varphi(n)$ EAC computing n (where φ is the Euler's totient function), but very few is known about the length of the chains obtained. A general asymptotic result due to Yao and Knuth [14] states that the average length of such a chain is

$$6\pi^{-2}(\ln n)^2 + \mathcal{O}(\log n(\log\log n)^2).$$

To find short EAC, Meloni suggests in [7] to choose g close to $\frac{n}{\phi}$ (where ϕ is the golden ratio) adapting this way a heuristic proposed by Montgomery [9] in the context of Lucas chains.

Nowadays, there are no known methods to find a chain of fixed length computing a prescribed integer n. The exhaustive method of listing the integers coprime with n and applying Euclidean algorithm will be clearly inefficient for large n as $\varphi(n)$ will be large too.

We will introduce in this paper a subset $\mathcal{M}_\ell^0$ of EAC of length 2ℓ such that two distinct elements of $\mathcal{M}_\ell^0$ will compute two different integers. Moreover, if $c \in \mathcal{M}_\ell^0$ computes an integer n, we will describe a simple and efficient method to determine c from the knowledge of n.

These remarks are our point of departure to propose a public key cryptosystem based upon EAC. Using chains of the set $\mathcal{M}_\ell^0$ induces a trapdoor in the problem of finding a chain of fixed length computing a prescribed integer.

This paper is organized as follows. Section 2 deals with links between Euclidean addition chains and the Euclidean algorithm. In section 3 we define the set $\mathcal{M}_\ell^0$ and give some of its properties. In section 4 we describe our cryptosystem. Section 5 deals with its security. We detail the scrambling actions of the cryptosystem, and show why they are important. We make links between difficult problems and the problem an intruder will have to solve to break the cryptosystem. We also discuss the parameters of the cryptosystem. In section 6 we discuss the performances of the cryptosystem. Section 7 gives a useful toy example which can help to better understand the cryptosystem. We conclude in section 8.

2 Euclidean Algorithm and Euclidean Addition Chains

For the sequel of the paper, we will use an equivalent definition for EAC. This way EAC can be in practice interpreted as binary sequences.

Definition 4. *An Euclidean addition chain (EAC) of length s is a sequence $(c_i)_{i=1\ldots s}$ with $c_i \in \{0,1\}$. The integer k computed from this sequence is obtained from the sequence $(v_i,u_i)_{i=0..s}$ such that $v_0 = 1$, $u_0 = 2$ and $\forall i \geqslant 1$, $(v_i,u_i) = (v_{i-1}, v_{i-1}+u_{i-1})$ if $c_i = 1$ (small step), or $(v_i,u_i) = (u_{i-1}, v_{i-1}+u_{i-1})$ if $c_i = 0$ (big step). The integer k associated to the sequence $(c_i)_{i=1\ldots s}$ is $v_s + u_s$.*

Example : From the EAC (1000111) one can compute the integer 39 as follows : $(1,2) \xrightarrow{1} (1,3) \xrightarrow{0} (3,4) \xrightarrow{0} (4,7) \xrightarrow{0} (7,11) \xrightarrow{1} (7,18) \xrightarrow{1} (7,25) \xrightarrow{1} (7,32)$, which corresponds to the EAC $1,2,3,4,7,11,18,25,32,39$.

From now on, we will define the length of an EAC as the length of the corresponding binary sequence $(c_i)_{i=1\ldots s}$.

Let us observe the progress of the substractive Euclidean algorithm when applied to coprime integers (see algorithm 1) in order to stress the link with EAC. The assertion $\{(v,u) = 1, v < u, u \geqslant 2, v \geqslant 1\}$ is an invariant of Algorithm 1. Moreover the variable u strictly decreases for each turn of the while loop. Hence the algorithm ends with $u = 2$ and $v = 1$.

Algorithm 1. Substractive Euclidean algorithm applied to coprime integers

Require: (v,u) with $(v,u) = 1$, $v < u$ and $v \geqslant 1$.
1: **while** $u > 2$ **do**
2: **if** $u \geqslant 2v$ **then**
3: $(v,u) \leftarrow (v, u-v)$
4: **else**
5: $(v,u) \leftarrow (u-v, v)$
6: **end if**
7: **end while**

EXAMPLE : Starting from $(5, 17)$ the algorithm successively computes $(5, 12)$, $(\mathbf{5}, \mathbf{7})$, $(2, 5)$, $(\mathbf{2}, \mathbf{3})$ and $(1, 2)$ where bold couples mean that $u < 2v$. Now, if we read the sequence of the couples from the last one to the first one, notice that at each step the couple (v, u) is replaced by $(u, u + v)$ or by $(v, u + v)$. That is to say that reading the couples computing by Algorithm 1 from the last one to the first one we obtain an addition chain (as defined in definition 4) which can compute the initial input u.

EXAMPLE : Starting from the previous example, we get $(1, 2) \xrightarrow{0} (\mathbf{2}, \mathbf{3}) \xrightarrow{1} (2, 5) \xrightarrow{0} (\mathbf{5}, \mathbf{7}) \xrightarrow{1} (5, 12)$, we obtain this way the EAC 0101 which computes the integer 17.

Taking into account this remark, we can easily define an algorithm computing an EAC for an integer k :

Algorithm 2. ComputeEACfor(k)

Require: $k \geqslant 4$.
1: Randomly computes an integer g, such that $g > k/2$ and $(g, k) = 1$.
2: $(v, u) \leftarrow (k - g, g)$
3: **while** $u > 2$ **do**
4: **if** $u \geqslant 2v$ **then**
5: $(v, u) \leftarrow (v, u - v)$
6: Output 1
7: **else**
8: $(v, u) \leftarrow (u - v, v)$
9: Output 0
10: **end if**
11: **end while**

Remark 1. Notice that in Algorithm 2, we choose $g > k/2$. Indeed suppose that $g \leqslant k/2$, then the first step of Algorithm 1 will compute the couple $(g, k - g)$ from (g, k). Now using the same algorithm with input (g', k) where $g' = k - g$, we will obtain after the first step the couple $(k - g', g') = (g, k - g)$ because $k - g \geqslant k/2$. Hence algorithm 2 applied to (g, k) or (g', k) will lead to the same EAC.

Notice also that, since $g > k/2$, the initialization $(v, u) \leftarrow (k - g, g)$ corresponds to the first execution of the While loop of Algorithm 1.

Remark 2. This algorithm outputs the mirror image of the EAC computing k when starting from an integer g (i.e. the sequence read from right to left). We will see in next section, that an EAC and its mirror image computes the same integer k.

3 Notations and Properties

We give in this section some notations and important results for the sequel of this paper.

Definition 5. *Let $n > 0$, we define :*

- *$\mathcal{M}$ as the set of EAC,*
- *$\mathcal{M}_n$ as the set of EAC of length $n > 0$,*
- *χ the map from $\mathcal{M}$ to $\mathbb{N}$, such that for $m \in \mathcal{M}$, $\chi(m)$ be the integer computed from the EAC m,*
- *ψ the map from $\mathcal{M}$ to $\mathbb{N} \times \mathbb{N}$, such that for $m \in \mathcal{M}$, $\psi(m) = (v_s, u_s)$ if $m \in \mathcal{M}_s$,*
- *S_0 the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ corresponding to a big step iteration,*
- *S_1 the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ corresponding to a small step iteration.*

With these notations, for $m = (m_1, \ldots, m_s) \in \mathcal{M}_s$, we have :

$$\psi(m) = (1,2)\prod_{i=1}^{s} S_{m_i} \text{ and } \chi(m) = \langle (1,2)\prod_{i=1}^{s} S_{m_i}, (1,1)\rangle.$$

Let r and s be two integers, we will denote by mm' the element of $\mathcal{M}_{r+s}$ obtained from the concatenation of $m \in \mathcal{M}_r$ and $m' \in \mathcal{M}_s$. This way, for $n > 0$, m^n is a word of $\mathcal{M}_{nr}$ if $m \in \mathcal{M}_r$.

Proposition 1. *Let $n > 0$, F_i be the i^{th} Fibonacci number (defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$) :*

- *$\psi(0^n) = (F_{n+2}, F_{n+3})$, $\psi(1^n) = (1, n+2)$, $\chi(0^n) = F_{n+4}$, $\chi(1^n) = n + 3$,*
- *$\forall m \in \mathcal{M}_n$, $\chi(1^n) \leqslant \chi(m) \leqslant \chi(0^n)$,*
- *$S_0^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$, $S_1^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.*

Proof. All these properties can easily be proved by induction.

Proposition 2. *Let $n > 0$ and $m = (m_1, \ldots, m_n) \in \mathcal{M}_n$, then :*

- *$\chi(m_1, \ldots, m_n) = \chi(m_n, \ldots, m_1)$,*
- *the map ψ is injective.*

Proof. We refer to [6] for standard link between EAC, Euclidean algorithm and continued fractions, which explains the first point. It is also explained that if $\psi(m) = (v, u)$ then $(u, v) = 1$ and the only chain which leads to (v, u) is obtained using the substractive version of Euclidean algorithm. □

From proposition 2 the restriction of χ to $\mathcal{M}_n$ is not injective because of the mirror symmetry property.

Proposition 3. *Let $\mathcal{M}_n^0$ be the subset of $\mathcal{M}_{2n}$ whose elements are EAC beginning with n zeros. The restriction of χ to $\mathcal{M}_n^0$ is injective.*

Proof. Let x and y be two words of $\mathcal{M}_n^0$ such that $\chi(x) = \chi(y)$, and $m0^n$, $m'0^n$, be the words obtained when reading x and y from right to left. Using the symmetry property, we have $\chi(m0^n) = \chi(m'0^n)$. Let $(v,u) = \psi(m)$ and $(v',u') = \psi(m')$, then

$$\begin{aligned} & \chi(m0^n) = \chi(m'0^n) \\ \Leftrightarrow\ & F_nu + F_{n-1}v + F_{n+1}u + F_nv = F_nu' + F_{n-1}v' + F_{n+1}u' + F_nv' \\ \Leftrightarrow\ & F_{n+2}(u-u') = F_{n+1}(v'-v)\,. \end{aligned}$$

Since $(F_{n+1}, F_{n+2}) = 1$, then F_{n+2} divides $v'-v$. Now from proposition 1, since v and v' are less or equal than F_{n+2} and nonzero, then $|v'-v| < F_{n+2}$. It implies that $v = v'$ and so $u = u'$. Hence $\psi(m) = \psi(m')$, so $m = m'$.

Proposition 4. *Let $c_{g,k}$ be the EAC computing the integer k from the integer g using Algorithm 2 then, $c_{g,k}$ ends with n zeros if and only if the n^{th} couple computed by Algorithm 2 is equal to $(kF_{n+1} - gF_{n+2}, gF_{n+1} - kF_n)$ if n is even or $(gF_{n+2} - kF_{n+1}, kF_n - gF_{n+1})$ if n is odd.*

Proof. Let us suppose that $c_{g,k}$ ends with n zeros. It means that the n^{th} couple computed by Algorithm 2 is equal to $(k-g, g)S_0^{-n}$. Now since $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ (Cassini's identity), then $S_0^{-n} = (-1)^n \begin{pmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{pmatrix}$. Hence $(k-g,g)S_0^{-n} = ((-1)^n(kF_{n+1} - gF_{n+2}), (-1)^n(gF_{n+1} - kF_n))$.

The converse can be easily proved by induction. □

Corollary 1. *Let $c_{g,k}$ be the EAC computing the integer k from the integer g using Algorithm 2. The chain $c_{g,k}$ ends with n zeros if and only if :*

- $k\frac{F_{n+2}}{F_{n+3}} < g < k\frac{F_{n+1}}{F_{n+2}}$, *if n is even.*
- $k\frac{F_{n+1}}{F_{n+2}} < g < k\frac{F_{n+2}}{F_{n+3}}$, *if n is odd.*

Proof. Let us suppose that $c_{g,k}$ ends with n zeros. From the preceding proposition, the n^{th} couple computed by Algorithm 2 is $((-1)^n(kF_{n+1} - gF_{n+2}), (-1)^n(gF_{n+1} - kF_n))$ and satisfies $(-1)^n(kF_{n+1} - gF_{n+2}) < (-1)^n(gF_{n+1} - kF_n)$. Thus $(-1)^n k\frac{F_{n+2}}{F_{n+3}} < (-1)^n g$. Now taking into account only the $n-1$ first steps, we also must have $(-1)^{n-1}k\frac{F_{n+1}}{F_{n+2}} < (-1)^{n-1}g$.

An easy induction proves the converse. □

The previous result means that to find an EAC (ending with n zeros) which computes an integer k, algorithm 2 has to be run with an integer g lying in a specific interval $\mathcal{I}$. Let $k \in \chi(\mathcal{M}_0^n)$ and c_k be the element of $\mathcal{M}_0^n$ such that $\chi(c_k) = k$. Let $\tilde{c}_k$ be the mirror of c_k, then $\tilde{c}_k$ ends with n zeros. The size $\mathcal{S}$ of the interval $\mathcal{I}$ is $|k\frac{F_{n+1}}{F_{n+2}} - k\frac{F_{n+2}}{F_{n+3}}|$ which is equal to $\frac{k}{F_{n+2}F_{n+3}}$. If $k < F_{n+2}F_{n+3}$ then $\mathcal{S} < 1$, hence at most one integer lies in $\mathcal{I}$. Now since k has been computed from a chain beginning with n zeros, then there is exactly one element g in $\mathcal{I}$ which can compute $\tilde{c}_k$ from k using algorithm 3.

Algorithm 3. InverseChi(k, n) for $k \in \chi(\mathcal{M}_0^n)$

1: **if** n is even **then**
2: $g \leftarrow \lfloor k\frac{F_{n+1}}{F_{n+2}} \rfloor$
3: **else**
4: $g \leftarrow \lfloor k\frac{F_{n+2}}{F_{n+3}} \rfloor$
5: **end if**
6: $(v, u) \leftarrow (k - g, g)$
7: **while** $u > 2$ **do**
8: **if** $u \geqslant 2v$ **then**
9: $(v, u) \leftarrow (v, u - v)$
10: Output 1
11: **else**
12: $(v, u) \leftarrow (u - v, v)$
13: Output 0
14: **end if**
15: **end while**

Remark 3. Since $\tilde{c}_k$ ends with n zeros, we can begin the preceding algorithm with :

$$0\text{: } \textit{Output } n \textit{ zeros}$$

and (using proposition 4) modify the line 6 as follows :

$$6\text{: } (v, u) \leftarrow ((-1)^n(kF_{n+1} - gF_{n+2}), (-1)^n(gF_{n+1} - kF_n)).$$

Remark 4. Let $0^n y$ be a chain computing the integer k. The algorithm was designed to compute the chain $\tilde{y}0^n$ where $\tilde{y}$ is the mirror of y. But because of the progress of the algorithm the chain is sent back from the left to the right. Hence the last n bits returned are exactly the word y.

4 The Cryptosystem

The cryptosystem is composed of three algorithms :

- Genparam which takes as input two integers n and t $(n > t)$ and returns the public key pk and the secret key sk of the system,
- Encrypt which takes as input a binary sequence of size $n - t$, the public key pk and returns the cryptogram c,
- Decrypt which takes as input the cryptogram c, the secret key sk and return the plaintext m.

Let us give some details on the decryption procedure. To this end, we will denote by $\chi_{\alpha,\beta}(m)$ the integer computed from the EAC m when starting from the couple (α, β) instead of $(1, 2)$.

Let M be the matrix equal to $\prod_{i=1}^{n-t} S_{m_i}$ so that $\chi_{\alpha,\beta}(m) = \alpha(M_{11} + M_{12}) + \beta(M_{21} + M_{22})$. First notice that if d is the gcd of (α, β) then $\chi_{\alpha/d,\beta/d}(m) = \chi_{\alpha,\beta}(m)/d$, hence we will only consider the case where $\gcd(\alpha, \beta)$=1.

Algorithm 4. Genparam(n, t)

1: Randomly computes a prime $p > F_{2n+4}$
2: Randomly choose $\lambda \in [1, p-1]$
3: Randomly choose $x \in \{0,1\}^t$
4: $(\delta_1, \delta_2) \leftarrow \psi(0^n x) = \psi_{(F_{n+2}, F_{n+3})}(x)$
5: $(a, b) \leftarrow (\lambda\delta_1 \mod p, \lambda\delta_2 \mod p)$
6: $d \leftarrow \gcd(a, b)$
7: $pk \leftarrow (a/d, b/d)$
8: $sk \leftarrow (d, p, \lambda^{-1} \mod p, x)$
9: return (pk, sk)

Algorithm 5. Encrypt$(pk, m$: binary seq. of length $n-t)$

1: $c \leftarrow \chi_{pk}(m)$
2: return c

Algorithm 6. Decrypt(sk, c)

1: $y \leftarrow \lambda^{-1} dc \mod p$
2: $c_y \leftarrow$ InverseChi(y, n)
3: $m \leftarrow$ last $n-t$ bits of c_y (see Remark 4.).
4: return m

Let us notice in the same way $\psi_{\alpha,\beta}(m)$ the last couple obtained from the EAC m when starting from (α, β). Let m_1 and m_2 be any two EAC, then

- $\psi_{\alpha,\beta}(m_1 m_2) = \psi_{\psi_{\alpha,\beta}(m_1)}(m_2)$,
- $\chi_{\alpha,\beta}(m_1 m_2) = \chi_{\psi_{\alpha,\beta}(m_1)}(m_2)$.

Taking into account these results, we have the following equalities for the cryptosystem :

$$\chi(0^n xm) = \chi_{1,2}(0^n xm) = \chi_{F_{n+2},F_{n+3}}(xm) = \chi_{\delta_1,\delta_2}(m).$$

Now, since $c = \chi_{a/d,b/d}(m) = \chi_{a,b}(m)/d = \frac{a(M_{11}+M_{12})+b(M_{21}+M_{22})}{d}$, then

$$\lambda^{-1} cd \equiv \delta_1(M_{11} + M_{12}) + \delta_2(M_{21} + M_{22}) \mod p\,.$$

But,

$$\begin{aligned}\delta_1(M_{11} + M_{12}) + \delta_2(M_{21} + M_{22}) &= \chi_{\delta_1,\delta_2}(m) \\ &= \chi_{F_{n+2},F_{n+3}}(xm)\end{aligned}$$

and since $\chi_{F_{n+2},F_{n+3}}(xm) \leqslant \chi_{F_{n+2},F_{n+3}}(0^n) = F_{2n+4}$ (from property 2), then

$$\lambda^{-1} cd \mod p = \chi_{F_{n+2},F_{n+3}}(xm) = \chi(0^n xm)\,,$$

because $p > F_{2n+4}$. Using Algorithm 3, we can find back the sequence xm and deduce the plaintext m. Indeed, from a practical point of view, for the values n

suggested in section 6, $\chi(0^n xm) < F_{n+2}F_{n+3}$ as soon as the Hamming weight of x is greater or equal than 4. Another way to guarantee this last property is to consider only plaintext of length $n-1$. With such a condition, $\chi(0^n xm) \leqslant F_{2n+3} < F_{n+2}F_{n+3}$ for $n > 0$ and the map χ still remains injective. See section 7 for a toy example.

5 Security

First let us explain the meaning of the integer λ and the vector x. The integer λ is used in order to scramble the value of the couple (δ_1, δ_2). Indeed, if the cryptogram were computed as $\chi_{\delta_1,\delta_2}(m)$, then since $\chi_{\delta_1,\delta_2}(m) = \chi(0^n xm)$, any intruder could use Algorithm 3 to find back the cleartext m.

Remember that using x such that its Hamming weight be greater or equal than 4 guarantees that the value of $\chi(0^n xm)$ for any plaintext m is always strictly less than $F_{n+2}F_{n+3}$ (for the practical parameters given in section 6), which is an essential condition for the decryption process. Let us suppose however that we don't use the vector x, here is a possible attack to find back the secret parameters λ and p. Without x, (δ_1, δ_2) would be equal to (F_{n+2}, F_{n+3}). Now, if a and b are coprime, then pk will be equal to (a, b) in Algorithm 4. Hence, we will have

$$\begin{aligned} a &= \lambda F_{n+2} \mod p \\ b &= \lambda F_{n+3} \mod p \end{aligned}$$

i.e, there exist two integers j_a, j_b such that $a = \lambda F_{n+2} - j_a p$ and $b = \lambda F_{n+3} - j_b p$. Now, let $\varepsilon_0 = b$, $\varepsilon_1 = a$ and consider the sequence $\varepsilon_i = \varepsilon_{i-2} - \varepsilon_{i-1}$, a simple induction shows that $\varepsilon_i = \lambda F_{n+3-i} + (-1)^i (j_a F_i - j_b F_{i-1})p$, for $i \geqslant 2$. Hence $\varepsilon_{n+3} = (-1)^{n+3}(j_a F_{n+3} - j_b F_{n+2})p$ is a multiple of p. Since $F_k \mid F_{\ell k}$ we can obtain a set of integers which are all multiples of p. As an example since $F_4 = 3F_2$ and $F_{10} = 11F_5$, then $\varepsilon_{n-1} - 3\varepsilon_{n+1} \equiv 0 \mod p$ and $\varepsilon_{n-2} - 11\varepsilon_{n-7} \equiv 0 \mod p$. Computing the gcd of these integers will give us the value of p. Now, since $\varepsilon_{n+1} \equiv \lambda \mod p$ and $\lambda < p$, the value of ε_{n+1} modulo p gives us λ.

Using a vector x discards the possibility to easily obtain a set of multiples of p from the public key (a, b).

A way to find back the cleartext is to try to solve the following computational problem, which we will denote by **GEAC** for Generalized Euclidean Addition Chain Problem :

Name : GEAC
Input : Four integers a, b, α and ℓ such that $(a, b) = 1$ and $\alpha = \chi_{a,b}(c)$
Question : Compute $c \in \{0, 1\}^\ell$.

Suppose that an efficient algorithm could be designed to solve GEAC. If it is fast enough , it could then be used to compute minimal length EAC. As a consequence, using the method described in [8], this will lead to an efficient point multiplication algorithm for elliptic curves resistant to side channel attacks. From all the works done over addition chains, we did not find any references about the GEAC problem. Most of the papers on this topic deal with classical addition

chains starting with (1,2). It is thus of importance to classify this problem. We can associate a decision problem to GEAC :

Name : D-GEAC
Input : Four integers a, b, α and ℓ such that $(a, b) = 1$.
Question : Does there exist an euclidean addition chain c of length ℓ such that $\alpha = \chi_{a,b}(c)$?

We cannot state if this problem is NP-complete (it is clearly in NP). However, we would like to point out a related problem which is NP-complete, as we will prove it.

Name : G-AS
Input : A sequence $n_1, \ldots, n_r, a, b$ of positive integers such that $\gcd(a, b) = 1$, a positive integer L.
Question : Does there exist an addition chain of length $\leqslant L$ starting with (a, b) which contains all the $n_i's$?

This problem is a generalization of the following one :

Name : AS
Input : A sequence $n_1, \ldots, n_r$ of positive integers and a positive integer L.
Question : Does there exist an addition chain of length $\leqslant L$ which contains all the $n_i's$?

From [4] this problem is NP-complete.

Proposition 5. *G-AS is NP-complete*

Proof. The proof given in [4] shows how to reduce AS to the well known problem of Vertex Cover in a graph G. To this end, the author constructs the sequence $\Delta_G = \{1, 2, 2^2, \ldots, 2^{\sigma n}\} \cup \{1 + 2^{\sigma u} + 2^{\sigma v}\}$ where n is the number of vertices of G and (u, v) describes the set of edges. He shows then how to build a vertex cover of size at most K from an addition chain of size at most $\sigma n + 1 + \#E + K$ which contains the sequence Δ_G. Now, let us consider the sequence $\Delta_{Ga,b} = \{b, 2b, 2^2b, \ldots, 2^{\sigma n}b\} \cup \{a + b2^{\sigma u} + b2^{\sigma v}\}$ rather than Δ_G. Then we can read exactly the same proof to establish that G-AS is NP-complete. □

For a first approach of the security of the scheme, we must define parameters n and t in order to avoid classical attacks. The parameter t must be chosen so that an intruder cannot retrieve the chain x using an exhaustive search. We suggest to choose $t = 80$.

Since the size of the cleartext is $n-t$, we have to choose n such that $n-t > 80$, which leads to take $n > 160$.

The prime p must be chosen so that $p > F_{2n+4}$. We suggest to randomly select p in the range $]F_{2n+4}, F_{2n+5}]$. For $n > 160$, there are at least 2^{215} such primes.

Notice that since the cryptogram has been computed using the algorithm of definition 4 starting from $v_0 = a$ and $u_0 = b$ with $(a, b) = 1$ then all the couples (v, u) generated satisfy $(v, u) = 1$. Hence one could try to choose an integer $g < c$ coprime with c and apply algorithm 2 until the current couple (v, u) be equal to

(a, b). Now, there are about $\varphi(c)/2$ candidates and $\varphi(c) > c/\ln c$. Since c is of the order of p, selecting randomly g without any strategy will fail.

This cryptosystem is deterministic, and hence is not semantically secure, thus we do not resist to any of the **IND**-xxx attack. For this first approach of a cryptosystem based upon EAC, we do not investigate the formal model of provable security.

6 Performances

Let us first consider the transmission rate of this system. The size of the cleartext m is $n - t$. The cryptogram is obtained by the computation of

$$\langle (a, b) \prod_{i=1}^{n-t} S_{m_i}, (1, 1) \rangle .$$

If we consider the m_i's as $n - t$ independent Bernoulli random variables, it can be proved that the mean value of a cryptogram is $(3/2)^{n-t}(a + b)$. Since a and b are of the order of p, and since p is of the order of F_{2n+4}, this mean value is about $2(3/2)^{n-t}F_{2n+4}$. Taking into account that $\log_2 F_k$ is about $0.694k$, then the average size of the cryptogram is $1.97n - 0.58t + 3.7$. Hence the transmission rate of the cryptosystem is on average

$$\frac{n - t}{1.97n - 0.58t + 3.7} .$$

Since we fixed $t = 80$, and $n > 160$, this is an increasing sequence which tends to $1/1.96 \simeq 0.5$. Notice that the worst transmission rate is obtained when the cryptogram is computed from the cleartext 0^{n-t}. In this case the cryptogram is equal to $aF_{n-t+1} + bF_{n-t+2}$ whose size is about $2.08n - 0.69t + 4.16$.

The public and the private datas (except for x) are all of the order of p, which is close to F_{2n+4}. Using this estimation, table 1 sums up for $t = 80$ the characteristics of the system and give some numerical results for $n = 592$, $n = 1104$, $n = 2128$ and $n = 336$ (this last one is only given for illustrative purpose). The value $\mathcal{I}$ denotes the ratio between the size of the cleartext and the size of the cryptogram.The value $\mathcal{I}_W$ denotes the worst transmission rate.

Table 1. Characteristics of the scheme

n	size of cleartext (bits)	size of p_k (bits)	size of s_k (bits)	$\mathcal{I}$	$\mathcal{I}_W$
	$n - 80$	$2.8n + 5.6$	$4.2n + 88.4$	$\frac{n-80}{1.97n-42.83}$	$\frac{n-80}{2.08n-51.36}$
336	256	947	1500	0.41	0.39
592	512	1664	2575	0.45	0.43
1104	1024	3097	4726	0.48	0.46
2128	2048	5965	9026	0.49	0.47

The encryption process only involves $n-t$ additions over integers. The size of these integers grows from $1.4n$ (the size of a and b) to $2.08n$ in the worst case. We can speed up this process by using the following remark :

$$\chi_{pk}(m) = (a,b)\prod_{i=1}^{n-t} S_{m_i}(1,1)^t = (1,1)\prod_{i=n-t}^{1} S_{m_i}^t(a,b)^t\,.$$

Hence to cipher a cleartext m, the user can first compute $n-t$ additions between integers whose size grows from 1 to $0.69(n-t+2)$ in the worst case (the size of F_{n-t+2}). Then, he has to compute the products between integers of size about $1.4n$ and $0.7n$ (au and bv) and the sum $au+bv$.

The decryption process involves :

- step 1 of algorithm 6 : a modular multiplication between integers whose size is about $1.4n$, if we suppose that $\lambda^{-1}d$ has already been computed,
- step 2 or 4 of algorithm 3 : a multiplication between integers of size $1.4n$ and $0.694n$,
- step 2 or 4 of algorithm 3 : a division between an integer of size $2.1n$ and an integer of size $0.694n$,
- last steps of algorithm 3 : $n-t$ subtractions between integers whose size decreases from $1.4n$ to 1.

From an asymptotic point of view, both processes are in $\mathcal{O}(n^2)$ while the same procedures for the classical RSA cryptosystem are in $\mathcal{O}(n^3)$ if n is the size of the modulus. Table 2 gives some numerical results obtained when ciphering and deciphering 20000 cleartext with our cryptosystem and the classical RSA cryptosystem. Since in RSA the ciphering and deciphering procedure are identical we only mention in table 2 the time of ciphering procedure for a random exponent e. The column EAC* corresponds to the optimization of the encryption process above mentioned. Tests have been carried out on a Quadcore 2.33Ghz processor using GnuMP library.

Table 2. Ciphering and deciphering rate in kilobytes per second

size of the cleartext (bits)	EAC-cipher	EAC*-cipher	EAC decipher	RSA
1024	1106 kb/sec	2551 kb/sec	1208 kb/sec	103 kb/sec
2048	693 kb/sec	2024 kb/sec	963 kb/sec	28.46 kb/sec

The transmission rate of our system is a drawback of our system as compared to RSA. But since the design of this latter, very few new asymmetric cryptosystems have been proposed. For example, one could compare our parameters with those of another cryptosystem which didn't use an RSA-like mechanism : the Naccache-Stern knapsack cryptosystem [10] presented at Eurocrypt'97. We choose this cryptosystem since its parameters have been recently improved in 2008 [3]. Moreover, while the system lacks provable security, it still has not been

broken to this date. Since the encryption process involves modular multiplications and the decryption process is equivalent to an RSA signature, we will only discuss the transmission rate and the size of the public-key. In NS cryptosystem, there is a trade-off to establish between these two parameters. A good one corresponds to a transmission rate of 0.38 for a 512 kilobytes public key. If one wants to improve the transmission rate to 0.5, public key will grow up to 14564 kilobytes. On the other hand, for the smallest possible size of the public key (59 kilobytes), the transmission rate drops to 0.11. With our cryptosystem, for a transmission rate between 0.4 and 0.5, the public key is less than 1 kilobyte. Notice also that the proposed cryptosystem has a natural integrity property, since the cleartext computed from the cryptogram must be well formatted : the first $n+t$ bits should be equal to $0^n x$.

7 A Toy Example

We illustrate the mechanism for $n = 6$ and $t = 2$.

• Key generation
$p = 991 > F_{16}$, $\lambda = 230$, $x = (10)$
$(\delta_1, \delta_2) = (55, 76) = \psi(00000010)$ $((1,2) \xrightarrow{0} (2,3) \xrightarrow{0} (3,5) \xrightarrow{0} (5,8) \xrightarrow{0} (8,13) \xrightarrow{0}$ $(13,21) \xrightarrow{0} (21,34) \xrightarrow{1} (21,55) \xrightarrow{0} (55,76))$
$(a, b) = (758, 633)$, $d = \gcd(a, b) = 1$
$pk = (758, 633)$, $sk = (1, 991, 642, (10))$ $(642 = 230^{-1} \mod 991)$.

• Encryption
Let $m = (1101)$ the message to encrypt, the following steps lead us to the computation of $\chi_{pk}(m)$:
$(758, 633) \xrightarrow{1} (758, 1391) \xrightarrow{1} (758, 2149) \xrightarrow{0} (2149, 2907) \xrightarrow{1} (2149, 5056)$
The cryptogram is 7205.

• Decryption
$y = \lambda^{-1} c \mod p = 7205 \times 642 \mod 991 = 613 < F_8 F_9 = 714$
$g = \lfloor 613 \frac{F_7}{F_8} \rfloor = 379$
Using the trick for the line 6 of algorithm 3, we initialize the couple (v, u) to $(613F_7 - 379F_8, 379F_7 - 613F_6) = (10, 23)$. Then the algorithm computes the following couples :
$(10, 13) \xrightarrow{1} (3, 10) \xrightarrow{0} (3, 7) \xrightarrow{1} (3, 4) \xrightarrow{1} (1, 3) \xrightarrow{0} (1, 2) \xrightarrow{1}$ end of algorithm. Last four bits are the cleartext m.

8 Conclusion

In this note we proposed to use Euclidean addition chains to define a public key cryptosystem. To this end, we used properties of a subset of Euclidean addition chains. It enabled us to design a polynomial time algorithm for the problem of

finding an EAC of fixed length computing a prescribed integer (GEAC). Even if we described difficult problems linked to GEAC, we do not know its level of difficulty. However, as we obtained good performances and as it is of interest to propose new public keys mechanisms, we think it is worth presenting this one. As it is usual in cryptography, we welcome readers for attacks and suggestions on this system. Although there exists a lot of efficient point multiplication algorithms for elliptic curves, few of them have been designed to intrisically resist to side channel attacks. Looking for an efficient cryptanalysis of GEAC may bring out new ideas in the theory of Euclidean addition chains. These ideas may have nice applications in the field of point multiplication algorithms resistant to side channel attacks.

References

1. Bahig, H.M.: Improved generation of minimal addition chains. Computing 78(2), 161–172 (2006)
2. Brauer, A.: On addition chains. Bull. Amer. Math. Soc. 45, 736–739 (1939)
3. Chevallier-Mames, B., Naccache, D., Stern, J.: Linear bandwidth naccache-stern encryption. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) SCN 2008. LNCS, vol. 5229, pp. 327–339. Springer, Heidelberg (2008)
4. Downey, P.J., Leong, B.L., Sethi, R.: Computing sequences with addition chains. SIAM J. Comput. 10(3), 638–646 (1981)
5. Goundar, R., Shiota, K., Toyonaga, M.: Spa resistant scalar multiplication using golden ration addition chain method. International Journal of Applied Mathematics 38(2), 83–88 (2008)
6. Knuth, D.E.: The Art of Computer Programming: Fundamental Algorithms, 3rd edn., vol. 2. Addison Wesley, Reading (July 1997)
7. Meloni, N.: Arithmétique pour la Cryptographie basée sur les Courbes Elliptiques. Ph.D. thesis, Université de Montpellier, France (2007)
8. Meloni, N.: New point addition formulae for ECC applications. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 189–201. Springer, Heidelberg (2007)
9. Montgomery, P.L.: Evaluating recurrences of form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas chains (2002), ftp://ftp.cwi.nl/pub/pmontgom/Lucas.ps.gz
10. Naccache, D., Stern, J.: A new public-key cryptosystem. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 27–36. Springer, Heidelberg (1997)
11. Sholz, A.: Aufgabe 253. Jahresbericht der deutschen Mathematiker-Vereinigung 47, 41–42 (1937)
12. Subbarao, M.: Addition chains - some results and problems. Number Theory and Applications, 555–574 (1989)
13. Yao, A.C.: On the evaluation of powers. SIAM Journal on Computing 5(1), 100–103 (1976)
14. Yao, A.C., Knuth, D.E.: Analysis of the substractive algorithm for greatest common divisors. Proc. Nat. Acad. Sci. USA 72(12), 4720–4722 (1975)

Optimal Authentication Codes from Difference Balanced Functions*

Yang Yang[1], Xiaohu Tang[1], and Udaya Parampalli[2]

[1] Institute of Mobile Communications, Southwest Jiaotong University
Chengdu, Sichuan, 610031, PRC, China
yang_data@yahoo.cn, xhutang@ieee.org
[2] Department of Computer Science and Software Engineering
University of Melbourne, VIC 3010, Australia
udaya@cs.mu.oz.au

Abstract. In this paper, we present two classes of optimal authentication codes without secrecy from difference balanced functions. The new codes are as good as or have more flexible parameters than the optimal codes from perfect nonlinear functions.

Keywords: Difference balanced functions, perfect nonlinear functions, authentication code, impersonation attack, substitution attack.

1 Introduction

One of the main problems in the communication field is the integrity of the messages. In the public communication channel, there exist the opponents except for the sender and the receiver. The opponents may have the ability to intercept the messages, modify the existing messages or/and insert a new message to the public communication channel. Thus, authentication codes are being developed to provide a solution to this scenario [16].

Authentication code is a four-tuple $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E})$, where $\mathcal{S}$ is the source state space associated with a probability distribution, $\mathcal{T}$ is the tag space, $\mathcal{K}$ is the key space associated with a probability distribution, and $\mathcal{E}$ is a set consisting of all encoding rules $E_k : \mathcal{S} \to \mathcal{T}, k \in \mathcal{K}$. In this paper, we assume that all source states and all keys are used equally likely.

For the authentication code, the secret key k shared by both the sender and receiver can be used for both encryption and authentication purpose. Accordingly, authentication codes come with two flavors, with or without secrecy. In an authentication code with secrecy, a source state s is sent to the receiver in an encrypted form. In an authentication code without secrecy, a source state s is sent to the receiver in a plaintext. The connections between coding theory and authentication codes without secrecy are well known [10,11]. Several approaches

* This work was in part supported by Australia-China Special Fund under Grant 61011120055.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 298–304, 2010.

are presented to construct authentication codes without secrecy using error correcting codes: the q-twist construction [11], the construction using rank distance code [18], and Gauss sum construction [1,9], cartesian authentication code [4,6], the constructions by using perfect nonlinear (PN) functions and almost perfect nonlinear (APN) functions [2,3,5].

Difference balanced function is a class of function with perfect difference property [7], which has been used to construct sequences with low correlations [8,12]. Our concern in this paper is to explore its application in authentication codes. As a result, we establish a generic connection between optimal authentication codes without secrecy and difference balanced functions, which give two constructions of optimal authentication codes without secrecy. The first one is as good as that constructed from PN functions, while the second one has more flexible parameters.

Finally, we conclude this section by introducing the following notations which will be used throughout this paper.

- q: a power of a prime p;
- n, m, l: three positive integers with $m|n$ and $l \leq m$;
- $GF(q^n), GF(q^m)$: two finite fields with q^n and q^m elements;
- $Tr_{q^n/q^m}(x) = \sum_{i=0}^{n/m-1} x^{q^{mi}}, x \in GF(q^n)$: the trace function from $GF(q^n)$ to $GF(q^m)$.

2 Authentication Codes

In [16], Simmons established a generic authentication model. He distinguished two different types spoofing attack, i.e., *impersonation attack* and *substitution attack*.

In the impersonation attack, the opponent wants to generate a message (s, t) so that the probability $Pr(t = E_k(s))$ is maximal, where $s \in \mathcal{S}$ and $t \in \mathcal{T}$. The maximum probability of success of the impersonation attack is

$$P_I = \max_{s \in \mathcal{S}, t \in \mathcal{T}} \frac{|\{k \in \mathcal{K} : \ t = E_k(s)\}|}{|\mathcal{K}|} \tag{1}$$

where $|A|$ denotes the cardinality of the set A. In the substitution attack, the opponent observes a message (s, t) and replaces it with another message (s', t') so that the probability $Pr(t' = E_k(s')|t = E_k(s))$ is maximal, where $s \neq s'$. The maximum probability of success of the substitution attack is

$$P_S = \max_{s \in \mathcal{S}, t \in \mathcal{T}} \max_{\substack{s' \in \mathcal{S}, s \neq s' \\ t' \in \mathcal{T}}} \frac{|\{k \in \mathcal{K} : \ t = E_k(s), t' = E_k(s')\}|}{|\{k \in \mathcal{K} : \ t = E_k(s)\}|}. \tag{2}$$

By choosing certain messages, the opponent can successful cheat. So the two maximum probabilities of authentication codes must be as small as possible. However, there exist the following lower bounds on P_I and P_S [15]:

$$P_I \geq \frac{1}{|\mathcal{T}|}, \quad \text{and} \quad P_S \geq \frac{1}{|\mathcal{T}|}. \tag{3}$$

The authentication code is called *optimal* if the equalities in (3) hold.

3 Authentication Codes from Functions with Difference Balanced Property

In this section, we will construct authentication codes from functions with difference balanced property.

3.1 A Generic Construction of Optimal Authentication Codes from Difference Balanced Functions

Definition 1. *A function $f(x)$ from $GF(q^n)$ to $GF(q^m)$ is said to be balanced if any element of $GF(q^m)$ appears q^{n-m} times with x ranging over $GF(q^n)$.*

Definition 2. *A function $f(x)$ from $GF(q^n)$ to $GF(q^m)$ is said to be difference balanced, if for any $\delta \in GF(q^n) \setminus \{0, 1\}$, the difference $f(\delta x) - f(x)$ is balanced.*

So far, there are three types of difference balanced functions [8,17]:

(1) $f(x)$ is a single trace form taken from binary and nonbinary m-sequences, i.e.,

$$f(x) = Tr_{q^n/q}(x^d) \tag{4}$$

where n and d are positive integers such that $\gcd(d, q^n - 1) = 1$.

(2) $h(x)$ is the Helleseth-Gong (HG) function extracted from nonbinary HG sequence defined in [8] by

$$h(x) = Tr_{q^n/q^m}\Big(\sum_{i=0}^{t} u_i x^{(q^{2mi}+1)/2}\Big) \tag{5}$$

where $n = (2t+1)m$, $1 \le s \le 2t+1$ is an integer such that $\gcd(s, 2t+1) = 1$, $b_0 = 1$, $b_{is} = (-1)^i$ and $b_i = b_{2t+1-i}$ for $i = 1, 2, \cdots, t$, $u_0 = b_0/2 = (p+1)/2$, and $u_i = b_{2i}$ for $i = 1, 2, \cdots, t$.

(3) *Composite difference balanced functions:* This class accounts for all the difference balanced functions that are composite function of the two classes of difference balanced functions $f(x)$ and $h(x)$ above, for example

$$g_1(x) = tr_{q^{n_1}/q}\big[tr_{q^{n_2 \cdot n_1}/q^{n_1}}(x^{d_2})\big]^{d_1},$$

$$g_2(x) = tr_{q^{n_1}/q}\Big[tr_{q^{n_2 \cdot n_1}/q^{n_1}}\Big(\sum_{i=0}^{m} u_i x^{(q^{2n_1 ki}+1)/2}\Big)\Big]^{d_1},$$

in which n_1, $n_2 = (2m+1)k$, d_1, and d_2 are positive integers, $\gcd(d_1, q^{n_1} - 1) = 1$, and $\gcd(d_2, q^{n_1 \cdot n_2} - 1) = 1$.

It should be noted that all the difference balanced functions above are d-form functions [13].

Definition 3. *Let d be an integer with $\gcd(d, q^m - 1) = 1$. A function $h(x)$ from $GF(q^n)$ onto $GF(q^m)$ is a d-form function if*

$$h(yx) = y^d h(x) \tag{6}$$

for any $y \in GF(q^m)$ and $x \in GF(q^n)$.

It is easy to see that $f(x)$ in (4) is d-form, $h(x)$ in (5) is 1-form, $g_1(x)$ is $(d_1 \cdot d_2)$-form, and $g_2(x)$ is d_1-form.

The following relationship of d-from function between balanced property and difference balanced property is well-known [14].

Lemma 1. *If a d-form function $f(x)$ from $GF(q^n)$ to $GF(q^m)$ is difference balanced, then $f(x)$ is balanced.*

By Lemma 1, we have

Lemma 2. *Let $f(x)$ be a d-form function from $GF(q^n)$ to $GF(q^m)$ with difference balanced property. For any $s, s' \in GF(q^n)$ with $s \neq s'$, $f(sx) - f(s'x)$ is balanced.*

Proof. If $s = 0$, then $s' \neq 0$ and $f(sx) - f(s'x) = -f(s'x)$ is a balanced function by Lemma 1. Similarly, $f(sx) - f(s'x) = f(sx)$ is balanced if $s' = 0$.

If $s \neq 0$ and $s' \neq 0$, then $s(s')^{-1} \neq 0, 1$. Let $y = s'x$, then $f(sx) - f(s'x) = f(s(s')^{-1}y) - f(y)$ is balanced due to the difference balanced property of $f(y)$. □

Based on the functions with difference balanced property, we can easily construct optimal authentication codes.

Theorem 1. *Let $f(x)$ be a d-form function with difference balanced property from $GF(q^n)$ to $GF(q)$. Define an authentication code as follows:*

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}) = (GF(q^n), GF(q), GF(q^n) \times GF(q), \{E_k : k \in \mathcal{K}\})$$

where for any $k = (k_0, k_1) \in GF(q^n) \times GF(q)$ and $s \in \mathcal{S}$,

$$E_k(s) = f(sk_0) + k_1.$$

Then such code has parameters $\mathcal{S} = q^n$, $|\mathcal{T}| = q$ and $|\mathcal{K}| = q^{n+1}$,

$$P_I = P_S = \frac{1}{q}.$$

and is optimal.

Proof. For any fixed $s \in GF(q^n)$ and $t \in GF(q)$, $k_1 = t - f(sk_0)$ is uniquely determined by given $k_0 \in GF(q^n)$. Thus we have $|\{(k_0, k_1) \in \mathcal{K} : f(sk_0) + k_1 = t\}| = q^n$, and then

$$P_I = \frac{q^n}{q^{n+1}} = \frac{1}{q}.$$

Let $s, s' \in \mathcal{S}$, $s \neq s'$ and $t, t' \in \mathcal{T}$. Then we have

$$\begin{aligned}
&|\{(k_0, k_1) \in \mathcal{K} : \ f(sk_0) + k_1 = t, \ f(s'k_0) + k_1 = t'\}| \\
&= |\{(k_0, k_1) \in \mathcal{K} : \ f(sk_0) - f(s'k_0) = t - t', \ f(s'k_0) + k_1 = t'\}| \\
&= |\{k_0 \in GF(q^n) : \ f(sk_0) - f(s'k_0) = t - t'\}| \\
&= q^{n-1}
\end{aligned}$$

where k_1 is cancel in the right hand side of the second equation since it is uniquely determined by k_0 and the last equality is due to the balanced property of $f(sx) - f(s'x)$ given by Lemma 2. Thus the maximum probability of success of the substitution attack is

$$P_S = \frac{q^{n-1}}{q^n} = \frac{1}{q}. \qquad \square$$

3.2 The Second Class of Optimal Authentication Codes with Flexible Parameters

Before presenting the second construction, we need the following lemma.

Lemma 3. *Let $a_1, a_2, \cdots, a_l \in GF(q^m)$ be l elements linearly independent over $GF(q)$. Then the following system of equations*

$$\begin{cases} Tr_{q^m/q}(a_1 y) = b_1 \\ Tr_{q^m/q}(a_2 y) = b_2 \\ \qquad\qquad \vdots \\ Tr_{q^m/q}(a_l y) = b_l \end{cases}$$

has q^{m-l} solutions for any given $b_i \in GF(q)$, $i = 1, 2, \cdots, l$.

Proof. The system of equations in l variables $y, y^q, \cdots, y^{q^{l-1}}$ has a coefficient matrix as follows:

$$A = \begin{pmatrix} a_1 & a_1^q & \cdots & a_1^{q^{l-1}} \\ a_2 & a_2^q & \cdots & a_2^{q^{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_l & a_l^q & \cdots & a_l^{q^{l-1}} \end{pmatrix}.$$

Since $a_1, a_2, \cdots, a_l \in GF(q^m)$ are linearly independent over $GF(q)$, the rank of A is equal to l. This finishes the proof. $\square$

Now we introduce the construction of authentication codes.

Theorem 2. *Let $a_1, a_2, \cdots, a_l \in GF(q^m)$ be l elements linearly independent over $GF(q)$. Let $f(x)$ be a function from $GF(q^n)$ to $GF(q^m)$ with difference balanced property. Define a code as follows:*

$$(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E}) = (GF(q^n), GF(q)^l, GF(q^n) \times GF(q)^l, \{E_k : k \in \mathcal{K}\})$$

where for any $s \in \mathcal{S}$, $k = (k_0, k_1, \cdots, k_l) \in GF(q^n) \times GF(q) \times \cdots \times GF(q)$,

$$E_k(s) = (Tr_{q^m/q}(a_1 f(sk_0)) + k_1, \cdots, Tr_{q^m/q}(a_l f(sk_0)) + k_l).$$

Then the code has parameters $|\mathcal{S}| = q^n, |\mathcal{T}| = q^l, |\mathcal{K}| = q^{n+l}$,

$$P_I = P_S = \frac{1}{q^l}$$

and meets the bounds of (3).

Proof. For any given $s, k_0 \in GF(q^n)$ and $(t_1, t_2, \cdots, t_l) \in GF(q)^l$, there exists a unique k_i such that $k_i = t_i - Tr_{q^m/q}(a_i f(sk_0))$, i.e.,

$$|\{k \in \mathcal{K} : Tr_{q^m/q}(a_i f(sk_0)) + k_i = t_i, i = 1, 2, \cdots, l\}| = q^n.$$

Thus we have

$$P_I = \frac{q^n}{q^{n+l}} = \frac{1}{q^l}.$$

For any $s, s' \in GF(q^n)$, $s \neq s'$ and $t = (t_1, t_2, \cdots, t_l), t' = (t'_1, t'_2, \cdots, t'_l) \in GF(q)^l$, consider the number of solutions to the system of equations

$$\begin{cases} Tr_{q^m/q}(a_i f(sk_0)) + k_i = t_i, \ i = 1, 2, \cdots, l \\ Tr_{q^m/q}(a_i f(s'k_0)) + k_i = t'_i, \ i = 1, 2, \cdots, l \end{cases} \tag{7}$$

Again by the fact that k_i is uniquely determined by k_0, the system of equations in (7) can then be reduced as

$$Tr_{q^m/q}(a_i(f(sk_0) - f(s'k_0))) = t_i - t'_i, \ i = 1, 2, \cdots, l. \tag{8}$$

By Lemma 2, for any given $y \in GF(q^m)$, the equation $y = f(sk_0) - f(s'k_0)$ has q^{n-m} solutions $k_0 \in GF(q^n)$. Hence, by Lemma 3, (8) and (7) have $q^{n-m} \cdot q^{m-l} = q^{n-l}$ solutions in $GF(q^n) \times GF(q)^l$. We have

$$P_S = \frac{q^{n-l}}{q^n} = \frac{1}{q^l}.$$

□

3.3 Comparison between Our Codes and Codes from Perfect Nonlinear Functions in [3]

Theorem 16 of [3], the authors construct authentication codes in with parameters

$$|\mathcal{S}| = q^n, |\mathcal{T}| = q, |\mathcal{K}| = q^{n+1}, P_I = P_S = \tfrac{1}{q}$$

using perfect nonlinear functions. Obviously, our codes in Theorem 1 are as good as those codes in [3].

Now we compare those codes with our codes in Theorem 2 of this paper. If l is a factor of n, then the parameters of our codes are the same as those of the codes in Theorem 16 of [3]; Otherwise, the parameters of our codes can not be obtained by those of the codes in Theorem 16 of [3]. So the parameters of our codes in Theorem 2 are more flexible than those of the codes in [3].

4 Conclusion

In this paper, we first present a generic construction of authentication codes from difference balanced functions and an extensive class of authentication codes. It is shown that the newly proposed codes are: (1) either as good as the optimal codes from PN functions given in [3]; (2) or more flexible than the latter with respect to the parameters.

Note that difference balanced functions which are mainly used in the literature to construct sequences can also be applied to authentication codes and they lead to results with flexible parameters. It is surprising that this potential of difference balanced functions was not realized earlier.

References

1. Bini, G.: A-codes from rational functions over galois rings. Designs, Codes and Cryptography 39, 207–214 (2006)
2. Carlet, C., Ding, C.: Authentication schemes from highly nonlinear functions. In: ISIT 2006, Seattle, USA (July 2006)
3. Chanson, S., Ding, C., Salomaa, A.: Cartesian authentication codes from functions with optimal nonlinearity. Theoretical Computer Science 290, 24–33 (2003)
4. Ding, C., Helleseth, T., Klϕve, T., Wang, X.: A generic construction of cartesian authentication code. IEEE Trans. Inform. Theory 53(6), 2229–2235 (2007)
5. Ding, C., Niederreiter, N.: Systematic authentication code from highly nonlinear functions. IEEE Trans. Inform. Theory 50(10), 2421–2428 (2004)
6. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theoretical Computer Science 330, 81–99 (2005)
7. Golomb, S.W., Gong, G.: Signal design for good correlation for wireless communication, cryptography and radar. Cambridge Press, Cambridge (2005)
8. Helleseth, T., Gong, G.: New binary sequences with ideal-level autocorrelation function. IEEE Trans. Inform. Theory 154(18), 2868–2872 (2002)
9. Helleseth, T., Johansson, T.: Universal hash functions from exponential sums over finite fields and galois rings. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 31–44. Springer, Heidelberg (1996)
10. Kabatianskii, G.A., Sweets, B., Joansson, T.: On the relationship between A-codes and codes correcting independent errors. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 1–11. Springer, Heidelberg (1994)
11. Kabatianskii, G.A., Sweets, B., Joansson, T.: On the cardinality of systematic authentication codes via error-correcting codes. IEEE Trans. Inform. Theory 42(2), 566–578 (1996)
12. Jang, J.-W., Kim, Y.-S., No, J.-S., Helleseth, T.: New family of p-ary sequences with optimal correlation property and large linear span. IEEE Trans. Inform. Theory 50(8), 1839–1844 (2004)
13. Klapper, A.: d-from sequence: Families of sequences with low correlaltion values and large linear spans. IEEE Trans. Inform. Theory 51(4), 1469–1477 (1995)
14. No, J.-S.: New cyclic difference sets with Singer parameters constructed from d-homogeneous function. Designs, Codes and Cryptography 33, 199–213 (2004)
15. Stinson, D.R.: Cryptography: Theory and Practice. CRC, Boca Raton (1995)
16. Simmons, G.J.: Authentication theory/coding theory. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 411–431. Springer, Heidelberg (1985)
17. Tang, X.H.: A note on d-form function with differencebalanced property (Preprint)
18. Wang, H., Xing, C., Safavi-Naini, R.: Linear authentication codes: Bounds and constructions. IEEE Trans. Inform. Theory 49(4), 866–872 (2003)

New Extensions and Applications of Welch-Bound-Equality Sequence Sets*
(Invited Paper)

James L. Massey

Prof.-em. ETH-Zürich and JLM Consulting,
Trondhjemsgade 3, 2TH,
DK-2100 Copenhagen East, Denmark
jamesmassey@compuserve.com

Abstract. This paper gives a sampling of the results on Welch-Bound-Equality sequence sets that were presented in the keynote lecture on which this paper is based. Emphasis is placed on identities that lend themselves to use in the design and analysis of good sequence sets.

Keywords: Welch's bound, correlation functions, WBE sequence sets.

1 Preliminaries

Let $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ be vectors in $\mathcal{C}^L$ where $\mathcal{C}$ is the complex field. These vectors form a *set* of sequences of length L, or a *multiset* of sequences of length L, depending on whether the M vectors are all distinct or include duplicates. When a statement applies equally well to a sequence set or to a sequence multiset, we will write "(multi)set". We write $\langle \mathbf{x}^{(i)}, \mathbf{x}^{(j)} \rangle$ to denote the usual inner product between $\mathbf{x}^{(i)}$ and $\mathbf{x}^{(j)}$ in $\mathcal{C}^L$.

Welch [1] has derived a very useful bound on the correlation of a sequence set in which all sequences have the same "energy" (which can and will be taken as L with no loss of essential generality), i.e., $\langle \mathbf{x}^{(i)}, \mathbf{x}^{(i)} \rangle = L$. This bound is usually stated in terms of the maximum correlation between sequences in the (multi)set, but in our opinion it is more fundamentally stated as a bound on the total squared correlation between pairs of signals as we do now.

Bound 1. *Welch's Bound: Let* $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ *be a multiset of equal-energy complex sequences of length* L *and energy* L*. Then*

$$\sum_{i=1}^{M} \sum_{j=1}^{M} \|\langle \mathbf{x}^{(i)}, \mathbf{x}^{(j)} \rangle\|^2 \geq M^2 L \tag{1}$$

Equality holds in (1) if and only if the $M \times L$ *array having* $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ *as rows has equal-energy and pairwise-orthogonal columns. Moreover, when equality holds, the sequences are* uniformly good *in the sense that*

* This work was supported in part by the European Space Agency under Contract No.22369/09/NL/JK performed under subcontract with Thales Alenia Space Italia.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 305–308, 2010.

$$\sum_{j=1}^{M} \|\langle \mathbf{x}^{(i)}, \mathbf{x}^{(j)} \rangle\|^2 = ML \tag{2}$$

for $1 \le i \le M$.

The condition for equality in (1) was first derived in [2]; the "uniformly good" property (2) was first shown in [3].

Sequence (multi)sets that achieve equality in (1) were called *Welch-Bound-Equality (WBE) sequence (multi)sets* in [3] where the close connection between these WBE sequence sets and cyclic codes was pointed out and where many constructions of WBE sequence sets were given.

2 Correlation Functions

The *periodic crosscorrelation function* (or *even crosscorrelation function*) between the sequences $\mathbf{x^{(i)}}$ and $\mathbf{x^{(j)}}$ in $\mathcal{C}^L$ is the function

$$R_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(k) = \langle \mathbf{x}^{(i)}, T^k \mathbf{x}^{(j)} \rangle \quad \text{for } 0 \le k < L, \tag{3}$$

where T is the left cyclic shift operator on sequences of length L. When $i = j$, $R_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(.)$ is called the *periodic autocorrelation function* (or *even autocorrelation function*) and denoted simply as $R_{\mathbf{x}^{(i)}}(.)$.

Gold [4] proved the following result for even correlation functions.

Identity 1. *Gold's identity:*

$$\sum_{k=0}^{L-1} R_{\mathbf{x}^{(i)}}(k) R_{\mathbf{x}^{(j)}}(k) = \sum_{k=0}^{L-1} (R_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(k))^2. \tag{4}$$

The *odd crosscorrelation function* between the sequences $\mathbf{x^{(i)}}$ and $\mathbf{x^{(j)}}$ in $\mathcal{C}^L$ is the sequence

$$O_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(k) = \langle \mathbf{x}^{(i)}, N^k \mathbf{x}^{(j)} \rangle \quad \text{for } 0 \le k < L, \tag{5}$$

where N is the left *compacyclic* shift operator on sequences of length L introduced by Seguin [5], i.e., the operator that shifts each component one position leftwards, except for the first component which is changed in sign and moved to the rightmost position. When $i = j$, $O_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(.)$ is called the *odd autocorrelation function* and denoted as $O_{\mathbf{x}^{(i)}}(.)$.

Pursley and Sarwate [6] proved the following interesting result for odd correlation functions.

Identity 2. *Pursley-Sarwate identity:*

$$\sum_{k=0}^{L-1} O_{\mathbf{x}^{(i)}}(k) O_{\mathbf{x}^{(j)}}(k) = \sum_{k=0}^{L-1} (O_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(k))^2. \tag{6}$$

3 Extensions

We first note that if $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ is a WBE (multi)set of equal-energy complex sequences of length L and energy L, then so is the cyclically shifted (multi)set $T^k\mathbf{x}^{(1)}, T^k\mathbf{x}^{(2)}, \ldots, T^k\mathbf{x}^{(M)}$. This follows from Bound 1 and the fact that pairwise orthogonality of the columns of the matrix with $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ as rows implies the pairwise orthogonality of the columns of the matrix with $T^k\mathbf{x}^{(1)}, T^k\mathbf{x}^{(2)}, \ldots, T^k\mathbf{x}^{(M)}$ as rows. Moreover, the union of these two (multi)sets is also a WBE (multi)set. Now making use of the uniformly good property (2) of WBE sequence multisets and invoking the definition (3), we obtain after a little algebra the following identity, which appears to be new.

Identity 3. *If $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ is a WBE (multi)set of equal-energy complex sequences of length L and energy L, then*

$$\sum_{j=1}^{M} (R_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(k))^2 = ML \quad \text{for } 0 \le k < L. \tag{7}$$

We next note that if $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ is a WBE (multi)set of equal-energy complex sequences of length L and energy L, then so is the compacyclically shifted (multi)set $N^k\mathbf{x}^{(1)}, N^k\mathbf{x}^{(2)}, \ldots, N^k\mathbf{x}^{(M)}$. This follows again from the Bound 1 and the fact that pairwise orthogonality of the columns of the matrix with $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ as rows implies the pairwise orthogonality of the columns of the matrix with $N^k\mathbf{x}^{(1)}, N^k\mathbf{x}^{(2)}, \ldots, N^k\mathbf{x}^{(M)}$ as rows. Moreover, the union of these two (multi)sets is also a WBE (multi)set. Now making use of the uniformly good property (2) of WBE sequence multisets and invoking the definition (5), we obtain after some algebra the following identity, which again appears to be new.

Identity 4. *If $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(M)}$ is a WBE (multi)set of equal-energy complex sequences of length L and energy L, then*

$$\sum_{j=1}^{M} (O_{\mathbf{x}^{(i)}\mathbf{x}^{(j)}}(k))^2 = ML \quad \text{for } 0 \le k < L. \tag{8}$$

Identities 3 and 4 suggest that WBE sequence (multi)sets can be expected to have odd correlation properties that are just as good as the usual periodic (or "even") correlation properties usually considered in the analysis of sequence (multi)sets.

References

1. Welch, L.R.: Lower Bounds on the Maximum Cross Correlation of Signals. IEEE Trans. Information Theory IT-20, 397–399 (1974)
2. Massey, J.L.: On Welch's Bound for the Correlation of a Sequence Set. In: Proc. IEEE Intl. Symp. Information Theory, Budapest, p. 385 (1991)

3. Massey, J.L., Mittelholzer, T.: Welch's Bound and Sequence Sets for Code-Divison Multiple-Access Systems. In: Capocelli, R., De Santis, A., Vaccaro, U. (eds.) Sequences II: Methods in Communication, Security and Computer Sciences, pp. 63–78. Springer, Heidelberg (1993)
4. Gold, R.: Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions. IEEE Trans. Information Theory IT-14, 154–156 (1968)
5. Seguin, G.: Binary Sequences with Specified Correlation Properties. Ph.D. Thesis, Dept. of Elec. Engr., Univ. of Notre Dame, Notre Dame, IN (1972)
6. Sarwate, D.V., Pursley, M.B.: Evaluation of Correlation Parameters for Periodic Sequences. IEEE Trans. Information Theory IT-23, 508–513 (1977)

Evaluation of Randomness Test Results for Short Sequences

Fatih Sulak, Ali Doğanaksoy, Barış Ege, and Onur Koçak

Institute of Applied Mathematics,
Middle East Technical University, Ankara, Turkey
{sulak,aldoks,e132689,e132713}@metu.edu.tr

Abstract. Randomness testing of cryptographic algorithms are of crucial importance to both designer and the attacker. When block ciphers and hash functions are considered, the sequences subject to randomness testing are of at most 512-bit length, "*short sequences*". As it is widely known, NIST has a statistical test suite to analyze the randomness properties of sequences and generators. However, some tests in this suite can not be applied to short sequences and most of the remaining ones do not produce reliable test values for the sequences in question. Consequently, the analysis method which is proposed in this suite is not suitable for evaluation of generators which produce relatively short sequences. In this work, we propose an alternative approach to analyze short sequences without tweaking the tests.

1 Introduction

Random sequences are used in a large variety of areas, such as quantum mechanics, game theory, statistics, cryptography, and so on. These sequences can be generated either by physical sources or deterministic algorithms. In cryptography, some applications require transmitting large random sequences, which is inefficient, or regenerating random sequences, which is not possible for physical sources. Therefore, randomness in cryptography is achieved through deterministic algorithms, which are called pseudo random number generators (PRNGs). Analysis of PRNGs is performed by taking a sample sequence from them, and evaluating this sequence by statistical randomness tests. These statistical tests are designed to examine the randomness of a sequence through comparing certain characteristics of the sequence with the expected ones of a random sequence and producing a p-value as an output of this examination process.

Statistical testing of block cipher and hash function algorithms is essential, because the outputs of such algorithms should be random looking. As approximations and asymptotic approaches used in the distribution functions of statistical randomness tests force the user to use long sequences, a common approach to overcome this problem is to concatenate the outputs of block ciphers or hash functions to form long sequences. Using this approach, a method is proposed for statistical testing of block ciphers by Soto [1]. In this method, outputs of several different input data sets are tested with NIST test suite [2], by forming

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 309–319, 2010.

sequences of length approximately 2^{20} bits through concatenation. However, the nature of block cipher and hash function algorithms necessitates devising tests and test parameters focused particularly on "*short sequences*", which are formed directly by the outputs of these algorithms.

Our aim is to test a generator which produces short sequences of length between 128 and 256 bits. To attain this, we improve the evaluation method given in [2] for the test results obtained from short sequences.

2 Evaluation of the Test Results

In this section, we first overview the method described in the NIST test suite for evaluation of the test results and point out why this method is not reliable for short sequences. Then, we propose an alternative approach to evaluate test results of short sequences.

2.1 The Method Proposed by NIST

NIST suggests two approaches to evaluate test results: examination of the proportion of sequences with a p-value greater than a certain bound; and the distribution of p-values. The latter one assumes that the p-values are uniformly distributed over the interval $[0, 1]$. A goodness of fit distribution test is performed to measure whether the p-values are uniform or not by dividing the interval $[0, 1]$ into 10 equal subintervals. Let m be the number of sequences tested, and F_i be the number of p-values in subinterval i for $i = 1, 2, \ldots, 10$. Then the χ^2 value and the corresponding p-value are calculated as

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - \frac{m}{10})^2}{\frac{m}{10}} \quad \text{and} \quad p\text{-value} = \texttt{igamc}\left(\frac{9}{2}, \frac{\chi^2}{2}\right)$$

where `igamc` is the incomplete gamma function. If p-value$\geq$0.0001, the test results are considered to be uniformly distributed [2].

However, when short sequences are in question, two main problems arise. First problem is noted in [2], *"the asymptotic reference distributions would be inappropriate and would need to be replaced by exact distributions that would commonly be difficult to compute"*. The second problem is that, for short sequences, the probability of a p-value being in a subinterval is not the same for all subintervals. This problem arises from the fact that the test parameters are discrete values, that is integer valued, where the asymptotic reference distribution assumes real valued inputs. To overcome these problems, we propose an alternative method to evaluate the test results of the short sequences.

2.2 The Alternative Approach

In this approach, we use the distribution functions as they are originally used in the NIST test suite, instead of replacing them with exact distributions. Then for each test, we compute the probability of a p-value being in a given subinterval.

NIST assumes that this probability is $\frac{1}{10}$ for 10 subintervals but this is not the case for short sequences. Hence, we compute the subinterval probabilities for each test. The bit lengths for the computations are chosen as; 128, 160 and 256 for evaluating the algorithms given in Section 3.

The distributions of p-values are computed by making a table consisting of the probabilities of all possible test variables, and the corresponding p-values. Thus, for each $i = 0, 1, \ldots, 9$, we need to compute

$$Pr\left(\frac{i}{10} \leq p\text{-value} \leq \frac{i+1}{10}\right).$$

Using these probabilities for subintervals we propose an improved method for evaluation of the test results. Let p_i be the probability of a p-value being in subinterval i, then

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - m \cdot p_i)^2}{m \cdot p_i} \quad \text{and} \quad p\text{-value} = \texttt{igamc}\left(\frac{9}{2}, \frac{\chi^2}{2}\right).$$

Similar to the approach proposed by NIST, when p-value$\geq$0.0001, the test results are considered to be distributed properly. For specific sequence lengths, the case $m \cdot p_i < 5$ may occur for some i. In that case, degree of freedom should be modified accordingly.

Considering the length of sequences in question, suitable tests in the NIST test suite are *Frequency Test*, *Frequency Test within a Block*, *Runs Test*, *Test for the Longest Run of Ones in a Block*, *Serial Test*, *Approximate Entropy Test* and *Cumulative Sums Tests*. In the remaining part of this section, we explain how the p_i's are computed for each of these tests. Also the distribution tables are given in Appendix B.

Frequency Test. Frequency Test compares the weight W (that is, the number of ones) of an n-bit sequence with the expected weight of a random sequence. The p-value of the sequence depends only on the weight W of the sequence as a variable. As for a given weight w, there are $\binom{n}{w}$ many n-bit sequences, the probability $Pr(W = w)$ is

$$Pr(W = w) = \frac{\binom{n}{w}}{2^n}.$$

We form a table which contains all possible weights with the corresponding p-values. For example, Table 1 shows p-values for Frequency Test according to the weights w for $n = 256$.

As it can be seen in Table 1, the p-value of a sequence is in the interval $[0.8, 0.9]$ if and only if the weight of the sequence is 126 or 130. In that case

$$Pr(0.8 < p\text{-value} < 0.9) = \frac{\binom{256}{126} + \binom{256}{130}}{2^{256}} \approx 0.0966.$$

Table 1. Weights and the corresponding p-values

w	$\lvert w - \frac{n}{2} \rvert$	p-value
125	3	0.707660
126	2	0.802587
127	1	0.900523
128	0	1.000000
129	1	0.900523
130	2	0.802587
131	3	0.707660

Frequency Test within a Block. This test separates the sequence into m-bit blocks and compares the proportion of ones in each block with the expected values for a random sequence. The variables used for computing p-values are the weights W_i of each block. Then, the probability for each p-value is calculated as,

$$Pr(W_i = w_i) = \frac{\prod_{i=1}^{\lfloor \frac{n}{m} \rfloor} \binom{m}{w_i}}{2^n} \ .$$

We choose $m = 32$ and calculate the corresponding subinterval probabilities.

Runs Test. A run is an uninterrupted maximal sequence of identical bits. In the Runs Test, the number of runs in the sequence is compared with the expected number of runs in a random sequence. The p-value is determined by the variables W and V, which denote the weight of the sequence and the number of runs in the sequence respectively. Now we need to compute $Pr(W = w_1, V = v_1)$ for a given sequence of length n, and calculate the probabilities of subintervals. We consider the question in two cases:

i) $v_1 = 2a$: Since there is an even number of runs, the number of runs of zeroes and ones are equal to each other. First we write ones and zeroes consecutively to define $2a$ runs. Now, we find the distribution of $(w_1 - a)$ many ones and $(n - w_1 - a)$ many zeroes so that the number of runs remains the same. The number of such distributions is equal to the number of non-negative integer solutions of the system

$$\begin{aligned} x_1 + x_2 + \cdots + x_a &= w_1 - a \\ y_1 + y_2 + \cdots + y_a &= n - w_1 - a \ . \end{aligned}$$

The first bit can be zero or one, then the probability is computed as:

$$Pr(W = w_1, V = 2a) = \frac{2\binom{w_1 - 1}{a-1}\binom{n - w_1 - 1}{a-1}}{2^n} \ .$$

ii) $v_1 = 2a+1$: If $v_1 = 1$, the only possibilities are all one and all zero sequences. Hence the probability for this case is $Pr(W = w_1, V = 1) = \frac{2}{2^n}$. Now, assume

that $a > 0$. Then, considering the first bit, the problem can be handled in two parts using the previous method. If the first bit is one, there are $(a+1)$ runs of ones and a runs of zeroes; if the first bit is zero, there are a runs of ones and $(a+1)$ runs of zeroes. The number of such distributions is equal to the number of non-negative integer solutions of the systems

$$\begin{aligned} x_1 + x_2 + \cdots + x_{a+1} &= w_1 - a - 1 \\ y_1 + y_2 + \cdots + y_a &= n - w_1 - a \end{aligned} \tag{1}$$

$$\begin{aligned} x_1 + x_2 + \cdots + x_a &= w_1 - a \\ y_1 + y_2 + \cdots + y_{a+1} &= n - w_1 - a - 1 \ . \end{aligned} \tag{2}$$

Therefore, the probability is computed as:

$$Pr(W = w_1, V = 2a+1) = \begin{cases} \frac{\binom{w_1-1}{a}\binom{n-w_1-1}{a-1} + \binom{w_1-1}{a-1}\binom{n-w_1-1}{a}}{2^n} & \text{if } a \neq 0 \\ \frac{2}{2^n} & \text{if } a = 0 \ . \end{cases}$$

As stated in NIST test suite, if $\left|\frac{W}{n} - \frac{1}{2}\right| \geq \frac{2}{\sqrt{n}}$, the p-value is set to 0. Hence, the subinterval probabilities are calculated regarding this.

Test for the Longest Run of Ones in a Block. This test separates the sequence into m bit blocks, and compares whether the length of the longest run of ones of the blocks are consistent with the expected number of those for a random sequence. We choose $m = 8$ and use the same categories, as NIST suggested [2]. Therefore, denoting the length of the longest run of ones within a block as V, we get $q_0 = Pr(V \leq 1) = 55/256$, $q_1 = Pr(V = 2) = 94/256$, $q_2 = Pr(V = 3) = 59/256$ and $q_3 = Pr(V \geq 4) = 48/256$. Here, the only variables for the calculation of p-values are the frequencies of the longest runs of ones in each category (V_i). In that case, $d = \lfloor n/8 \rfloor$ implies that, for each $i = 0, \ldots, 3$ we have

$$Pr(V_i = x_i) = \frac{\binom{d}{x_0}\binom{d-x_0}{x_1}\binom{d-x_0-x_1}{x_2}\binom{d-x_0-x_1-x_2}{x_3} {q_0}^{x_0} {q_1}^{x_1} {q_2}^{x_2} {q_3}^{x_3}}{2^n} \ .$$

Approximate Entropy Test and Serial Test. Approximate Entropy Test compares the frequencies of overlapping m and $(m+1)$-bit blocks of a sequence with the expected frequencies of those in a random sequence. Similarly, Serial Test focuses on the frequencies of overlapping m and $(m-1)$-bit blocks of a sequence. We take $m = 1$ for Approximate Entropy Test, and $m = 2$ for Serial Test. In both cases, the p-values are determined by the frequencies of 1-bit and 2-bit blocks.

Let X denote the number of zeroes, and Y denote the number of ones in an n-bit sequence. For 2-bit blocks, the first bit of the sequence is appended to the end of the sequence. Now, let A, B, C and D denote the number of `00`, `01`, `10` and `11` overlapping blocks respectively.

The p-values of both tests are computed depending on variables X, Y, A, B, C and D.

We first note some immediate facts:

Fact 1. *For any sequence the number of* `01` *blocks is equal to the number of* `10` *blocks (that is,* $B = C$*).*

Each run in the sequence defines either a `01` or a `10` block, if the sequence contains more than one runs. Also, in two consecutive runs, there will be a `01` and a `10` block. Considering the overlapping blocks, the number of runs will be even, which implies $B = C$.

Fact 2. $X{=}A{+}B$.

Any `00` or `10` block is defined by a `0` bit. Therefore, the total number of `00` and `10` blocks sum up to the number of zeroes.

Since $A + B + C + D = n$, if n, X, and B are known, the values of the other parameters can easily be computed using the facts above. Our aim is to compute the probability $Pr(B = b, X = x)$. Now, if $b = 0$, the sequence is either an all one or an all zero sequence. Thus the probability $Pr(B = 0, X = x) = \frac{2}{2^n}$. If $b > 0$, the probability $Pr(B = b, X = x)$ is computed in three steps assuming the bits are arranged on a circle to visualize the overlapping characteristic of the test. First, locate b many `01` blocks on the circle. Then place $(x - b)$ many zeroes between `01` blocks. The number of different arrangements is equal to the number of non-negative integer solutions of the equation $x_1 + x_2 + \cdots + x_b = x - b$ which is $\binom{x-1}{b-1}$. Afterwards, locate the remaining $(n - x - b)$ many ones. These bits can not be placed between zeroes, otherwise the number of `01` blocks would increase. Therefore, these ones should be placed adjacent to other ones on the circle. The number of such arrangements is equal to the number of non-negative integer solutions of the equation $x_1 + x_2 + \cdots + x_b = n - x - b$ which is equal to $\binom{n-x-1}{b-1}$.

Here, each arrangement on the circle gives n sequences. However, since there are b many `01` blocks, b of these sequences are identical. Therefore, the probability $Pr(B = b, X = x)$ is equal to the number of different arrangements divided by all possible n bit sequences which gives,

$$Pr(B = b, X = x) = \begin{cases} \frac{\binom{x-1}{b-1}\binom{n-x-1}{b-1}\frac{n}{b}}{2^n} & \text{if } s > 0 \\ \frac{2}{2^n} & \text{otherwise .} \end{cases}$$

Cumulative Sums Test. Cumulative Sums Test evaluates the sequence as a random walk and compares the maximum distance of the random walk from the x-axis to the expected value for a random sequence. The only variable for computing the p-value is the variable z, which is the maximum distance of random walk from the x-axis. Note that the test produces two p-values; one from producing the random walk from left to right, and one from right to left. Hence, we need to calculate $Pr(z = r)$ for a given sequence of length n. Assume that we know the weight W of a sequence. Then,

$$Pr(z < r | W = w) = \begin{cases} \frac{\binom{n}{w} - \sum_{i=1}^{\infty}\left(\left[\binom{n}{w-ir} + \binom{n}{n-w-ir}\right](-1)^{i+1}\right)}{2^n} & \text{if } r > |n - 2w| \\ 0 & \text{otherwise} \end{cases}$$

as in [3]. Considering all possible weights of an n-bit sequence, we get

$$Pr(z < r) = \sum_{w=0}^{n} Pr(z < r|W = w) \ .$$

Therefore, we get $Pr(z = r) = Pr(z < r + 1) - Pr(z < r)$.

3 Application to Block Ciphers and Hash Functions

Prior to testing cryptographic algorithms, the theoretical results mentioned in the previous section are applied to random data in order to check the reliability of these results. We test 10^6 pseudo-random sequences of lengths 128, 160 and 256 (taken from [4] and [5]) for randomness, using the alternative approach proposed in Section 2.2. The results match the expected p-value distributions calculated in the previous section, as the p-values obtained from these sources are all greater than 0.0001. These results can be seen in Table 2 and Table 3. In contrast to our results, same data are considered to be non-random as the p-values of the tests are smaller than 0.0001, when evaluated with the method proposed by NIST (see Table 4). Therefore, the approach of NIST is not suitable for testing short sequences.

Afterwards, we have applied our approach to test some block cipher and hash function algorithms for randomness. First, we test the finalists of AES selection process: MARS, RC6, Rijndael, Serpent and Twofish. In order to test these algorithms, integers from 0 to $(10^6 - 1)$ are encrypted using all zero key and then the ciphertext is XORed with the plaintext. This process is similar to the *plaintext-ciphertext correlation* in [1] except the plaintext is not random. Testing results of the 128-bit outputs, prepared in this way, are in Table 5. If all the p-values are greater than 0.0001 for a certain number of rounds, the algorithm is considered to behave random with at least that many rounds. Therefore, Mars

Table 2. Our test results for the random data from [4]

Random-DIEHARD								
Length	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
128	0.1249	0.4492	0.1390	0.6260	0.5581	0.4803	0.6440	0.3745
160	0.3266	0.6176	0.6775	0.0193	0.4575	0.5604	0.1485	0.6893
256	0.5803	0.9776	0.1091	0.1284	0.2609	0.2189	0.3347	0.2776

Table 3. Our test results for the random data from [5]

Random-Atmospheric Noise								
Length	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
128	0.9735	0.3525	0.0917	0.9502	0.3330	0.0125	0.4482	0.4824
160	0.9818	0.7928	0.5998	0.6720	0.7104	0.7838	0.9379	0.5580
256	0.5339	0.2856	0.4172	0.2722	0.9930	0.3656	0.2117	0.9161

Table 4. NIST test results for the random data from [4]

Random-DIEHARD								
Length	Freq	B.Freq	Run	L. Run	Ap. En.	C.Sum1	C.Sum2	Serial
128	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
160	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
256	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

achieves randomness in the first round, RC6 in the fourth round, Rijndael in the third round, Serpent and Twofish in the second round. These results are consistent with the results in [1] except for Serpent.

Hash algorithms are also tested in the same manner. The outputs are generated as in the block cipher case with initialization vectors set to zero, then 10^6 outputs of lengths 128, 160, and 256 are tested for MD4, SHA-1 and SHA-256 respectively. We consider the step functions of MD4 algorithm as three separate generators and produce outputs for each of them. As it can be seen in Table 6, MD4-IF achieves randomness in the sixth round, MD4-XOR and MD4-MAJORITY in the fourth round. Also, SHA-1 and SHA-256 achieve randomness in the eleventh and fifth round respectively.

4 Conclusion and Future Work

In this work, we calculated the probabilities of subintervals for each test, and proposed an alternative approach to evaluate test results for short sequences. Then, we applied our approach to test the randomness of some block cipher and hash function algorithms. As a future work, this study can be extended to other test suites or individual statistical tests. Moreover, this approach can be applied to evaluate the randomness of SHA-3 candidate algorithms.

References

1. Soto, J.: Randomness Testing of the AES Candidate Algorithms (1999), http://csrc.nist.gov/aes/
2. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S.: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (2001), http://www.nist.gov
3. Doğanaksoy, A., Çalık, Ç., Sulak, F., Turan, M.S.: New Randomness Tests Using Random Walk. In: National Cryptology Symposium II, Ankara (2006)
4. Marsaglia, G.: The Marsaglia Random Number CDROM Including The DIEHARD Battery of Tests of Randomness (1996), http://stat.fsu.edu/pub/diehard
5. Haahr, M.: Pregenerated Random Numbers, http://www.random.org/files/

A Results for Some Block Ciphers and Hash Functions

Table 5. Block Cipher Results

MARS								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
1	0.8698	0.3289	0.5914	0.8848	0.1702	0.3659	0.2129	0.5484
2	0.4330	0.3106	0.4138	0.4819	0.3953	0.3474	0.0906	0.3304
3	0.3328	0.9079	0.5933	0.3932	0.1405	0.2391	0.2145	0.1942
RC6								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
4	0.2504	0.2245	0.0371	0.1145	0.1413	0.0755	0.9803	0.1453
5	0.6958	0.7972	0.9787	0.1823	0.6092	0.9830	0.5004	0.3810
Rijndael								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
2	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
3	0.7717	0.4658	0.4507	0.3248	0.7001	0.1536	0.6747	0.8385
4	0.2878	0.5585	0.2322	0.3352	0.3156	0.8272	0.3832	0.6447
Serpent								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
1	0.0063	0.0000	0.1820	0.5037	0.5924	0.0000	0.0000	0.3469
2	0.3487	0.8226	0.0463	0.0599	0.5569	0.5131	0.6117	0.4858
3	0.3421	0.4239	0.5364	0.6143	0.4860	0.5027	0.4299	0.2736
Twofish								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
1	0.1557	0.4578	0.0000	0.0157	0.0000	0.0575	0.0009	0.0000
2	0.4383	0.7038	0.9565	0.7466	0.7321	0.4159	0.9779	0.6924
3	0.3933	0.0131	0.8354	0.8263	0.3163	0.0109	0.6482	0.2544

Table 6. Hash Function Results

MD4-IF								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
5	0.5274	0.0429	0.0069	0.1030	0.7345	0.0000	0.1613	0.6395
6	0.7797	0.6023	0.8079	0.1829	0.6171	0.4825	0.8867	0.5444
MD4-MAJORITY								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
4	0.0099	0.0725	0.0108	0.4089	0.8129	0.0025	0.0027	0.9536
5	0.3413	0.1881	0.0374	0.3737	0.0899	0.0479	0.7843	0.0391
MD4-XOR								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
4	0.4752	0.7832	0.9424	0.5294	0.3286	0.9390	0.8295	0.1527
5	0.5445	0.0367	0.1649	0.4447	0.9201	0.4628	0.8138	0.6849
SHA-1								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
10	0.6457	0.0000	0.0000	0.0186	0.0046	0.0118	0.0187	0.0029
11	0.3676	0.0611	0.0096	0.2313	0.0440	0.0659	0.8919	0.0149
12	0.4358	0.6513	0.8530	0.7604	0.6916	0.9537	0.0746	0.6042
SHA-256								
Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
5	0.8400	0.5539	0.3852	0.5205	0.8497	0.8933	0.9329	0.7359
6	0.4722	0.9613	0.3563	0.3588	0.9210	0.9630	0.9242	0.6938

B Probabilities of Subintervals

Table 7. Theoretical distributions of test results for individual sequence lengths

	Frequency			*Block Frequency*		
	128	**160**	**256**	**128**	**160**	**256**
1	0.092690	0.096569	0.091312	0.096702	0.101330	0.099498
2	0.091993	0.082208	0.097936	0.103781	0.096417	0.097137
3	0.146253	0.125283	0.098741	0.090851	0.103623	0.100424
4	0.095504	0.080507	0.128568	0.116406	0.099707	0.109070
5	0.109829	0.092315	0.075286	0.103756	0.107205	0.101255
6	0.122433	0.103247	0.082019	0.073678	0.095472	0.095544
7	0.000000	0.112633	0.087971	0.131696	0.105087	0.097023
8	0.132306	0.119853	0.092898	0.084071	0.101300	0.106247
9	0.138606	0.124405	0.096584	0.109276	0.098890	0.100846
10	0.070386	0.062980	0.148685	0.089780	0.090969	0.092955

	Runs			*Longest Run*		
	128	**160**	**256**	**128**	**160**	**256**
1	0.100679	0.101767	0.099315	0.095011	0.094127	0.094347
2	0.101395	0.098738	0.099622	0.104278	0.101135	0.104510
3	0.113361	0.106146	0.100594	0.101632	0.107367	0.105749
4	0.102226	0.094736	0.110248	0.106461	0.100669	0.101619
5	0.095862	0.094915	0.089509	0.102993	0.102986	0.090870
6	0.104063	0.101219	0.096585	0.120047	0.116485	0.112755
7	0.071873	0.103284	0.095026	0.077501	0.086725	0.096412
8	0.110294	0.105341	0.106260	0.109233	0.091818	0.097298
9	0.114290	0.110820	0.102243	0.089208	0.110189	0.098344
10	0.085956	0.083033	0.100598	0.093636	0.088499	0.098095

	Aproximate Entropy			*Cumulative Sums*		
	128	**160**	**256**	**128**	**160**	**256**
1	0.105734	0.102096	0.099245	0.083277	0.095534	0.091424
2	0.095735	0.099609	0.097256	0.102103	0.097604	0.091200
3	0.092841	0.103599	0.102839	0.079860	0.072497	0.085796
4	0.110089	0.089717	0.103637	0.104008	0.091824	0.109924
5	0.091082	0.113919	0.098356	0.130600	0.113019	0.090897
6	0.119882	0.079515	0.098838	0.078669	0.067413	0.103963
7	0.077519	0.111236	0.096122	0.076607	0.141934	0.114207
8	0.119499	0.095412	0.103614	0.086252	0.071586	0.060357
9	0.084588	0.092816	0.101217	0.153731	0.138093	0.111896
10	0.103031	0.112081	0.098876	0.104892	0.110497	0.140337

	Serial-1		
	128	**160**	**256**
1	0.101931	0.100969	0.097450
2	0.095514	0.093451	0.098970
3	0.101915	0.125194	0.099146
4	0.112556	0.061970	0.091051
5	0.082076	0.110750	0.114303
6	0.108904	0.095763	0.093207
7	0.089985	0.122586	0.094892
8	0.119499	0.084420	0.118739
9	0.084588	0.092816	0.093366
10	0.103031	0.112081	0.098876

Statistical Analysis of Search for Set of Sequences in Random and Framed Data

Dragana Bajić and Čedomir Stefanović

Department of Power, Electronics and Communication Engineering,
University of Novi Sad Trg Dositeja Obradovića 6,
21000 Novi Sad, Serbia
dragana.bajic@gmail.com, cex@uns.ac.rs

Abstract. In this paper we analyze the search for a set of predefined sequences in random and framed data and derive a number of corresponding statistical parameters. Most importantly, we derive probability mass function of the search process from which all moments can obtained. The presented solution is based on sequences' descriptors called cross-bifices, which express similarities among sequences in the set. The derived results can be used to evaluate the properties of frame-synchronization sequences.

Keywords: synchronization sequences, frame synchronization.

1 Introduction

The pioneering analysis of the search for a predefined sequence in random data stream was given in [1], where the term *bifix* was introduced to describe the sequence structure. A bifix is a subsequence that is both a prefix and a suffix of a longer sequence; its existence is denoted by corresponding *bifix-indicator*. Set of bifix-indicators can be defined for every sequence, describing its self-overlapping properties - matching between its prefices and suffices of equal length. The initial employment of the bifix indicators yielded the formula for the expected duration of a search for the first occurrence of a sequence in an infinite stream of random equiprobable data [1].

A possibility that the bifix analysis, as introduced in [1], could be applied to acquisition of frame synchronization was noticed in [2,3,4,5,6,7,8,9]. However, although frequently quoted, the results given in [1], were never extended to fully match frame synchronization issues; the only reference was the notion that frame synchronization sequences of practical interest should be *bifix-free*, i.e., without bifices.

The aim of this paper is to derive a comprehensive analytical description for the extended problem of search for the set of predefined sequences in random data stream and to apply it to the problem of the search in frame, both in error-free and erroneous conditions. The given analysis corresponds to practical low-complexity frame-synchronization algorithms that perform serial search with hard correlation, where a predefined threshold is used as the sequence detection

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 320–332, 2010.

criteria. Another example that falls within similar scenario is the search for distributed sequences [7,10].

The organization of the rest of the paper is as follows. In the next section we analyze the search for a set of sequences in a infinite stream of random data, introduce all the necessary prerequisites and derive the probability mass function (pmf) of the search process, its first and second moments. In the third section we extend the analysis to the practical case of framed data and investigate properties of synchronization sequences using developed tools. The final section gives the concluding remarks and outlines the topics for further research.

Some of the less important derivations presenting straightforward but extensive mathematical exercises are omitted due to their length; they are accessible at [11]. Preliminary versions of these results were presented in [12,13].

2 Search in Infinite Random Data Stream

We consider an infinite stream of random and independent data symbols x from an alphabet of size L, $x \in \{A_1, A_2, ..., A_L\}$, and assume that symbol values are not equiprobable, $\Pr\{x = A_l\} = p_l$, $1 \leq j \leq L$ and $\sum_{l=1}^{L} p_l = 1$. Our aim is to derive the probability of the first occurrence of a sequence belonging to the predefined set S, at a given position in the stream of random data; we will refer to this as a search for a set of sequences in random data stream. We assume that there are M sequences in the set S, $S = \{\mathbf{s}_1, \mathbf{s}_2, ..., \mathbf{s}_M\}$, and that each sequence from the set is N symbols long, $\mathbf{s}_i = [s_{i1}, s_{i2}, ..., s_{iN}]$, where s_{in} is the n-th symbol of the i-th sequence.

The search starts at a random position, denoted as position 1 (Fig. 1). The search process is modeled using sliding window of length N. Starting from the position 1, the window slides symbol by symbol through the stream and stops at the first occurrence of some sequence from the set S. Number of tests performed prior to the end of search is a random variable (its expected value and pmf for a simple case of equiprobable data and just one sequence were derived in [1] and [14], respectively).

In order to derive the pmf of the search process, we introduce the concepts of cross-bifices and suffix probability. Cross-bifix is a subsequence of length n, $0 \leq n \leq N$, that is both a suffix of some sequence from the set and a prefix of another one. The indicator related to the existence of cross-bifix of length n is

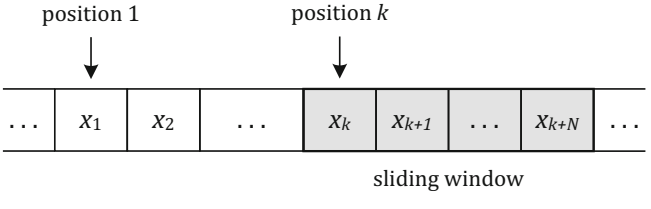


Fig. 1. Search in infinite random data stream

$h_{ji}^{(n)}$, where subscripts j and i denote respectively sequences $\mathbf{s}_j$ and $\mathbf{s}_j$, whose suffix and prefix are observed. The default values are:

$$h_{ji}^{(n)} = \begin{cases} 1 & n = 0, 1 \leq i, j \leq M \text{ or } n = N, j = i, \\ 0 & n = N, j \neq i. \end{cases} \tag{1}$$

Cross-bifix indicators for the given set S of M sequences can be written in matrices $\mathbf{h}^{(n)}$:

$$\mathbf{h}^{(n)} = \begin{bmatrix} h_{11}^{(n)} & \cdots & h_{1M}^{(n)} \\ \vdots & \ddots & \vdots \\ h_{M1}^{(n)} & \cdots & h_{MM}^{(n)} \end{bmatrix}, \; 0 \leq n \leq N. \tag{2}$$

Set S is cross-bifix free (analogous to the bifix-free sequences from [1]) if all its cross-bifix indicators are zero, except the default ones (Eq. 1).

Example 1 clarifies the above stated, where $S = \{\mathbf{s}_1, \mathbf{s}_2\}$, $\mathbf{s}_1 = [0\ 0\ 0]$ and $\mathbf{s}_2 = [1\ 0\ 0]$:

$$\mathbf{h}^{(0)} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \; \mathbf{h}^{(1)} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \; \mathbf{h}^{(2)} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \; \mathbf{h}^{(3)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3}$$

Additional parameter needed for the derivation of the pmf is suffix probability $r_i^{(n)}$, where subscript i denotes the sequence $\mathbf{s}_i$ and superscript n denotes the suffix length. Suffix probability $r_i^{(n)}$ is a product of probabilities of last n symbol values of the sequence $\mathbf{s}_i$. By default we assume $r_i^{(0)} = 1$. All suffix probabilities for a given set of sequences can be written in a matrix:

$$\mathbf{r} = \begin{bmatrix} r_1^{(0)} & \cdots & r_1^{(N)} \\ \vdots & \ddots & \vdots \\ r_M^{(0)} & \cdots & r_M^{(N)} \end{bmatrix}. \tag{4}$$

For Example 1, if we assume $\Pr = \{x = 0\} = q$ and $\Pr\{x = 1\} = p$, the suffix probability matrix is:

$$\mathbf{r} = \begin{bmatrix} 1 & q & q^2 & q^3 \\ 1 & q & q^2 & pq^2 \end{bmatrix}. \tag{5}$$

In case of search for a single sequence ($M = 1$) the cross-bifix matrices are reduced to scalars (bifix indicators) and the suffix probability matrix is reduced to a vector.

We describe the search process with probabilities $p_i(k)$, $1 \leq i \leq M$ and $1 \leq k$, where $p_i(k)$ is probability that, starting from the position 1, the sequence $\mathbf{s}_i$ has occurred at the position k for the first time and no sequence from the set S has been found at positions prior to k. The central result of the paper is the following theorem:

Theorem 1. *The probability $p_i(k)$ is given by the following recursive expression:*

$$p_i(k) = \begin{cases} r_i^{(N)} & k = 1 \\ \displaystyle\sum_{j=1}^{M} \sum_{n=1}^{\min(N,k-1)} \left(h_{ji}^{(N-n+1)} r_i^{(n-1)} - h_{ji}^{(N-n)} r_i^{(n)} \right) p_j(k-n) & k > 1 \end{cases} \tag{6}$$

The probability that some sequence from the set S is found after exactly k tests is given by:

$$p(k) = \sum_{i=1}^{M} p_i(k) \tag{7}$$

as the simulation of different sequences at the position k are mutually exclusive independent events. We give the proof of Eqs. 6 and 7 for $k > N$, since for $1 \leq k \leq N$, the extension is straightforward.

Proof. Suppose that a sequence $\mathbf{s}_i$ has occurred at the position k for the first time, including all sequences of the set S. The probability of this event, $p_i(k)$, is a probability of occurrence of a data stream of length $k+N-1$ that ends with the sequence $\mathbf{s}_i$, with no sequence from the set S contained at positions prior to position k. We call such data stream as k-constrained $\mathbf{s}_i$-stream and denote the set consisting of all k-constrained $\mathbf{s}_i$-stream by $C_i(k)$. All other streams of length $k+N-1$ that also end with sequence $\mathbf{s}_i$, but do not satisfy the above constraint are called k-unconstrained $\mathbf{s}_i$-streams and we denote the corresponding set by $U_i(k)$. Since sets $C_i(k)$ and $U_i(k)$ are disjoint and the first $k-1$ symbols of both sets form a complete set of data streams that are $k-1$ symbols long, the following holds:

$$\Pr\{C_i(k) \cup U_i(k)\} = \Pr\{C_i(k)\} + \Pr\{U_i(k)\} = p_i(k) + \Pr\{U_i(k)\} = r_i^{(N)}, \tag{8}$$

$$p_i(k) = r_i^{(N)} - \Pr\{U_i(k)\}. \tag{9}$$

Set $U_i(k)$ can be further decomposed into subsets $U_{ij}(k,f)$, where each subset consists of the streams that contain a sequence $\mathbf{s}_i$ at the position k and a sequence $\mathbf{s}_j$, $1 \leq j \leq M$, at the position f, with the constraint that the occurrence of the sequence $\mathbf{s}_j$ is the first occurrence of any sequence from the set S in the unconstrained stream $U_{ij}(k,f)$. The symbols between the sequence $\mathbf{s}_j$ at the position f and the sequence $\mathbf{s}_i$ at the position k are arbitrary. Number of these subsets is $M(k-1)$ and since they are disjoint, it follows:

$$U_i(k) = \bigcup_{f=1}^{k-1} \bigcup_{j=1}^{M} U_{ij}(k,f), \tag{10}$$

$$\Pr\{U_i(k)\} = \sum_{f=1}^{k-1} \sum_{j=1}^{M} \Pr\{U_{ij}(k,f)\}. \tag{11}$$

The decomposition of the unconstrained stream $U_1(k)$ for the Example 1 is shown in Fig. 2.

For $f \leq k-N$, each stream from a subset $U_{ij}(k,f)$ consists of an f-constrained $\mathbf{s}_j$-stream, arbitrary stream of length $k-f-N$ and sequence $\mathbf{s}_i$. Hence, the probability of the subset $U_{ij}(k,f)$ is:

$$\Pr\{U_{ij}(k,f)\} = \Pr\{C_j(f)\} \cdot r_i^{(N)} = p_j(f) \cdot r_i^{(N)}. \tag{12}$$

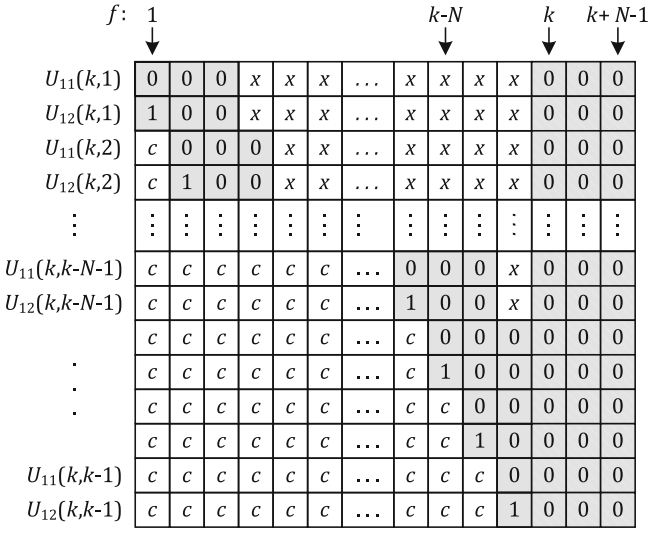


Fig. 2. Decomposition of set $U_1(k)$ into subsets $U_{1i}(k,f)$ for Example 1, $\mathbf{s}_1 = [0\ 0\ 0]$ and $\mathbf{s}_2 = [1\ 0\ 0]$, c - constrained data, x - arbitrary data

For $f > k-N$, sequences $\mathbf{s}_i$ and $\mathbf{s}_j$ overlap and Eq. 12 does not hold. The subset $U_{ij}(k,f)$ exists only if the overlapping symbols enable it, i.e. if a cross-bifix of length $N-(k-f)$ exists (Fig. 3). In this case, a $N-(k-f)$ symbols long suffix of sequence $\mathbf{s}_j$ (the same as a prefix of $\mathbf{s}_i$) is followed by $k-f$ symbols long suffix of sequence $\mathbf{s}_i$, thus forming sequence $\mathbf{s}_i$ at the end of the stream. Consequently, the probability of the subset $\Pr\{U_{ij}(k,f)\}$ is:

$$\Pr\{U_{ij}(k,f)\} = h_{ji}^{(N-(k-f))} \cdot p_j(f) \cdot r_i^{(k-f)}. \tag{13}$$

Summation of Eqs. 12 and 13 according to Eq. 11, with substitution $n = k-f$, yields:

$$\Pr\{U_i(k)\} = \begin{cases} \displaystyle\sum_{n=1}^{k-1}\sum_{j=1}^{M} h_{ji}^{(N-n)} r_i^{(n)} p_j(k-n) & k \le N+1 \\ \displaystyle\sum_{n=1}^{N-1}\sum_{j=1}^{M} h_{ji}^{(N-n)} r_i^{(n)} p_j(k-n) + \sum_{n=N}^{k-1}\sum_{j=1}^{M} p_j(k-n) & k > N+1 \end{cases} \tag{14}$$

Eq. 8 holds for any k, so it holds for $k-1$ as well:

$$r_i^{(N)} = p_i(k-1) + \Pr\{U_i(k-1)\}. \tag{15}$$

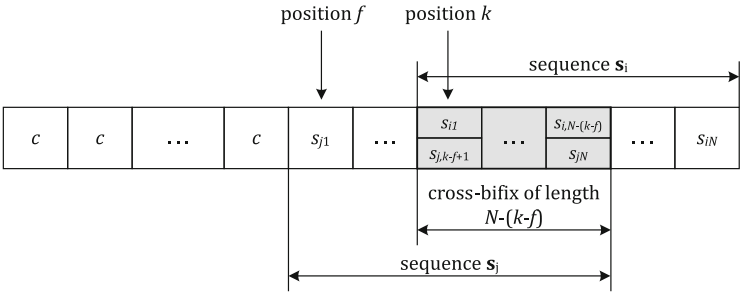


Fig. 3. Illustration of $U_{ij}(k, f)$ when $f > k - N$, c - constrained data

Inserting Eq. 15 into Eq. 9 and substituting $\Pr\{U_i(k-1)\}$ and $\Pr\{U_i(k)\}$ with Eq. 14 gives:

$$p_i(k) = \sum_{n=1}^{N-1} \sum_{j=1}^{M} \left(h_{ji}^{(N-n+1)} r_i^{(n-1)} - h_{ji}^{(N-n)} r_i^{(n)} \right) p_j(k-n) \tag{16}$$

This concludes the proof. □

The evaluation of the first moment (expected duration of the search, denoted by T) and the second moment yields:

$$\mu_1 = T = \sum_{k=1}^{\infty} k \cdot p(k) = 1 - N + \frac{\sum_{i=1}^{M} \sum_{j=1}^{M} P_i R_{ij}}{\sum_{i=1}^{M} r_i^{(N)}}, \tag{17}$$

$$\mu_2 = \sum_{k=1}^{\infty} k^2 \cdot p(k) = (N-1)^2 + \frac{\sum_{i=1}^{M} \sum_{j=1}^{M} \left(2T_i R_{ij} + P_i (W_{ij} - 2N R_{ij}) \right)}{\sum_{i=1}^{M} r_i^{(N)}}, \tag{18}$$

where:

$$P_i = \sum_{k=1}^{\infty} p_i(k), \; R_{ij} = \sum_{n=1}^{N} r_j^{(n-1)} h_{ij}^{(N-n+1)}, \tag{19}$$

$$T_i = \sum_{k=1}^{\infty} k \cdot p_i(k), \; W_{ij} = \sum_{n=1}^{N} (2n-1) r_j^{(n-1)} h_{ij}^{(N-n+1)}. \tag{20}$$

Vectors $\mathbf{P} = [P_1\ P_2 \cdots P_M]$ and $\mathbf{T} = [T_1\ T_2 \cdots T_M]$ can be evaluated as solutions of the following set of linear equations:

$$\mathbf{A} \cdot \mathbf{P}^T = 0, \quad \sum_{i=1}^{M} P_i = 1, \tag{21}$$

$$\mathbf{A} \cdot \mathbf{T}^T = \mathbf{B}, \quad \sum_{i=1}^{M} T_i = T. \tag{22}$$

where $\mathbf{A} = [A_{ij}]_{MxM}$, $\mathbf{B} = [B_1\ B_2 \cdots B_M]$ and:

$$A_{ij} = \frac{R_{ji}}{r_i^{(N)}} - \frac{R_{j,i+1}}{r_{i+1}^{(N)}}, \tag{23}$$

$$B_i = \frac{1}{2} \sum_{j=1}^{M} \left(\frac{W_{j,i+1}}{r_{i+1}^{(N)}} - \frac{W_{ji}}{r_i^{(N)}} \right) P_j. \tag{24}$$

If data values are equiprobable, $\Pr\{x = A_i\} = L^{-1}$, $1 \le j \le L$, and if the set of sequences is cross-bifix free, then Eqs. 17-24 are simplified to:

$$R_{ij} = W_{ij} = \delta_{ij},\ \mathbf{A} = \begin{bmatrix} 1 & -1 & 0 \cdots 0 & 0 \\ 1 & 0 & -1 \cdots 0 & 0 \\ \vdots & \vdots & \vdots \ldots \vdots & \vdots \\ 1 & 0 & 0 \cdots 0 & -1 \\ 1 & 1 & 1 \cdots 1 & 1 \end{bmatrix},\ \mathbf{B} = [0\ 0 \cdots 0\ T] \tag{25}$$

where δ_{ij} is the Kronecker delta. From Eq. 25 it follows: $P_i = M^{-1}$, $T_i = T \cdot M^{-1}$, $1 \le i \le M$, and

$$\mu_1 = T = 1 - N + L^N M^{-1}, \tag{26}$$

$$\mu_2 = T(2T - 1) - N(N - 1). \tag{27}$$

This is of particular importance for distributed sequences [7,10] that are by construction cross-bifix free.

For equiprobable data and just a single sequence ($M = 1$), the pmf, first and second moments of the search are reduced to the expressions given in [1,15]:

$$p(k) = \begin{cases} L^{-N} & k = 1 \\ \sum_{n=1}^{\min(N,k-1)} \left(L^{1-n} h^{(N-n+1)} - L^{-n} h^{(N-n)} \right) p(k-N) & k > 1 \end{cases}, \tag{28}$$

$$T = 1 - N + \sum_{n=1}^{N} h^{(n)} L^n, \tag{29}$$

$$\mu_2 = T(2T - 1) - N(N - 1) - 2 \sum_{n=1}^{N} n h^{(N-n)} L^{N-n}. \tag{30}$$

Finally, for bifix-free sequence Eqs. 28-29 reduce to:

$$p(k) = \begin{cases} L^{-N} & 1 \leq k \leq N \\ p(k-1) - p(k-N) & k > N \end{cases}, \tag{31}$$

$$T = 1 - N + L^N, \tag{32}$$

$$\mu_2 = T(2T-1) - N(N+1). \tag{33}$$

In the next section we apply the derived results to the practical problem of the search in framed data, which is an integral part of any algorithm for the acquisition of frame synchronization in a synchronous transmission.

3 Search in Frame

In case of synchronous transmission, data is usually transmitted in equal-length frames where every frame starts with a predefined frame-synchronization sequence. We assume that the frame and synchronization sequence length are F and N symbols, respectively; we denote the synchronization sequence with $\mathbf{s}_1$ and its position in the frame as position 0. After establishing carrier and symbol synchronization, receiver has to acquire frame synchronization in order to correctly receive incoming data. In order to do so, receiver searches for $\mathbf{s}_1$, sliding through the incoming stream; we assume that the search starts at some random offset position O with respect to the start of frame (Fig. 4). Furthermore, we consider the general case when up to E errors are allowed when detecting a synchronization sequence, hence the search is performed for all sequences that are up to Hamming distance E from the sequence $\mathbf{s}_1$. In other words, there are $M = \sum_{e=0}^{E} \binom{N}{e}$ sequences in the set S.

In case of search in framed data stream there are three distinct search regions (Fig. 4): the first and the second overlap regions, where the sliding window partially overlaps received synchronization sequence; and data region, where data within the window is purely random. The results from Section 2 are readily

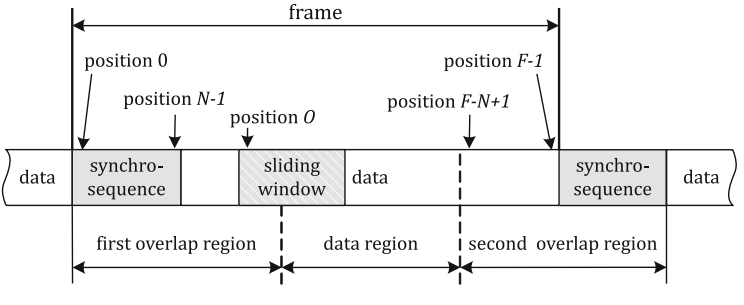


Fig. 4. Search in frame

applicable only to the search in the data region, while the search in the overlap regions is impacted by the presence of synchronization symbols in the sliding window. The following lemma describes the search within the first overlap region.

Lemma 1. *The sequence* $\mathbf{s}_i$, $1 \leq i \leq M$, *will occur for the first time within the first overlap region at position* k, $1 \leq k \leq N - O + 1$, *starting from position* O, $1 \leq O < N$, *and no sequence from* S *will occur prior to position* k, *if the following three conditions are satisfied:*

1. $h_{1i}^{(N-O-k+1)} = 1$,
2. *The first* $O + k - 1$ *data symbols immediately following synchronization sequence in frame are equal to the suffix of the sequence* $\mathbf{s}_i$*; probability of this event is* $r_i^{(O+k-1)}$,
3. $h_{1z}^{(N-O-d+1)} h_{zi}^{(N-k+d)} \neq 1$, *for* $1 \leq z \leq M$ *and* $1 \leq d < k$,

where k *is given with respect to* O.

Proof. The first two conditions are straightforward - at the position k the last $N - O - k + 1$ symbols (suffix) of the sequence $\mathbf{s}_1$ are compared to the prefix of the sequence $\mathbf{s}_i$; sequence $\mathbf{s}_i$ can not occur unless $h_{1i}^{(N-O-k+1)} = 1$ and unless the following $O + k - 1$ data symbols are equal to the suffix of $\mathbf{s}_i$. However, these two conditions are not sufficient, as there may exist a sequence $\mathbf{s}_z$ from the set S with the following properties:

a) its prefix of length $N - O - d + 1$, $1 \leq d < k$, is equal to the suffix of the sequence $\mathbf{s}_1$ (i.e., $h_{1z}^{(N-O-d+1)} = 1$),
b) its suffix of length $N - k + d$ is equal to the prefix of sequence $\mathbf{s}_i$ (i.e., $h_{zi}^{(N-k+d)} = 1$).

The property b) implies that suffix symbols of $\mathbf{s}_z$ that overlap data are equal to these data symbols (striped symbols in Fig. 5), since they are equal to that part of sequence $\mathbf{s}_i$ that also overlaps the same data symbols and by the second condition of Lemma 1 are equal to them. Moreover, both properties imply that the sequence $\mathbf{s}_z$ has already occurred at the position d. From this it follows that the occurrence of sequence $\mathbf{s}_i$ could not happen, since the data symbols immediately following the synchronization sequence had been already exhausted for simulation of the sequence $\mathbf{s}_z$ and the search has stopped before reaching the position k. Finally, from this it follows that the sequence $\mathbf{s}_i$ can appear only if no sequence from S with properties a) and b) can occur at any position d prior the position k, which is summarized in the third condition of Lemma 1. This condition could be rewritten as:

$$\prod_{z=1}^{M} \prod_{d=1}^{k-1} \left(1 - h_{1z}^{(N-O-d+1)} h_{zi}^{(N-k+d)}\right) \neq 0 \tag{34}$$

for $1 \leq O < N$ and $1 \leq k \leq N - O + 1$. □

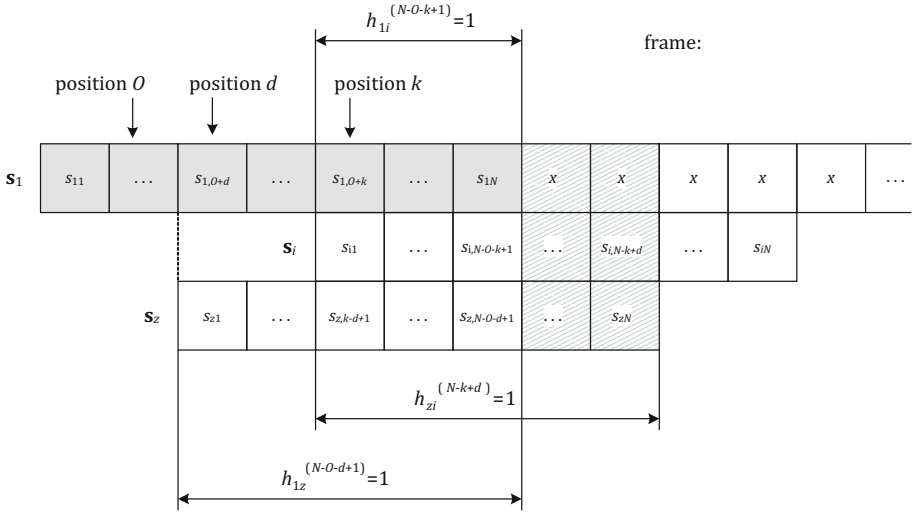


Fig. 5. Search in the first overlap region

Example 2 in Fig. 6 clarifies the above condition; the synchronization sequence is $\mathbf{s}_1 = [1\ 1\ 0\ 1\ 0]$ and $E = 1$ symbol errors are accepted when detecting a synchronization sequence. In total, six sequences are considered as correct at the receiver (Fig 6a). We assume that search has started at position $O = 2$. If data bits are $x_1 = 1$ and $x_2 = 0$, the sequence $\mathbf{s}_2$ is found at position $k = 1$, as its prefix of length $N - O - k + 1 = 3$ is equal to the suffix of the sequence $\mathbf{s}_1$ ($h_{12}^{(3)} = 1$, Fig. 6b); if data bits are $x_1 = 0$, $x_2 = 1$ and $x_3 = 0$, the sequence $\mathbf{s}_3$ is simulated at $k = 2$, as its prefix of length $N - O - k + 1 = 2$ is equal to the suffix of the $\mathbf{s}_1$ ($h_{13}^{(2)} = 1$, Fig. 6c). In both cases, other sequences that satisfy first two conditions, but not the third condition of Lemma 1 can not be found, since the search has stopped prior to their potential occurrence.

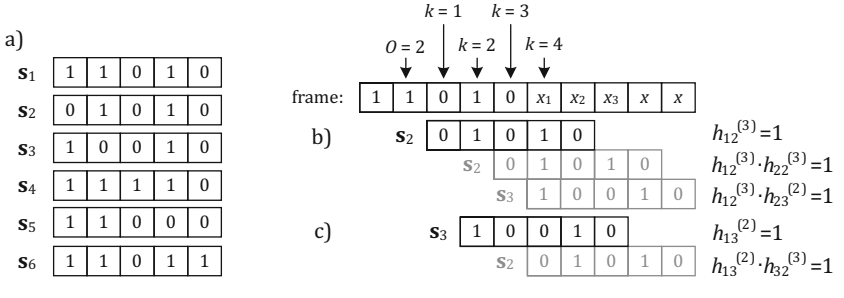


Fig. 6. a) Sequences from the set S for Example 2 b) $x_1 = 1$ and $x_2 = 0$, $\mathbf{s}_2$ found at position 1, preventing occurrence of $\mathbf{s}_2$ at position 3 and $\mathbf{s}_3$ at position 4, c) $x_1 = 0$, $x_2 = 1$ and $x_3 = 0$, $\mathbf{s}_3$ found at position 2, preventing occurrence of $\mathbf{s}_2$ at position 3

Combining the conditions of Lemma 1, Eqs. 34 and 6, a conditional pmf that sequence $\mathbf{s}_i$ is found at position k, if the search has started from the offset position O, for $1 \leq O < N$ is equal to:

$$p_i(k/O) = \begin{cases} h_{1i}^{(N-O-k+1)} r_i^{(O+k-1)} \prod_{z=1}^{M} \prod_{d=1}^{k-1} \left(1 - h_{1z}^{(N-O-d+1)} h_{zi}^{(N-k+d)}\right) \\ \qquad \text{for } 1 \leq k \leq N-O+1 \\ \sum_{j=1}^{M} \sum_{n=1}^{\min(N,k-1)} \left(h_{ji}^{(N-n+1)} r_i^{(n-1)} - h_{ji}^{(N-n)} r_i^{(n)}\right) p_j(k-n/O) \\ \qquad \text{for } N-O+2 \leq k \leq F-O+1 \end{cases} \tag{35}$$

and for $N \leq O \leq F$, is equal to:

$$p_i(k/O) = \begin{cases} r_i^{(N)} \text{ for } k = 1 \\ \sum_{j=1}^{M} \sum_{n=1}^{\min(N,k-1)} \left(h_{ji}^{(N-n+1)} r_i^{(n-1)} - h_{ji}^{(N-n)} r_i^{(n)}\right) p_j(k-n/O) \\ \qquad \text{for } 1 < k \leq F-O+1 \end{cases} \tag{36}$$

Within the second overlap region, suffix of window contents overlaps with synchronization sequence and hence cross-bifix indicator should substitute suffix probability. Finally, the conditional probability $p(k/O)$ that some sequence from the set S will be found is equal to:

$$p(k/O) = \begin{cases} \sum_{i=1}^{M} p_i(k/O) & 1 \leq k \leq F-N-O+1 \\ \sum_{i=1}^{M} h_{i1}^{(N+O-F-1+k)} \frac{p_i(k/O)}{r_i^{(N+O-F-1+k)}} & F-N-O+1 < k \leq F-O+1 \end{cases} \tag{37}$$

To illustrate the derived formulas, we calculate the probability that the search would "survive", i.e., the probability that no sequence from the set S would be found prior the correct position F:

$$P_{SV}(O) = p(F-O+1/O). \tag{38}$$

The worst case occurs if the search starts immediately after the correct position, i.e. $O = 1$ and $P_{SV}(1) = p(F/1)$. Table 1 gives $P_{SV}(1)$ for several binary sequences with 7 bits, when a single error is allowed ($E = 1$) and frame length is $F = 50$ bits. As shown in table, sequences 0000000 and 0000001 can not survive the search. This is due to the allowed error when detecting a sequence, implying that sequences from corresponding sets S certainly occur during search. Barker, Jones and PDH sequences are all bifix-free, however, when $E = 1$, corresponding sets S have different cross-bifix matrices, causing different survival probabilities. Distributed Barker-like sequence, which is a cros-bifix free sequence, performs better than contiguous bifix-free ones, due to its larger length and hence larger overlap regions. Finally, periodical sequence 0101010, although having plenty of bifices, induces less cross-bifices in the corresponding set S when $E = 1$ and has the greatest survival probability for the given frame length.

Table 1. Survival probabilities $P_{SV}(1)$ of binary sequences with 7 synchronization bits when one bit error is allowed, for equiprobable data and frame length of 50 bits

Sequence	$P_{SV}(1)$
Barker sequence 0001101	0.026844
Jones sequence 0001011 [5]	0.036263
PDH sequence 0010011 [16]	0.036156
0000000	0
0000001	0
0101010	0.051202
Distributed Barker-like sequence 000xx1xxx1x01 [7]	0.032508

4 Conclusion

In this paper we presented a statistical description of the search for set of sequences, both in the case of random and framed data. The obtained results can be applied to analysis and evaluation of the properties of frame-synchronization sequences, and establish the optimal sequence structure and length with respect to the frame length. The straightforward application of the derived formulas would be an exact expression of frame-synchronization acquisition time that would incorporate framing algorithm, errors and sequence structure. This acquisition time could serve as a guideline for joint optimization of frame and sequence length and structures, and amount of allowed sequence distortion. Finally, another interesting application of the given analysis could be in the field of biological sequences in terms of frame synchronization of gene expressions, as proposed in [17,18].

References

1. Nielsen, P.T.: On the Expected Duration of a Search for a Fixed Pattern in Random Data. IEEE Trans. Inform. Theory 19, 702–704 (1973)
2. Scholtz, R.: Frame Synchronization Techniques. IEEE Trans. Comm. 28, 1204–1213 (1980)
3. Georghiades, C.N., Snyder, D.L.: Locating Data Frames in Direct-Detection Optical Communication Systems. IEEE Trans. Comm. 32, 118–123 (1984)
4. Lui, G.L., Tan, H.H.: Frame Synchronization for Direct-Detection Optical Communications. IEEE Trans. Comm. 34, 227–237 (1986)
5. Al-Subbagh, M.N., Jones, E.V.: Optimum patterns for frame alignment. IEE Proc. part F - Commun., Radar & Signal Processing 135(6), 594–603 (1988)
6. Patarasen, S., Gheorghiades, C.N.: Frame Synchronization for Optical Overlapping Pulse-Position Modulation Systems. IEEE Trans. Comm. 40, 783–794 (1992)
7. de Lind van Wijngaarden, A.J., Willink, T.J.: Frame Synchronization Using Distributed Sequences. IEEE Trans. Comm. 48(12), 2127–2138 (2000)
8. Newton, N.J.: Data Synchronization and Noisy Environments. IEEE Trans. Inform. Theory 48(8), 2253–2262 (2002)

9. Chiani, M., Martini, M.G.: On Sequential Frame Synchronization in AWGN Channels. IEEE Trans. Comm. 54(2), 339–348 (2006)
10. Villanti, M., Iubatti, M., Corazza, A.V.C.G.E.: Design of Distributed Unique Words for Enhanced Frame Synchronization. IEEE Trans. Comm. 57(8), 2430–2440 (2009)
11. Bajic, D.: On statistical aspects of search for set of predefined sequences (2010), http://www.ktios.net/images/stories/clanovi_katedre/dragana_bajic/On_statistical_aspects_of_search_for_set_of_predefined_sequences.pdf
12. Bajic, D., Stefanovic, C., Vukobratovic, D.: Search Process and Probabilistic Bifix Approach. In: Proc. of IEEE ISIT 2005. Adelaide, Australia (September 2005)
13. Stefanovic, C.: Synchronization sequences and bifix analysis (in Serbian). Master's thesis, Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia (2006)
14. Bajic, D., Drajic, D.: Duration of a search for a fixed pattern in random data: Distribution function and variance. Electron. Lett. 31(8), 631–632 (1995)
15. Bajic, D., Stojanovic, J.: Distributed Sequences and Search Process. In: Proc. of IEEE ICC 2004, Paris, France (June 2004)
16. CCITT Recommendation, C.: Blue Book III.4. Geneve, Switzerland (1988)
17. Weindl, J., Hagenauer, J.: Applying Techniques from Frame Synchronization for Biological Sequence Analysis. In: Proc. of IEEE ICC 2007, Glasgow, Scotland (June 2007)
18. Weindl, J.: Frame Synchronization Processes in Gene Expression. Ph.D. thesis, Technischen Universität München, Munich, Germany (2008)

On the Nonlinearity of Discrete Logarithm in $\mathbb{F}_{2^n}$

Risto M. Hakala[1] and Kaisa Nyberg[1,2]

[1] Department of Information and Computer Science,
Aalto University School of Science and Technology,
P.O. Box 15400, FI-00076 Aalto, Finland
{risto.m.hakala,kaisa.nyberg}@tkk.fi
[2] Nokia Research Center, Finland
kaisa.nyberg@nokia.com

Abstract. In this paper, we derive a lower bound to the nonlinearity of the discrete logarithm function in $\mathbb{F}_{2^n}$ extended to a bijection in $\mathbb{F}_2^n$. This function is closely related to a family of S-boxes from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ proposed recently by Feng, Liao, and Yang, for which a lower bound on the nonlinearity was given by Carlet and Feng. This bound decreases exponentially with m and is therefore meaningful and proves good nonlinearity only for S-boxes with output dimension m logarithmic to n. By extending the methods of Brandstätter, Lange, and Winterhof we derive a bound that is of the same magnitude. We computed the true nonlinearities of the discrete logarithm function up to dimension $n = 11$ to see that, in reality, the reduction seems to be essentially smaller. We suggest that the closing of this gap is an important problem and discuss prospects for its solution.

Keywords: Symmetric cryptography, Boolean functions, S-boxes, nonlinearity, discrete logarithm.

1 Introduction

The discrete logarithm function has a long history in public key cryptography. It has previously been investigated also from the point of view of symmetric key cryptography. For example, a bound for the linear complexity of sequences generated by the discrete logarithm function was determined in [6] and the differential uniformity was shown to be good in [8]. Recently Brandstätter, Lange, and Winterhof showed that the least significant bit of the discrete logarithm function in $\mathbb{F}_{2^n}$ is highly nonlinear [1]. Later Carlet and Feng [2] considered a closely related function and proved a lower bound to its nonlinearity, which is about the same as the one obtained in [1]. They also showed that this function has very good algebraic immunity. The Boolean function of Carlet and Feng is a special case of the class of vectorial Boolean functions, that is, S-boxes constructed by Feng, Liao, and Yang [5]. Carlet and Feng [3] derived a lower bound to the nonlinearity of such S-boxes. This lower bound is meaningful only for S-boxes with small

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 333–345, 2010.

output dimension in this class. Very little is known about the nonlinearity of S-boxes in this class with about equal input and output dimensions, which is most commonly the case in practical symmetric key cryptography.

The definition of S-boxes within the infinite class of vectorial Boolean functions given in [5] can also be given in terms of the discrete logarithm function. Actually, as will be shown in this paper, these functions are equivalent to truncations of the discrete logarithm function up to a linear transform of the input space and change of values at two points. The goal of this paper is to investigate the problem of nonlinearity of the discrete logarithm function. We extend the tools of [1] to handle integer valued discrete logarithm and develop a characterization of a linear approximation of the discrete logarithm. We use this characterization to derive an upper bound to the Walsh transform of the linear combinations of the coordinates of the discrete logarithm. For fixed dimension, this upper bound depends only on the length of the masking vector determining the linear combination. While the derived bounds are not essentially better than those given in [3] the method gives some new insight to this problem. Supported by the nonlinearity values we computed for small dimensions we conjecture that the absolute values of the Walsh transform for the discrete logarithm in dimension n are bounded from above by $c(n)2^{n/2}$, where $c(n)$ is a polynomial of low degree.

The outline of the paper is as follows: In Section 2, we give some basic definitions that are used throughout the paper. In Section 3, we describe the discrete logarithm function and some of its basic properties. In Section 4, we discuss the S-box of Feng, Liao, and Yang, and compare it to the discrete logarithm. We derive our lower bound for the nonlinearity of discrete logarithm in Section 5. In Section 6, we estimate the accuracy of our bound and discuss how it could be improved. We conclude the paper in Section 7.

2 Preliminaries

Let n be a positive integer and denote by $\mathbb{F}_q$ the finite field of order $q = 2^n$. We associate every element of $\mathbb{F}_q$ to a unique vector of $\mathbb{F}_2^n$ using a fixed basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. We also identify the vectors in $\mathbb{F}_2^n$ and the elements in $\mathbb{Z}_q$ using the natural correspondence $(u_{n-1}, \ldots, u_1, u_0) \in \mathbb{F}_2^n \leftrightarrow u_{n-1}2^{n-1} + \cdots + u_1 2^1 + u_0 2^0 \in \mathbb{Z}_q$. Given two vectors $u = (u_{n-1}, \ldots, u_1, u_0) \in \mathbb{F}_2^n$ and $v = (v_{n-1}, \ldots, v_1, v_0) \in \mathbb{F}_2^n$ we denote $u \cdot v = u_{n-1}v_{n-1} + \cdots + u_1 v_1 + u_0 v_0 \in \mathbb{F}_2$. The Hamming weight of a vector $v \in \mathbb{F}_2^n$ is denoted by $w_{\mathrm{H}}(v)$. A mapping $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is called a Boolean function. An $n \times m$ S-box is a vector-valued Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$. Given an S-box $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, we use $f_0, f_1, \ldots, f_{m-1}$ to denote its coordinate functions such that $f = (f_{m-1}, \ldots, f_1, f_0)$.

Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The Walsh transform of f at $u \in \mathbb{F}_2^n$ is defined as

$$\widehat{f}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u\cdot x}.$$

The nonlinearity of a Boolean function f is defined as

$$\mathcal{N}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} |\widehat{f}(u)|. \tag{1}$$

The nonlinearity of an S-box $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is then defined as

$$\mathcal{N}(f) = \min_{\substack{v \in \mathbb{F}_2^m \\ v \neq 0}} \mathcal{N}(v \cdot f) = 2^{n-1} - \frac{1}{2} \max_{\substack{v \in \mathbb{F}_2^m \\ v \neq 0}} \max_{u \in \mathbb{F}_2^n} |\widehat{v \cdot f}(u)|,$$

where $v \cdot f$ denotes the Boolean function $x \mapsto v \cdot f(x)$. In this context, the vector v is called the linear mask of f.

A character χ of an Abelian group H (written multiplicatively) is a homomorphism from H into the multiplicative group of complex numbers of absolute value 1. A trivial character χ_0 is defined as $\chi_0(h) = 1$ for all $h \in H$. For every character χ of H, there is a conjugate character $\overline{\chi}$ defined by $\overline{\chi}(h) = \overline{\chi(h)}$ for all $h \in H$, where the bar denotes complex conjugation. It is not hard to show that $\overline{\chi}(h) = \chi^{-1}(h) = \chi(h^{-1})$ for all $h \in H$. Characters of the additive group of $\mathbb{F}_q$ are called additive characters of $\mathbb{F}_q$. Similarly, characters of the multiplicative group $\mathbb{F}_q^*$ are called multiplicative characters of $\mathbb{F}_q$. For an overview of characters and related results, we refer to [7].

3 The Discrete Logarithm Function

Let α be a primitive element of $\mathbb{F}_q$. The discrete logarithm $\log_\alpha x$ of $x \in \mathbb{F}_q^*$ to the base α is the integer l such that $0 \leq l \leq q-2$ and $x = \alpha^l$. In this paper, we study properties of the function $f\colon \mathbb{F}_q \to \mathbb{Z}_q$ defined as

$$f(x) = \begin{cases} \log_\alpha x & \text{for } x \neq 0, \\ q-1 & \text{for } x = 0. \end{cases} \tag{2}$$

Let $\phi^i\colon \mathbb{F}_q \to \mathbb{F}_q$ denote the ith iterate of Frobenius automorphism defined by $\phi^i(x) = x^{2^i}$. It is not hard to see that $\phi^a \circ \phi^b = \phi^{a+b}$, where $a+b$ is taken modulo n.

Theorem 1. *The coordinate functions $f_0, \ldots, f_{n-1}$ of f are given by*

$$f_i(x) = f_0(\phi^{-i}(x))$$

for all $0 \leq i \leq n-1$.

Proof. For all $0 \leq i \leq n-1$, we have

$$f_i(x) = \begin{cases} \mathrm{lsb}(2^{-i} \log_\alpha(x) \bmod (q-1)) = \mathrm{lsb}(\log_\alpha \phi^{-i}(x)) & \text{for } x \neq 0, \\ 1 & \text{for } x = 0, \end{cases}$$

where lsb denotes the least significant bit of an integer. Since both cases are equal to $f_0(\phi^{-i}(x))$, the result follows. □

Theorem 2. *Let $v \in \mathbb{F}_2^n$ be a vector and denote by $v \lll a$ the cyclic shift of v to left by a coordinates. We have*

$$\mathcal{N}(v \cdot f) = \mathcal{N}((v \lll a) \cdot f)$$

for all $a \in \mathbb{Z}$.

Proof. It follows from Theorem 1 that

$$(v \lll a) \cdot f(x) = v \cdot f(\phi^{-a}(x))$$

for all $a \in \mathbb{Z}$. The mapping $x \mapsto \phi^{-a}(x)$ is a linear bijection for all $a \in \mathbb{Z}$. Applying a linear bijection to the input of a function does not change its nonlinearity, so the result follows. □

4 The Feng–Liao–Yang S-Boxes

Recently Feng, Liao, and Yang [5] presented a family of balanced S-boxes with optimal algebraic immunity. Carlet and Feng [3] showed that these functions have optimal algebraic degree and determined a lower bound for their nonlinearity. We give the definition of their family here for completeness. Let n be the dimension of the input and m, $m \leq n$, be the dimension of the output. Given a primitive element $\alpha \in \mathbb{F}_{2^n}$ and an integer s, $0 \leq s \leq 2^n - 2$, they divide the input space $\mathbb{F}_{2^n}$ into a union of 2^m disjoint subsets as follows

$$S_b = \begin{cases} \{\alpha^l \mid s \leq l \leq s + 2^{n-m} - 2\} \cup \{0\} & \text{for } b = 0, \\ \{\alpha^l \mid s + 2^{n-m}b - 1 \leq l \leq s + 2^{n-m}(b+1) - 2\} & \text{for } 1 \leq b \leq 2^m - 1. \end{cases}$$

We use g to denote the $n \times m$ S-boxes of Feng, Liao, and Yang defined by $g(x) = b$ for all $x \in S_b$.

It is straightforward to verify that, for $s = 1$ and for $1 \leq m \leq n$, the following holds

$$g(x) = \begin{cases} \lfloor \log_\alpha(x)/2^{n-m} \rfloor & \text{for } x \neq 0, 1, \\ 0 & \text{for } x = 0, \\ 2^m - 1 & \text{for } x = 1. \end{cases}$$

In other words, the $n \times m$ S-boxes of Feng, Liao, and Yang are identical to the discrete logarithm to the base α truncated to the most significant m bits for all inputs in $\mathbb{F}_{2^n} \setminus \{0, 1\}$. In particular, the Boolean function introduced in [2] can be obtained from the previously known highly nonlinear function given in [1] using the Frobenius automorphism ϕ and multiplication by α on the input space and interchanging the values at 0 and 1.

The lower bound for the nonlinearity of the Feng–Liao–Yang S-box derived in [3] decreases rapidly as the output dimension m increases and is negative for $m \geq n/2$. According to our computations shown in Table 1 this should not be the case as there seems to be only a slight decrease in the nonlinearity of the

discrete logarithm function compared to the nonlinearity of one of its output coordinate functions. Therefore the nonlinearity of practical S-boxes with about equal input and output size remains an open problem.

The purpose of this paper is to investigate the nonlinearity of the discrete logarithm function. Using the methods from [1] and generalizing them we determine a lower bound to the nonlinearity of any linear combination of the coordinate functions of the discrete logarithm function. While the obtained lower bound of nonlinearity is not essentially better than the one derived by Carlet and Feng in [3] we try to identify steps in the estimation chain that could potentially be improved.

5 Lower Bound for the Nonlinearity

To find a lower bound for the nonlinearity of function f, we examine the quantity $\max_{u\in\mathbb{F}_2^n}|\widehat{v\cdot f}(u)|$ using character sums. We formulate $(-1)^{v\cdot f(x)}$ for each $v\in\mathbb{F}_2^n$ as a character sum such that $\widehat{v\cdot f}(u)$ can be written as a sum of additive and multiplicative characters. Using known bounds on the absolute values of these sums, we obtain an upper bound for $\max_{u\in\mathbb{F}_2^n}|\widehat{v\cdot f}(u)|$ and thus a lower bound for the nonlinearity. Our bound heavily relies on the absolute value of a certain incomplete character sum, which seems to be quite hard to estimate. In the course of our analysis we develop a decomposition of this sum and derive estimates for it.

Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$ and denote $\eta=\overline{\chi}(\alpha)$. Given a vector $v\in\mathbb{F}_2^n$, let

$$W=W(v)=\{w\in\mathbb{Z}_{q-1}\mid v\cdot w=0,\, w\in\mathbb{F}_2^n\}. \tag{3}$$

Hence, the cardinality $\#W$ of W is $q/2$ if $w_{\mathrm{H}}(v)$ is odd and $q/2-1$ if $w_{\mathrm{H}}(v)$ is even. Next we generalize the formula for $(-1)^{\mathrm{lsb}(\log_\alpha x)}$ given in the proof of Lemma 1 in [1] for an arbitrary linear combination of the coordinate functions of the discrete logarithm.

Lemma 1. *For every $x\in\mathbb{F}_q^*$, we have*

$$(-1)^{v\cdot\log_\alpha x}=\frac{2}{q-1}\left(\sum_{j=1}^{q-2}\sum_{w\in W}\eta^{jw}\chi^j(x)-\frac{(-1)^{w_{\mathrm{H}}(v)}}{2}\right).$$

Proof. It is well-known (see e.g. [7]) that

$$\frac{1}{q-1}\sum_{j=0}^{q-2}\chi^j(x)=\begin{cases}1 & \text{if } x=1,\\ 0 & \text{otherwise,}\end{cases}$$

for all $x\in\mathbb{F}_q^*$. Substituting x by $x\alpha^{-a}$ implies

$$\frac{1}{q-1}\sum_{j=0}^{q-2}\chi^j(x\alpha^{-a})=\frac{1}{q-1}\sum_{j=0}^{q-2}\eta^{ja}\chi^j(x)=\begin{cases}1 & \text{if } \log_\alpha x=a,\\ 0 & \text{otherwise,}\end{cases}$$

for all $0 \le a \le q-2$. Given a set $A \subseteq \{0, 1, \ldots, q-2\}$, it follows that

$$\sum_{a \in A} \frac{1}{q-1} \sum_{j=0}^{q-2} \eta^{ja} \chi^j(x) = \begin{cases} 1 & \text{if } \log_\alpha x \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Since $v \cdot \log_\alpha x = 0$ if and only if $\log_\alpha x \in W$, we get

$$\begin{aligned} (-1)^{v \cdot \log_\alpha x} &= 2 \sum_{w \in W} \frac{1}{q-1} \sum_{j=0}^{q-2} \eta^{jw} \chi^j(x) - 1 \\ &= \frac{2}{q-1} \left(\sum_{j=1}^{q-2} \sum_{w \in W} \eta^{jw} \chi^j(x) + \#W \right) - 1, \\ &= \frac{2}{q-1} \left(\sum_{j=1}^{q-2} \sum_{w \in W} \eta^{jw} \chi^j(x) - \frac{(-1)^{w_{\mathrm{H}}(v)}}{2} \right) \end{aligned}$$

for all $x \in \mathbb{F}_q^*$. □

The goal is to extend the approach of [1] to an arbitrary linear mask v. To this end we need to find a good upper bound to the sum

$$R(v, q) = \sum_{j=1}^{q-2} \left| \sum_{w \in W} \eta^{jw} \right|.$$

To our knowledge, no results exist that could be applied directly. In Lemma 3, we present a result by Cochrane [4] that was used in [1] to derive a good upper bound to such a sum, where the inner sum is taken over the set of even integers, that is, the set $W = W(v)$ for $v = (0, \ldots, 0, 1)$. This result is given below as Corollary 2, where we denote Cochrane's upper bound by $C(q)$.

To examine the inner sum in $R(v, q)$ for an arbitrary linear mask v we will use the following strategy. First, we will extend the sum by adding one term to it, which will be done only in case $w_{\mathrm{H}}(v)$ is even, and develop a decomposition of the extended sum. The result will be given in Theorem 3. Using this decomposition we will then establish an upper bound to $R(v, q)$ in terms of $C(q)$ in Theorem 4. Given a vector $v \in \mathbb{F}_2^n$, we denote

$$\overline{W} = \overline{W}(v) = \begin{cases} W(v) & \text{if } w_{\mathrm{H}}(v) \text{ is odd,} \\ W(v) \cup \{q-1\} & \text{if } w_{\mathrm{H}}(v) \text{ is even.} \end{cases}$$

Definition 1. *Let $v = (v_{n-1}, \ldots, v_1, v_0) \in \mathbb{F}_2^n$ and suppose that $\overline{W} = \overline{W}(v)$ is defined as above. We call the polynomial*

$$G(v)(x) = \sum_{w \in \overline{W}} x^w \in \mathbb{Z}[x] / \langle x^{q-1} - 1 \rangle$$

the mask polynomial for v.

We use $G_k(v)(x)$ to denote the mask polynomial $G((0,\ldots,0,v_{k-1},\ldots,v_0))(x)$ for $1 \le k \le n$. We explicitly define $G_0(v)(x) = 1$. Then $G_1(v)(x) = G_0(v)(x)$ if $v_0 = 0$. Also it is known from [1] that $G_1(v)(x) = x^0 + x^2 + \cdots + x^{q-2}$ if $v_0 = 1$. The following lemma gives a recursive representation for $G_{k+1}(v)(x)$, where $k \ge 0$, which will be used in Theorem 3 to obtain the formulation for $G_{k+1}(v)(x)$.

Lemma 2. *For all* $0 \le k < n$,

$$G_{k+1}(v)(x) = v_k \frac{x^{2^k}}{1+x^{2^k}} + \frac{1+(-1)^{v_k}x^{2^k}}{1+x^{2^k}} G_k(v)(x).$$

Proof. For any $k \ge 0$, let

$$A_k = \{w \in \overline{W} \mid v \cdot w = 0,\ w = (0,\ldots,0,w_{k-1},\ldots,w_0) \in \mathbb{F}_2^n\}$$

and denote $B_k = \{0,1,\ldots,2^k-1\} \setminus A_k$. Let $P_k(x)$ and $Q_k(x)$ be polynomials in $\mathbb{Z}[x]/\langle x^{q-1}-1\rangle$ defined by

$$P_k(x) = \sum_{a \in A_k} x^a \quad \text{and} \quad Q_k(x) = \sum_{b \in B_k} x^b.$$

Then,

$$P_k(x) + Q_k(x) = \sum_{i=0}^{2^k-1} x^i = \frac{1-x^{2^k}}{1-x}. \tag{4}$$

Since the $n-k$ most significant bits of v are zeroes, then for any $w \in A_k$ it holds that $w + i2^k \in \overline{W}$ for $i = 0,1,\ldots,2^{n-k}-1$. Hence we obtain

$$G_k(v)(x) = P_k(x) \sum_{i=0}^{2^{n-k}-1} x^{i2^k} = P_k(x)\frac{1-x}{1-x^{2^k}}. \tag{5}$$

From (4) and (5), we get

$$Q_k(x) = \frac{x^{2^k}-1}{x-1} - G_k(v)(x)\frac{x^{2^k}-1}{x-1} = (1-G_k(v)(x))\frac{1-x^{2^k}}{1-x}. \tag{6}$$

Next we formulate $G_{k+1}(v)(x)$ using $G_k(v)(x)$. There are two cases to consider: If $v_k = 0$, the polynomial $G_{k+1}(v)(x)$ is the same as $G_k(v)(x)$. If $v_k = 1$, we have $A_{k+1} = A_k \cup \{2^k + b \mid b \in B_k\}$, so $P_{k+1}(x) = P_k(x) + x^{2^k}Q_k(x)$. Using (5) and (6) we then deduce that

$$\begin{aligned}
G_{k+1}(v)(x) &= (P_k(x) + x^{2^k}Q_k(x))\frac{1-x}{1-x^{2^{k+1}}} \\
&= \left[G_k(v)(x)\frac{1-x^{2^k}}{1-x} + (1-G_k(v)(x))\frac{x^{2^k}(1-x^{2^k})}{1-x}\right]\frac{1-x}{1-x^{2^{k+1}}} \\
&= (G_k(v)(x) + x^{2^k} - G_k(v)(x)x^{2^k})\frac{1}{1+x^{2^k}} \\
&= \frac{x^{2^k}}{1+x^{2^k}} + \frac{1-x^{2^k}}{1+x^{2^k}}G_k(v)(x).
\end{aligned}$$

Combining both cases $v_k = 0, 1$ into a single equation we get the desired representation for $G_{k+1}(v)(x)$. □

Theorem 3. *For all* $0 \le k < n$,

$$\begin{aligned} G_{k+1}(v)(x) = v_k \frac{x^{2^k}}{1+x^{2^k}} + \frac{1-x}{1-x^{2^{k+1}}} \prod_{i=0}^{k} (1+(-1)^{v_i} x^{2^i}) \\ + \sum_{s=0}^{k-1} v_s \frac{x^{2^s}(1-x^{2^s})}{1-x^{2^{k+1}}} \prod_{i=s+1}^{k} (1+(-1)^{v_i} x^{2^i}), \end{aligned} \tag{7}$$

where the sum is zero if $k = 0$.

Proof. For $k = 0$ and $v_0 = 1$, the formula gives

$$G_1(v)(x) = \frac{x}{1+x} + \frac{1-x}{1+x} = \frac{1}{1+x} = x^0 + x^2 + \cdots + x^{q-2},$$

which holds true as noted above. If $v_0 = 0$, the formula gives $G_1(v)(x) = G_0(v)(x) = 1$, which is also true. Assume now that the statement holds for $k = l - 1 \ge 0$. We prove it for $k = l$. By Lemma 2 we get

$$\begin{aligned} G_{l+1}(v)(x) &= v_l \frac{x^{2^l}}{1+x^{2^l}} + \frac{1+(-1)^{v_l} x^{2^l}}{1+x^{2^l}} \left[\frac{1-x}{1-x^{2^l}} \prod_{i=0}^{l-1} (1+(-1)^{v_i} x^{2^i}) \right. \\ &\quad \left. + \sum_{s=0}^{l-2} v_s \frac{x^{2^s}(1-x^{2^s})}{1-x^{2^l}} \prod_{i=s+1}^{l-1} (1+(-1)^{v_i} x^{2^i}) + v_{l-1} \frac{x^{2^{l-1}}}{1+x^{2^{l-1}}} \right] \\ &= v_l \frac{x^{2^l}}{1+x^{2^l}} + \frac{(1-x)(1+(-1)^{v_l} x^{2^l})}{(1+x^{2^l})(1-x^{2^l})} \prod_{i=0}^{l-1} (1+(-1)^{v_i} x^{2^i}) \\ &\quad + \sum_{s=0}^{l-2} v_s \frac{x^{2^s}(1-x^{2^s})(1+(-1)^{v_l} x^{2^l})}{(1+x^{2^l})(1-x^{2^l})} \prod_{i=s+1}^{l-1} (1+(-1)^{v_i} x^{2^i}) \\ &\quad + v_{l-1} \frac{x^{2^{l-1}}(1-x^{2^{l-1}})(1+(-1)^{v_l} x^{2^l})}{(1+x^{2^l})(1+x^{2^{l-1}})(1-x^{2^{l-1}})} \\ &= v_l \frac{x^{2^l}}{1+x^{2^l}} + \frac{1-x}{1-x^{2^{l+1}}} \prod_{i=0}^{l} (1+(-1)^{v_i} x^{2^i}) \\ &\quad + \sum_{s=0}^{l-1} v_s \frac{x^{2^s}(1-x^{2^s})}{1-x^{2^{l+1}}} \prod_{i=s+1}^{l} (1+(-1)^{v_i} x^{2^i}). \end{aligned}$$

The result follows by induction. □

Lemma 3 (Cochrane [4]). *For any positive integers* b, c *with* $b > 1$ *we have*

$$T(b,c) = \sum_{a=1}^{b-1} \left| \frac{\sin(\pi ac/b)}{\sin(\pi a/b)} \right| < \frac{4}{\pi^2} b \ln b + 0.38b + 0.608 + 0.116 \frac{d^2}{b},$$

where $d = \gcd(b, c)$. *The constant* $4/\pi^2$ *in the main term is the best possible.*

We will use

$$C(q) = \frac{4}{\pi^2}(q-1)\ln(q-1) + 0.38(q-1) + 0.608 + 0.116\frac{1}{q-1}$$

as the upper bound for $T(q-1,c)$, where $\gcd(q-1,c) = 1$.

Theorem 4. *Let $k \geq 2$ be an integer and $v = (0,\ldots,0,1,v_{k-2},\ldots,v_1,1) \in \mathbb{F}_2^n$ be a vector. Suppose that $W = W(v)$ is defined as above. Let η be a $(q-1)$th root of unity. Then,*

$$R(v,q) = \sum_{j=1}^{q-2}\left|\sum_{w\in W}\eta^{jw}\right| < (2^{k+1}+1)C(q) + q - 2.$$

Proof. By Definition 1 we know that

$$\sum_{w\in\overline{W}}\eta^{jw} = G(v)(\eta^j) = G_k(v)(\eta^j) \tag{8}$$

for all $1 \leq j \leq q-2$. By (7) and (8) we obtain

$$\begin{aligned}\sum_{j=1}^{q-2}\left|\sum_{w\in\overline{W}}\eta^{jw}\right| &\leq \sum_{j=1}^{q-2}\left|\frac{\eta^{j2^{k-1}}}{1+\eta^{j2^{k-1}}}\right| + \sum_{j=1}^{q-2}\left|\frac{1-\eta^j}{1-\eta^{j2^k}}\right|\left|\prod_{i=0}^{k-1}(1+(-1)^{v_i}\eta^{j2^i})\right| \\ &\quad + \sum_{s:v_s=1}\sum_{j=1}^{q-2}\left|\frac{\eta^{j2^s}(1-\eta^{j2^s})}{1-\eta^{j2^k}}\right|\left|\prod_{i=s+1}^{k-1}(1+(-1)^{v_i}\eta^{j2^i})\right| \qquad (9) \\ &< \sum_{j=1}^{q-2}\left|\frac{1-\eta^{j2^{k-1}}}{1-\eta^{j2^k}}\right| + 2^k\sum_{j=1}^{q-2}\left|\frac{1-\eta^j}{1-\eta^{j2^k}}\right| \\ &\quad + \sum_{s:v_s=1}2^{k-s-1}\sum_{j=1}^{q-2}\left|\frac{1-\eta^{j2^s}}{1-\eta^{j2^k}}\right|. \qquad (10)\end{aligned}$$

Substituting η by $\eta^{2^{n-k}}$ on the right-hand side we obtain

$$\begin{aligned}\sum_{j=1}^{q-2}\left|\sum_{w\in\overline{W}}\eta^{jw}\right| &< \sum_{j=1}^{q-2}\left|\frac{1-\eta^{j2^{n-1}}}{1-\eta^j}\right| + 2^k\sum_{j=1}^{q-2}\left|\frac{1-\eta^{j2^{n-k}}}{1-\eta^j}\right| \\ &\quad + \sum_{s:v_s=1}2^{k-s-1}\sum_{j=1}^{q-2}\left|\frac{1-\eta^{j2^{n-k+s}}}{1-\eta^j}\right|.\end{aligned}$$

Let l be a nonnegative integer. By Lemma 3 we have

$$\sum_{j=1}^{q-2}\left|\frac{1-\eta^{j2^l}}{1-\eta^j}\right| = \sum_{j=1}^{q-2}\left|\frac{\sin(2^l\pi j/(q-1))}{\sin(\pi j/(q-1))}\right| = T(q-1,2^l) < C(q),$$

where $C(q)$ is defined as above. Thus,

$$\sum_{j=1}^{q-2}\left|\sum_{w\in\overline{W}}\eta^{jw}\right| < C(q)+2^kC(q)+2^{k-1}C(q)\sum_{s:v_s=1}2^{-s}$$
$$\le C(q)+2^kC(q)+2^kC(q),$$

and

$$\sum_{j=1}^{q-2}\left|\sum_{w\in W}\eta^{jw}\right| \le \sum_{j=1}^{q-2}\left|\sum_{w\in\overline{W}}\eta^{jw}\right| + q-2 < (2^{k+1}+1)C(q)+q-2.$$

□

Theorem 5. *Let $k\ge 2$ be an integer and $v=(0,\dots,0,1,v_{k-2},\dots,v_1,1)\in\mathbb{F}_2^n$ be a vector. For $q\ge 4$, we have*

$$\max_{u\in\mathbb{F}_2^n}|\widehat{v\cdot f}(u)| < \frac{8}{\pi^2}(2^{k+1}+1)(\ln(q-1)+2)q^{1/2}.$$

Proof. Function f is balanced, so $\widehat{v\cdot f}(u)=0$ if $u=0$. Suppose that $u\ne 0$ and $W=W(v)$ is defined as above. Let $\psi_u\colon\mathbb{F}_q\to\{-1,1\}$ be the mapping defined by $x\mapsto(-1)^{u\cdot x}$. By the definition of function f we have $f(0)=q-1$. Hence, $v\cdot f(0)=w_{\mathrm{H}}(v) \bmod 2$. By Lemma 1 we obtain

$$\begin{aligned}
|\widehat{v\cdot f}(u)| &= \left|\sum_{x\in\mathbb{F}_q}(-1)^{v\cdot f(x)+u\cdot x}\right| \\
&= \left|\sum_{x\in\mathbb{F}_q^*}(-1)^{v\cdot\log_\alpha x+u\cdot x}+(-1)^{w_{\mathrm{H}}(v)}\right| \\
&= \left|\sum_{x\in\mathbb{F}_q^*}\frac{2}{q-1}\left(\sum_{j=1}^{q-2}\sum_{w\in W}\eta^{jw}\chi^j(x)-\frac{(-1)^{w_{\mathrm{H}}(v)}}{2}\right)\psi_u(x)+(-1)^{w_{\mathrm{H}}(v)}\right| \\
&\le \frac{2}{q-1}\sum_{j=1}^{q-2}\left|\sum_{w\in W}\eta^{jw}\right|\left|\sum_{x\in\mathbb{F}_q^*}\chi^j(x)\psi_u(x)\right|+\frac{1}{q-1}\left|\sum_{x\in\mathbb{F}_q^*}\psi_u(x)\right|+1.
\end{aligned}$$

Since ψ_u is an additive character of $\mathbb{F}_q$, we have (see e.g. [7])

$$\sum_{x\in\mathbb{F}_q^*}\psi_u(x)=-1 \quad\text{and}\quad \left|\sum_{x\in\mathbb{F}_q^*}\chi^j(x)\psi_u(x)\right|=q^{1/2}$$

for $u\ne 0$. Thus,

$$|\widehat{v\cdot f}(u)| \le \frac{2}{q-1}\sum_{j=1}^{q-2}\left|\sum_{w\in W}\eta^{jw}\right|q^{1/2}+\frac{q}{q-1}. \tag{11}$$

The result follows by Theorem 4. □

Corollary 1. *Let $k \geq 2$ be an integer and $v = (0, \ldots, 0, 1, v_{k-2}, \ldots, v_1, 1) \in \mathbb{F}_2^n$ be a vector. For $q \geq 4$, we have*

$$\mathcal{N}(v \cdot f) > 2^{n-1} - \frac{4}{\pi^2}(2^{k+1} + 1)(\ln(2^n - 1) + 2)2^{n/2}. \tag{12}$$

Proof. The result follows directly from the definition of nonlinearity and Theorem 5. □

Corollary 2. *For $q \geq 4$ and for all f_i, $0 \leq i \leq n-1$, we have*

$$\mathcal{N}(f_i) > 2^{n-1} - \frac{4}{\pi^2}(\ln(2^n - 1) + 2)2^{n/2}. \tag{13}$$

Proof. Let $v = (0, \ldots, 0, 1) \in \mathbb{F}_2^n$, in which case $v \cdot f = f_0$, and suppose that $W = W(v)$ is defined as above. By Lemma 3 we have

$$\sum_{j=1}^{q-2} \left| \sum_{w \in W} \eta^{jw} \right| = \sum_{j=1}^{q-2} \left| \frac{1 - \eta^j}{1 - \eta^{2j}} \right| = \sum_{j=1}^{q-2} \left| \frac{\sin(2^{n-1}\pi j/(q-1))}{\sin(\pi j/(q-1))} \right| < C(q).$$

We can obtain an upper bound for $\max_{u \in \mathbb{F}_2^n} |\widehat{v \cdot f}(u)|$ as in the proof of Theorem 5, but using the above bound in (11). The result follows from the definition of nonlinearity and Theorem 2. □

6 Discussion

We present several values related to the nonlinearity of f in Table 1. For $n = 2, \ldots, 11$, we give the true nonlinearities for f and its coordinate functions f_i. On the rightmost column, we give one of the masks $v \in \mathbb{F}_2^n$ for which $v \cdot f$ has the lowest nonlinearity. Each mask is presented as a binary number $v_{n-1} \ldots v_1 v_0$ unless the nonlinearity of $v \cdot f$ is the same for all $v \in \mathbb{F}_2^n$. In addition, we present the values given by the lower bound for the nonlinearity of each coordinate function f_i of f. These values, denoted by $\mathcal{B}(f_i)$, are slightly better than the ones given by (13), since we have not used the estimates that were used to simplify the appearance of the bound. We also give the values of

$$D(q) = \max_{\substack{v \in \mathbb{F}_2^n \\ v \neq 0}} R(v, q) = \max_{\substack{v \in \mathbb{F}_2^n \\ v \neq 0}} \sum_{j=1}^{q-2} \left| \sum_{w \in W} \eta^{jw} \right|$$

and $C(q)$, which is the basis for the upper bound given by Theorem 4. All values are rounded to the nearest (nonnegative) integer.

Table 1 shows that the nonlinearity of f seems to grow about at the same rate as the nonlinearity of the coordinate functions of f. However, our lower bound (12) for the nonlinearity of f gets exponentially worse as the length k of the linear mask v increases. The main reason for this seems to be the non-strict upper bound for $D(q)$ given by Theorem 4. Table 1 shows that the real maximum

Table 1. Nonlinearity of f and related values

n	$\mathcal{N}(f_i)$	$\mathcal{N}(f)$	$\mathcal{B}(f_i)$	$D(q)$	$C(q)$	v
2	0	0	0	2	3	-
3	2	0	0	8	9	111
4	4	4	1	24	23	-
5	10	10	5	68	56	-
6	24	20	15	179	132	001001
7	54	44	37	471	301	1111111
8	112	100	85	1236	675	00110011
9	232	198	190	3253	1479	111111111
10	484	420	409	8520	3283	0101010101
11	980	934	866	22542	7145	00010110111

values $D(q)$ for $R(v, q)$ over all nonzero $v \in \mathbb{F}_2^n$ are significantly smaller than the values given by the bound. In the proof of Theorem 4, we use coarse estimates to arrive at (10). To obtain a better bound, one should estimate the sums in (9) more accurately. These sums can be rewritten as trigonometric sums that resemble the sum in Lemma 3, but are more complicated. For $n = 2, \ldots, 11$, we can use the real maximum values $D(q)$ for $R(v, q)$ in (11) to determine how accurate a bound could be obtained with our approach if we had a good estimate for $D(q)$. The bound obtained this way is not as tight as the bound for each coordinate function of f. However, it seems to grow at the same rate as the true nonlinearity. Note that the bound for each coordinate function is actually better than the one given by Carlet and Feng [2], who did not use the bound given by Lemma 3.

7 Conclusion

We investigated nonlinearity of the discrete logarithm in $\mathbb{F}_{2^n}$. By extending the methods of Brandstätter et al., who studied the least significant bit of discrete logarithm, we were able to derive a lower bound for the nonlinearity of an arbitrary linear combination of the discrete logarithm function extended to a bijection in $\mathbb{F}_2^n$. According to our experiments, the length of the linear combination, which corresponds to the output dimension of the Feng–Liao–Yang S-boxes, should not affect the nonlinearity to the same extent as it affects the bound. For this reason, we investigated experimentally steps in our estimation chain that could potentially be improved. Determining a more accurate lower bound and proving that S-boxes based on discrete logarithm, such as the Feng–Liao–Yang S-boxes, are highly nonlinear remains an interesting open problem.

Acknowledgements. We wish to thank the anonymous reviewers for helpful comments. The research work of the first author has been supported by Helsinki Graduate School in Computer Science and Engineering, Academy of Finland (project #122736), Nokia Foundation, and KAUTE Foundation.

References

1. Brandstätter, N., Lange, T., Winterhof, A.: On the non-linearity and sparsity of Boolean functions related to the discrete logarithm in finite fields of characteristic two. In: Ytrehus, Ø. (ed.) WCC 2005. LNCS, vol. 3969, pp. 135–143. Springer, Heidelberg (2006)
2. Carlet, C., Feng, K.: An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 425–440. Springer, Heidelberg (2008)
3. Carlet, C., Feng, K.: An infinite class of balanced vectorial Boolean functions with optimum algebraic immunity and good nonlinearity. In: Chee, Y.M., Li, C., Ling, S., Wang, H., Xing, C. (eds.) IWCC 2009. LNCS, vol. 5557, pp. 1–11. Springer, Heidelberg (2009)
4. Cochrane, T.: On a trigonometric inequality of Vinogradov. Journal of Number Theory 27(1), 9–16 (1987)
5. Feng, K., Liao, Q., Yang, J.: Maximal values of generalized algebraic immunity. Designs, Codes and Cryptography 50(2), 243–252 (2009)
6. Konyagin, S., Lange, T., Shparlinski, I.: Linear complexity of the discrete logarithm. Designs, Codes and Cryptography 28(2), 135–146 (2003)
7. Lidl, R., Niederreiter, H.: Finite fields. In: Encyclopedia of Mathematics and its Applications, 2nd edn., vol. 20. Cambridge University Press, Cambridge (1997)
8. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994)

On a Conjecture about Binary Strings Distribution

Jean-Pierre Flori[1], Hugues Randriam[1], Gérard Cohen[1], and Sihem Mesnager[2]

[1] Institut Télécom, Télécom ParisTech, CNRS LTCI, 46 rue Barrault
F-75634 Paris Cedex 13, France
[2] LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS,
Department of Mathematics, University of Paris XIII and University of Paris VIII
2 rue de la liberté, 93526 Saint-Denis Cedex, France

Abstract. It is a difficult challenge to find Boolean functions used in stream ciphers achieving all of the necessary criteria and the research of such functions has taken a significant delay with respect to cryptanalyses. Very recently, an infinite class of Boolean functions has been proposed by Tu and Deng having many good cryptographic properties under the assumption that the following combinatorial conjecture about binary strings is true:

Conjecture 0.1. Let $S_{t,k}$ be the following set:

$$S_{t,k} = \left\{ (a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 \,|\, a+b=t \text{ and } w(a)+w(b)<k \right\} \ .$$

Then:

$$|S_{t,k}| \leq 2^{k-1} \ .$$

The main contribution of the present paper is the reformulation of the problem in terms of *carries* which gives more insight on it than simple counting arguments. Successful applications of our tools include explicit formulas of $|S_{t,k}|$ for numbers whose binary expansion is made of one block, a proof that the conjecture is *asymptotically* true and a proof that a family of numbers (whose binary expansion has a high number of 1s and isolated 0s) reaches the bound of the conjecture. We also conjecture that the numbers in that family are the only ones reaching the bound.

1 Introduction

Symmetric cryptosystems are commonly used for encrypting and decrypting owing to their efficiency. A classical model of symmetric cryptosystem are stream ciphers. They are composed of one or several Linear Feedback Shift Register (LFSR) combined or filtered by a Boolean function. These cryptosystems have been the objects of a lot of cryptanalyses and several design criteria have been proposed concerning the filtering or combining functions, mainly: balancedeness,

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 346–358, 2010.

a high algebraic degree, a high nonlinearity. Moreover, because of the recent algebraic attacks of Courtois and Meier [1], which have received a lot of attention in cryptographic literature, the notion of algebraic immunity has been introduced. A high algebraic immunity is now an absolutely necessary (but not sufficient for resisting the Fast Algebraic Attacks introduced by Courtois [2]) property for Boolean functions used in stream ciphers. Several constructions of Boolean functions with high algebraic immunity have been provided but very few of them are of optimal algebraic immunity. More importantly, those having other good cryptographic properties, as bentness, balancedness or high nonlinearity for instance, are even rarer.

In 2008, Carlet and Feng [3] proposed for the first time an infinite class of functions which seems able to satisfy all of the main criteria for being used as a filtering function in a stream cipher. Their functions are balanced with optimal algebraic degree, optimal algebraic immunity, good immunity to Fast Algebraic Attacks and good nonlinearity. Very recently, it has been revealed by Tu and Deng in [4] that there may be Boolean functions of optimal algebraic immunity in a classical class of Partial Spread functions due to Dillon [5] provided that Conjecture 0.1 is correct.

The authors of [4] assume the validity of the conjecture and checked it for $k \leq 29$. They also proved that, if the conjecture is true, then one can get in even dimension balanced Boolean functions of optimal algebraic immunity and of high nonlinearity (better than that of the function proposed in [3]). The approach of the authors was to identify annihilators of the Boolean functions in n variables that they consider with codewords of BCH codes. The role of the conjecture is then to deduce from the BCH bound that those codewords are equal to zero if the algebraic degree of the corresponding annihilator is less than $\lceil \frac{n}{2} \rceil$. Very recently, Carlet [6] has observed that the function introduced by Tu and Deng is weak against Fast Algebraic Attacks and tried to repair its weakness. Any possibility of a real repair of this weakness (or an alternative function sharing all the properties of the Tu-Deng function but not having this weakness) should give an infinite class of balanced functions having a good behavior against Fast Algebraic Attacks, optimal algebraic immunity, optimal algebraic degree and good nonlinearity; that is, the best construction of an infinite class of Boolean functions proposed in the literature.

In the present paper we attack this conjecture. It is organized as follows. In Sect. 2, we prove several simple properties and reformulate the problem in terms of *carries*. In Sect. 3 we apply our new formulation in different situations. In particular we compute in Sect. 3.3 exact formulas of $|S_{t,k}|$for numbers made of only one block. We then introduce a constraint in Sect. 3.4 which greatly simplifies calculations. It leads us to a proof that the conjecture is *asymptotically* true in Subsection 3.5 and to a proof that a family of numbers reaches the bound (we believe they are the only ones to do so) in Sect. 3.7. The most important notations are given in Definitions 3.1 and 3.3. An extended version of this paper, including proofs and additional results, is available on `http://eprint.iacr.org/` [7].

2 Reformulation and First Results

2.1 Notations

Unless stated otherwise, we use the following notations:

- $k \in \mathbb{N}$ the number of bits (or length of binary strings) we are currently working on.
- $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ a fixed modular integer.

We denote the binary (or Hamming) weight of t by $w(t)$ (or simply w).

The sets we are interested in are:

- $C_{t,k,i} = \left\{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2 | a+b=t, w(a)+w(b)=k+i\right\}$, the modular integers whose sum is t and whose sum of weights is $k+i$ for $i \in \mathbb{Z}$.
- $C_{t,k} = \bigsqcup_{i\in\mathbb{Z}} C_{t,k,i}$, $S_{t,k} = \bigsqcup_{i<0} C_{t,k,i}$, $T_{t,k} = \bigsqcup_{i>0} C_{t,k,i}$.

2.2 Negation

For $a \neq 0 \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, we define $\overline{a}$ as the modular integer whose binary expansion is the binary not on k bits of the binary expansion of a. It is easy to see that $a+\overline{a} = \sum_{i=0}^{k-1} 2^i = 2^k - 1 = 0$ so that $-a = \overline{a}$ and $w(-a) = w(\overline{a}) = k - w(a)$.

We are now able to deal with the pathological case $t = 0$:

Proposition 2.1

$$S_{0,k} = \{(0,0)\} \text{ and } |S_{0,k}| = 1 \ .$$

Proof. Indeed $(a,b) \in S_{0,k}$ iff $b = -a$ and $w(a) + w(-a) = k$ iff $a \neq 0$ (and if $a = 0 = -a$, then $w(a) + w(a) = 0$) so that $S_{0,k} = \{(0,0)\}$. □

From now on we suppose $t \neq 0$.

2.3 Rotation

Another simple transformation is multiplication by 2. Indeed, working modulo $2^k - 1$, it is just rotating the binary expansion one bit to the left, so that for all $i \in \mathbb{Z}$ and $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, we have $w(2^i a) = w(a)$ and we get the following proposition:

Proposition 2.2. *For $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ and $i \in \mathbb{Z}$:*

$$S_{2^i t,k} = 2^i S_{t,k} = \left\{(2^i a, 2^i b) | (a,b) \in S_{t,k}\right\} \text{ and } |S_{t,k}| = \left|S_{2^i t,k}\right| \ .$$

We say that for any $i \in \mathbb{Z}$, $2^i t$ and t are equivalent and we write $t \simeq 2^i t$.

Proof. Indeed for $(a,b) \in S_{t,k}$, $2^i a + 2^i b = 2^i t$ and $w(2^i a) + w(2^i b) = w(a) + w(b) < k$. □

2.4 Carries

We now define the main tool used in this paper:

Definition 2.3. *For $a \in \mathbb{Z}/(2^k-1)\mathbb{Z}$, $a \neq 0$, we set:*

$$r(a,t) = w(a) + w(t) - w(a+t) \ ,$$

i.e. $r(a,t)$ is the number of carries occurring while performing the addition. By convention we set:

$$r(0,t) = k \ ,$$

i.e. 0 behaves like the $\underbrace{1\ldots1}_{k}$ binary string. We also remark that $r(-t,t) = k$.

The following proposition is fundamental. It brings to light the importance of the number of carries occuring during the addition.

Proposition 2.4

$$C_{t,k,i} = \{(a, t-a) | r(-a,t) = w(t) - i\} \ \textit{and} \ |S_{t,k}| = |\{a | r(a,t) > w(t)\}| \ .$$

Proof. For $(a,b) \in C_{t,k,i}$ we have $a + b = t$ so $b = t - a$ If $a \neq 0$, our condition for $C_{t,k,i}$ becomes:

$$\begin{aligned} w(a) + w(t-a) = k + i &\Leftrightarrow w(-(-a)) + w(-a+t) = k + i \\ &\Leftrightarrow k - w(-a) + w(-a+t) = k + i \\ &\Leftrightarrow r(-a,t) = w(t) - i \ . \end{aligned}$$

We also have $r(0,t) = k = w(t) - (w(t) - k)$ and $(0,t) \in C_{t,k,w(t)-k}$. □

The following lemma allows us to prove some relations between $S_{t,k}$, $T_{t,k}$ and $S_{-t,k}$.

Lemma 2.5. *If $a \neq 0, -t$, then $r(a,t) = k - r(-a,-t)$.*
If $a = 0, -t$, then $r(a,t) = r(-a,-t) = k$.

Proof. If $a \neq 0, -t$, going back to the definition of $r(a,t)$, we have:

$$\begin{aligned} r(a,t) &= w(a) + w(t) - w(a+t) \\ &= k - w(-a) + k - w(-t) - k + w(-a-t) \\ &= k - r(-a,-t) \ . \end{aligned}$$

□

Definition 2.6. *We define:*

$$S^*_{t,k} = S_{t,k} \backslash \{(0,t),(t,0)\} \ .$$

Proposition 2.7

$$T_{t,k} = -S^*_{-t,k} \ .$$

Proof. Indeed if $(a, t-a) \in T_{t,k}$, then $a \neq 0, t$ and $r(-a,t) < w(t)$, so that $r(a,-t) > w(-t)$ and $(-a, -t+a) \in S^*_{-t,k}$.

Conversely if $(a, -t-a) \in S^*_{-t,k}$, then $(-a, t+a) \in T_{t,k}$. □

Corollary 2.8

$$|S_{t,k}| + |S_{-t,k}| \leq 2^k \ .$$

Proof. We already know that $S_{t,k} \sqcup T_{t,k} \subset C_{t,k}$ so that $|S_{t,k}| + |S_{-t,k}| \leq 2^k + 1$. But in fact $w(t+t) = w(2t) = w(t)$ so that $(2t, -t)$ is in $C_{t,k,0}$, i.e. neither in $S_{t,k}$ nor in $T_{t,k}$ and:

$$|S_{t,k}| + |S_{-t,k}| \leq 2^k \ .$$

□

Corollary 2.8 and Proposition 2.2 together prove the conjecture in the specific case where $t \simeq -t$:

Theorem 2.9. *If $t \simeq -t$, then $|S_{t,k}| \leq 2^{k-1}$.*

3 A Block Splitting Pattern

3.1 General Situation

In this section, we often compute $P_{t,k} = 2^{-k}\,|S_{t,k}|$ rather than $|S_{t,k}|$. Therefore we use the words *proportion* or *probability* in place of *cardinality*. Moreover we often compute cardinalities considering all the binary strings on k bits, i.e. including `1...1` and `0...0`. The modular integer 0 is considered to act as the binary string `1...1` , but the binary string `0...0` should be discarded when doing final computation of $P_{t,k}$. However it ensures that variables are truly *independent*.

We split $t(\neq 0)$ (once correctly rotated, i.e. we multiply it by a correct power of 2 so that its binary expansion on k bits begins with a `1` and ends with a `0`) in blocks of the form $[1^*0^*]$ (i.e. as many `1`s as possible followed by as many `0`s as possible).

Definition 3.1. *We denote the number of blocks by d and the numbers of `1`s and `0`s of the ith block t_i by α_i and β_i.*

We define corresponding variables for a (a number to be added to t): γ_i the number of `0`s in front of the end of the `1`s subblock of t_i, δ_i the number of `1`s in front of the end of the `0`s subblock of t_i.

Those definitions are depicted below:

$$t = \overbrace{1\text{---}1}^{\alpha_1}\overbrace{0\text{---}0}^{\beta_1}\ldots\overbrace{1\text{---}1}^{\alpha_i}\overbrace{0\text{---}0}^{\beta_i}\ldots\overbrace{1\text{---}1}^{\alpha_d}\overbrace{0\text{---}0}^{\beta_d}\ ,$$

$$a = \underbrace{?10\text{-}0}_{\gamma_1}\underbrace{?01\text{-}1}_{\delta_1}\ldots\underbrace{?10\text{-}0}_{\gamma_i}\underbrace{?01\text{-}1}_{\delta_i}\ldots\underbrace{?10\text{-}0}_{\gamma_d}\underbrace{?01\text{-}1}_{\delta_d}\ ,$$

One should be aware that γ_is and δ_is depend on a and are considered as variables.

We first "approximate" $r(a,t)$ by $\sum_{i=0}^{d} \alpha_i - \gamma_i + \delta_i$ ignoring the two following facts:

- if a carry goes out of the $i-1$st block (we say that it *overflows*) and $\delta_i = \beta_i$, the 1s subblock produces α_i carries, whatever value γ_i takes,
- and if no carry goes out of the $i-1$st block (we say that it is *inert*), the 0s subblock produces no carries, whatever value β_i takes.

When computing that "approximation" of the number of carries produced by the ith block, we do as if a carry always goes out of the $i-1$st block and no carry goes out of the 0s subblock.

Then $r(a,t) > w(t)$ becomes "approximately" $\sum_{i=1}^{d} \gamma_i < \sum_{i=1}^{d} \delta_i$ and we have the following distributions for γ_i and δ_i:

$c_i =$	0	1	...	c_i	...	$\alpha_i - 1$	α_i	$\alpha_i + 1$	...
$P(\gamma_i = c_i)$	1/2	1/4	...	$1/2^{c_i+1}$	...	$1/2^{\alpha_i}$	$1/2^{\alpha_i}$	0	...

$d_i =$	0	1	...	d_i	...	$\beta_i - 1$	β_i	$\beta_i + 1$	...
$P(\delta_i = d_i)$	1/2	1/4	...	$1/2^{d_i+1}$	...	$1/2^{\beta_i}$	$1/2^{\beta_i}$	0	...

For $0 \leq c_i < \alpha_i$:

$$P(\gamma_i = c_i) = 2^{-c_i-1} \ ,$$

because we have to set c_i bits to 0 and one bit in front of them to 1 leaving the other bits free, and:

$$P(\gamma_i = \alpha_i) = 2^{-\alpha_i}$$

and not $2^{-\alpha_i-1}$ because the subblock is already full of 0s and there si no 1 in front of them.

The computations are similar for $P(\delta_i = d_i)$ with $0 \leq d_i \leq \beta_i$. Moreover all the γ_is and δ_is are independent, i.e. $P(\gamma_1 = c_1, \ldots, \gamma_d = c_n, \delta_1 = d_1, \ldots, \delta_d = d_d) = \prod_{i=1}^{d} P(\gamma_i = c_i) P(\delta_i = d_i)$.

We modify γ_i and δ_i to take the first fact into account and only do as as if a carry always goes out of the $i-1$st block:

- if $\delta_i \neq \beta_i$, we define $\delta'_i = \delta_i$ and $\gamma'_i = \gamma_i$ as before,
- if $\delta_i = \beta_i$, we define $\delta'_i = \delta_i = \beta_i$ and $\gamma'_i = 0$ (i.e. the carry coming from the previous block goes through the 0s subblock so the 1s subblock always produces α_i carries).

Then $\sum_{i=0}^{d} \alpha_i - \gamma'_i + \delta'_i$ should be a better "approximation" of $r(a,t)$, but the γ'_is and δ'_is are no longer pairwise independent. Indeed within the same block, γ'_i and δ'_i are correlated. However each block remains independent of the other ones and the distributions are as follows:

$c_i =$	0	1	...	c_i	...	$\alpha_i - 1$	α_i	$\alpha_i + 1$	...
$P(\gamma'_i = c_i)$	$\frac{1+1/2^{\beta_i}}{2}$	$\frac{1-1/2^{\beta_i}}{4}$	...	$\frac{1-1/2^{\beta_i}}{2^{c_i+1}}$	...	$\frac{1-1/2^{\beta_i}}{2^{\alpha_i}}$	$\frac{1-1/2^{\beta_i}}{2^{\alpha_i}}$	0	...

$d_i =$	0	1	...	d_i	...	$\beta_i - 1$	β_i	$\beta_i + 1$	...
$P(\delta'_i = d_i)$	1/2	1/4	...	$1/2^{d_i+1}$	...	$1/2^{\beta_i}$	$1/2^{\beta_i}$	0	...

Taking the second fact into account is more difficult, and we do it in an iterative way.

We first take care of the a's such that $r(a,t) = k$, that is exactly those with only `1`s in front of the `0`s of t:

– if $\forall i, \delta_i = \beta_i$, then $\delta''_i = \delta_i$ and $\gamma''_i = \gamma'_i = 0$.

We now suppose that there exists i_0 such that $\delta_{i_0} \neq \beta_{i_0}$. We first define γ''_{i_0}, then δ''_{i_0+1}, γ''_{i_0+1}, ... and finally δ''_{i_0}:

– set $\gamma''_{i_0} = \gamma_{i_0}$, $i = i_0 + 1$,
– do:
  • $\delta''_i = \delta_i$ if $\gamma_{i-1} \neq \alpha_{i-1}$, 0 otherwise,
  • $\gamma''_i = \gamma_i$ if $\delta''_i \neq \beta_i$, 0 otherwise,
  • $i = i + 1$

  while $i \neq i_0 + 1$

The γ''_is and δ''_is are no longer pairwise independent, even between different blocks, but $r(a,t) = \sum_d \alpha_i - \gamma''_i + \delta''_i$ and the following proposition is verified:

Proposition 3.2. *$a \in S_{t,k}$ iff $\sum_d \gamma''_i < \sum_d \delta''_i$.*

Remember that t is considered to be fixed so that the α_is and the β_is are considered to be constants, whereas the other quantities defined in this section depend on a which ranges over all binary strings on k bits and will be considered as variables, whence the vocabulary we use.

3.2 Combining Variables

In the previous subsection we defined two variables for each block. However we are only really interested in the number of carries, so one should suffice.

Definition 3.3. *We define $\epsilon_i = \gamma_i + \beta_i - \delta_i$ and $E = \sum_{i=1}^{d} \epsilon_i$, as depicted below:*

$$t = \overbrace{\texttt{1---1}}^{\alpha_1}\overbrace{\texttt{0---0}}^{\beta_1}\texttt{...}\overbrace{\texttt{1---1}}^{\alpha_i}\overbrace{\texttt{0---0}}^{\beta_i}\texttt{...}\overbrace{\texttt{1---1}}^{\alpha_d}\overbrace{\texttt{0---0}}^{\beta_d},$$
$$a = \texttt{?}\underbrace{\texttt{10-0?01}}_{\epsilon_1}\texttt{-1...?}\underbrace{\texttt{10-0?01}}_{\epsilon_i}\texttt{-1...?}\underbrace{\texttt{10-0?01}}_{\epsilon_d}\texttt{-1},$$

Then ϵ_i is "approximately" the number of carries that do not occur in the ith block. As in the previous subsection, we define $\epsilon'_i = \gamma'_i + \beta_i - \delta'_i$ and $\epsilon''_i = \gamma''_i + \beta_i - \delta''_i$ and Proposition 3.2 becomes:

Proposition 3.4. *$a \in S_{t,k}$ iff $\sum_d \epsilon''_i < \sum_d \beta_i = k - w(t)$.*

3.3 One Block: $d = 1$

If t is made of only one block, we compute closed forms for $|C_{t,k,i}| = 2^k P(\epsilon'' = k - i)$ for all i.

Such a t (or an equivalent one) is written $t = 2^k - 2^{k-\alpha}$ (i.e. $t = \underbrace{\texttt{1...1}}_{\alpha}\underbrace{\texttt{0...0}}_{\beta=k-\alpha}$) and its weight is $w(t) = \alpha$ with $\alpha \geq 1$.

In the following proposition, the computations are made without including the binary string `0...0` in contrast with what was done in the previous subsections because it does not complicate them.

Proposition 3.5. *The distribution of ϵ'' is as follows:*

$$P(\epsilon = 0) = 2^{-\beta} \ ;$$

for $0 < e < \alpha + \beta$:

$$P(\epsilon'' = e) = 2^{-|e-\beta|}\frac{1 - 4^{M-m}}{3} \ ,$$

with:

$$m = \min(e, \alpha) \text{ and } M = \max(0, e - \beta) \ ;$$

and

$$P(\epsilon'' = \alpha + \beta) = 2^{-\alpha} - 2^{-\alpha-\beta} \ .$$

Proof. If $\delta = \beta$, then $\gamma'' = 0$ and we lose no carries whatever value γ takes. Moreover those numbers are the only ones such that we lose no carries and the block overflows, therefore:

$$P(\epsilon'' = 0) = P(\delta = \beta) = 2^{-\beta} \ .$$

One must be aware that we included the binary string `1...1` but it accounts for the modular integer 0.

When $\delta \neq \beta$ and $\gamma = \alpha$, we lose all the carries whatever value δ takes, and that is the only possibility to do so Then:

$$P(\epsilon'' = \alpha + \beta) = P(\gamma = \alpha, \delta \neq \beta) - 2^{-\alpha-\beta} = 2^{-\alpha} - 2^{-\alpha-\beta} \ .$$

We substract $2^{-\alpha-\beta}$ because we do not want to count the binary string `0...0`.

Finally, when $\delta \neq \beta$ and $\gamma \neq \alpha$, the situation is described below:

$$t = \overleftarrow{\overbrace{\texttt{1---1}}^{\alpha}\overbrace{\texttt{0---0}}^{\beta}}, \qquad a = \texttt{?10-0?01-1} \ .$$

A carry comes out of the block and goes back into itself. Then we lose exactly $e = \epsilon'' = \gamma + \beta - \delta = \epsilon$ carries and $0 < e < \alpha + \beta - 1$. We have the following constraints:

$$0 \leq \gamma \leq \alpha - 1 \text{ and } 0 \leq \delta \leq \beta - 1 \ ,$$

but $\delta = \beta + \gamma - e$ so γ must be bounded as follows:

$$M = \max(0, e - \beta) \leq \gamma \leq m - 1 = \min(e, \alpha) - 1 \ .$$

And $P(\epsilon'' = e)$ for $0 < e < \alpha + \beta$ is computed below:

$$\begin{aligned} P(\epsilon'' = e) &= \sum_{\gamma=M}^{m-1} 2^{-\gamma-\delta-2} = \sum_{\gamma=M}^{m-1} 2^{e-\beta-2\gamma-2} \\ &= 2^{e-\beta-2M-2} \sum_{\gamma=0}^{m-M-1} 2^{-2\gamma} = 2^{-|e-\beta|-2} \frac{1-(1/4)^{m-M}}{3/4} \\ &= 2^{-|e-\beta|} \frac{1-4^{M-m}}{3} \ . \end{aligned}$$ □

Summing up the above formulas, we get the following theorem:

Theorem 3.6

$$P_{t,k} = \begin{cases} 2^{-\alpha-\beta} \frac{1-2^{-2\alpha}}{3} & \text{if } 1 \leq \alpha \leq \frac{k-1}{2} \\ \frac{1+2^{-2\beta+1}}{3} & \text{if } \frac{k-1}{2} \leq \alpha \leq k-1 \end{cases} .$$

For $\alpha = 1$, it reads $S_{1,k} = 2^{k-2} + 1$ and for $\alpha = k-1$, it reads $S_{-1,k} = 2^{k-1}$.

The probabilities that we computed above will be useful in the next section.

Definition 3.7. *For $0 \leq e < \alpha + \beta$, we define:*

$$P(e) = \begin{cases} 2^{-\beta} & \text{if } e = 0 \\ 2^{-|e-\beta|} \frac{1-4^{M-m}}{3} & \text{if } e \neq 0 \end{cases} ,$$

with:

$$m = \min(e, \alpha) \text{ and } M = \max(0, e-\beta) \ ;$$

the values of α and β will be clear from the context.

3.4 A Helpful Constraint: $\min_i(\alpha_i) \geq k - w(t) - 1$

Until the end of this section we add the following constraint on t:

$$\min_i(\alpha_i) \geq \sum_{i=1}^{d} \beta_i - 1 = k - w(t) - 1 \ .$$

That condition tells us that, if a is in $S_{t,k}$, a carry has to go through each subblock of 1s, i.e. $\gamma_i'' \neq \alpha_i$. Indeed, if $\gamma_i'' = \alpha_i$, then $\delta_i'' < \beta_i$ and $\epsilon_i'' = \gamma_i'' + \beta_i - \delta_i'' \geq \alpha_i + 1 \geq k - w(t)$, so that $a \notin S_{t,k}$. So if $a \in S_{t,k}$, each block overflows and we are in a situation where they are kind of independent.

In fact, if $\forall i$, $\gamma_i'' \neq \alpha_i$, then $\gamma_i'' = \gamma_i'$ and $\delta_i'' = \delta_i'$.

If $\forall i$, $\delta_i'' = \beta_i$, then $\gamma_i'' = \gamma_i' = 0$ and $\delta_i'' = \delta_i' = \beta_i$.

If there are a $\delta_i'' \neq \beta_i$ and a $\gamma_i'' = \alpha_i$, then $\sum_{i=1}^d \gamma_i'' \geq k - w(t) > \sum_{i=1}^d \delta_i''$. Moreover $\sum_{i=1}^d \gamma_i' \geq \sum_{i=1}^d \gamma_i''$ and $k - w(t) > \sum_{i=1}^d \delta_i'$, so that $\sum_{i=1}^d \gamma_i' \geq \sum_{i=1}^d \delta_i'$.

Finally, we have an equivalence between $r(a,t) > w(t)$ and $\sum_{i=1}^d \gamma_i' < \sum_{i=1}^d \delta_i'$:

Proposition 3.8

$$P_{t,k} = P\left[\sum_d \gamma'_i < \sum_d \delta'_i\right] \ .$$

It also means that $a \in S_{t,k}$ is equivalent to $\sum_d \epsilon'_i < k - w(t)$. Moreover that inequality implies that each block behaves like in the previous subsection and overflows into the next one, so that the computations we did are still valid (only to compute $|C_{t,k,i}|$ with $i < 0$, but not with $i \geq 0$) and we get the following proposition:

Proposition 3.9

$$P_{t,k} = \sum_{E=0}^{k-w(t)-1} \sum_{\substack{\sum_d e_i = E \\ 0 \leq e_i}} \prod_d P(e_i) \ .$$

In $P(e_i)$, we obviously replace α by α_i and β by β_i.

3.5 Asymptotic Behavior: $\beta_i \to \infty$

As the β_is go to infinity, the laws of the γ'_is and the δ'_is converge towards laws of independent geometrically distributed variables with parameter $1/2$, so that $P_{t,k} = P\left[\sum_d \gamma'_i < \sum_d \delta'_i\right]$ converges towards:

$$P\left[\sum_d Geo(1/2) < \sum_d Geo(1/2)\right] = \tfrac{1}{2}\left(1 - P\left[\sum_d Geo(1/2) = \sum_d Geo(1/2)\right]\right)$$

which is strictly lower than $1/2$ for any $d > 0$.

We have proved the following theorem:

Theorem 3.10. *Let d be a strictly positive integer. There exists a constant K_d such that if t verifies the two following constraints:*

$$\forall i, \beta_i \geq K_d \text{ and } \min_i \alpha_i \geq k - w(t) - 1 \ ,$$

then $|S_{t,k}| < 2^{k-1}$.

When the number of blocks, d, goes as well to infinity, we remark that $P_{t,k}$ converges toward $1/2$.

3.6 Analytic Study: $d = 2$

It is possible to compute the exact value of $|S_{t,k}|$ for a given d and a corresponding set of β_is. It is worth noting that the order of the β_is does not matter because each subblock behaves the same when a is in $S_{t,k}$, i.e. it overflows. We did the computation for $d = 2$ where the symmetry of the problem leads to only one situation and gives a quite general result.

Definition 3.11

$$f(x,y) = \frac{11}{27} + 4^{-x}\left(\frac{2}{9}x - \frac{2}{27}\right) + 4^{-y}\left(\frac{2}{9}y - \frac{2}{27}\right) + 4^{-x-y}\left(\frac{20}{27} - \frac{2}{9}(x+y)\right).$$

Proposition 3.12

$$P_{t,k} = f(\beta_1, \beta_2) \leq 1/2 \ .$$

Proof. An easy but quite lengthy and error-prone calculation, which can be checked with a symbolic calculus software, leads to the desired expression. The graph of f, computed with Maple$^{\text{TM}}$ [8], is given in Fig. 1. □

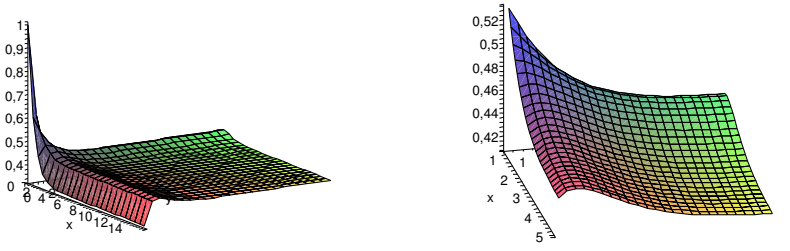


Fig. 1. $f(x, y)$

We have proved:

Theorem 3.13. *If t verifies the following constraints:*

$$d = 2 \text{ and } \alpha_1, \alpha_2 \geq k - w(t) - 1 \ ,$$

then $|S_{t,k}| \leq 2^{k-1}$.

3.7 Extremal Value: $\beta_i = 1$

We add another constraint: $\forall i, \beta_i = 1$. The previous one becomes: $\min_i(\alpha_i) \geq k - w(t) - 1 = d - 1$.

Theorem 3.14. *Let t verify the two following constraints:*

$$\forall i, \beta_i = 1 \text{ and } \min_i(\alpha_i) \geq k - w(t) - 1 = d - 1 \ ,$$

then $|S_{t,k}| = 2^{k-1}$.

Proof. Using Proposition 3.9, $P_{t,k}$ becomes:

$$P_{t,k} = \sum_{E=0}^{d-1} 2^{-E-d} \sum_{\substack{\sum_d e_i = E \\ 0 \leq e_i}} 1 = 2^{-d} \sum_{E=0}^{d-1} 2^{-E} \binom{E+d-1}{d-1}$$

$$= 2^{-d}.2^{d-1} = 1/2 \ . \square$$

In that case we can also see $\epsilon'_i = \gamma'_i + (1 - \delta'_i) = \gamma_i(1 - \delta_i)$ as the number of `0`s at the end of each block:

$$t = \texttt{1--10...1--10...1--10} \ ,$$

$$a = \underbrace{\texttt{?10-0}}_{\epsilon'_1} \ldots \underbrace{\texttt{?10-0}}_{\epsilon'_i} \ldots \underbrace{\texttt{?10-0}}_{\epsilon'_d} \ ,$$

and directly compute $P(\epsilon'_i = e_i) = 2^{-e_i - 1}$. □

Using Corollary 2.8, we prove the conjecture in the following case:

Corollary 3.15. *Let t verify the two following constraints:*

$$\forall i, \alpha_i = 1 \text{ and } \min_i(\beta_i) \geq w(t) - 1 = d - 1 \ ,$$

then $|S_{t,k}| \leq 2^{k-1}$.

We conjecture that the converse of Theorem 3.14 is also true, i.e. those numbers are the only ones reaching the bound of the original conjecture.

Conjecture 3.16. $S_{t,k} = 2^{k-1}$ iff t verifies the two following constraints:

$$\forall i, \beta_i = 1 \text{ and } \min_i(\alpha_i) \geq k - w(t) - 1 = d - 1 \ .$$

4 Toward a Complete Proof

The numbers for which $P_{t,k}$ is the nearest to the bound of the conjecture seem to be the ones which verify the constraint $\min(\alpha_i) \geq k - w(t) - 1$, and especially the ones which also verify $\forall i$, $\beta_i = 1$. Moreover puncturing a `1` of a binary string seems to make $P_{t,k}$ smaller most of the time.

We consequently hope to be able to completely solve the conjecture using one of the following strategies:

- Show that any number gives a smaller set than an *extremal* one by induction (i.e. by puncturing `1`s, even so that different blocks merge) and by comparing different expressions of $P_{t,k}$.
- Show that the conjecture is true for every number which verifies the constraint $\min(\alpha_i) \geq k - w(t) - 1$ and then that the numbers which do not, give smaller sets by induction (i.e. by puncturing `1`s, but without merging different blocks) and by comparing different expressions of $P_{t,k}$.

References

1. Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345–359. Springer, Heidelberg (2003)
2. Courtois, N.: Fast algebraic attacks on stream ciphers with linear feedback. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 176–194. Springer, Heidelberg (2003)
3. Carlet, C., Feng, K.: An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 425–440. Springer, Heidelberg (2008)
4. Tu, Z., Deng, Y.: A conjecture on binary string and its applications on constructing boolean functions of optimal algebraic immunity. Cryptology ePrint Archive, Report 2009/272 (2009), http://eprint.iacr.org/

5. Dillon, J.: Elementary Hadamard Difference Sets. PhD thesis, University of Maryland (1974)
6. Carlet, C.: On a weakness of the Tu-Deng function and its repair. Cryptology ePrint Archive, Report 2009/606 (2009), http://eprint.iacr.org/
7. Flori, J.P., Randriambololona, H., Cohen, G., Mesnager, S.: On a conjecture about binary strings distribution. Cryptology ePrint Archive, Report 2010/170 (2010), http://eprint.iacr.org/
8. Monagan, M.B., Geddes, K.O., Heal, K.M., Labahn, G., Vorkoetter, S.M., McCarron, J., DeMarco, P.: Maple 10 Programming Guide. Maplesoft, Waterloo ON, Canada (2005)

Nega–Hadamard Transform, Bent and Negabent Functions

Pantelimon Stănică[1], Sugata Gangopadhyay[2], Ankita Chaturvedi[2], Aditi Kar Gangopadhyay[2], and Subhamoy Maitra[3]

[1] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA
pstanica@nps.edu

[2] Department of Mathematics, Indian Institute of Technology Roorkee Roorkee 247667 India
{gsugata,ankitac17,ganguli.aditi}@gmail.com

[3] Applied Statistics Unit, Indian Statistical Institute, 203 B. T. Road, Calcutta 700 108, India
subho@isical.ac.in

Abstract. In this paper we start developing a detailed theory of nega–Hadamard transforms. Consequently, we derive several results on negabentness of concatenations, and partially-symmetric functions. We also obtain a characterization of bent–negabent functions in a subclass of Maiorana–McFarland set. As a by-product of our results we obtain simple proofs of several existing facts.

Keywords: Boolean functions, nega–Hadamard transforms, bent and negabent functions.

1 Introduction

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and let $\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function on n variables. The reader is referred to Section 1.1 for all the basic notations and definitions related to Boolean functions.

Boolean functions received a lot of attention in the field of coding theory, sequences and cryptology. The most important method of analyzing the Boolean functions is by exploiting a certain kind of discrete Fourier transform, which is known, in Boolean function literature, as Walsh, Hadamard, or Walsh–Hadamard transform [4]. The maximum nonlinearity of a Boolean function is achieved when the maximum absolute value in the Walsh spectrum is minimized. For even n, such functions are well known as bent functions and the magnitudes of all the values in Walsh spectrum are the same. From the perspective of coding theory, these functions attain the covering radius of first order Reed–Muller code. Towards a nega–periodic analogue of the bent criteria, one can use nega–Hadamard transform and investigate Boolean functions with nega flat spectrum. This motivated several works in the area of Boolean functions [11,13,14,19] in the last few years.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 359–372, 2010.

In this paper we concentrate on the nega–Hadamard transform in more details. In particular, we have the following broad contributions.

- We present a detailed study of some of the properties of nega–Hadamard transform in Section 2. We obtain several results analogous to Hadamard transformation.
- Based on the previous analysis, we obtain several results with respect to the decomposition of negabent functions in Section 3.
- In Section 4, we study negabent functions that are symmetric with respect to two variables. Our study results simple proof of the main result in the paper [17] that all the symmetric negabent functions must be affine.
- A characterization of some bent–negabent functions in Maiorana–McFarland class is obtained in Section 5, thus complementing some results of [19].

1.1 Definitions and Notations

The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. Any element $\mathbf{x} \in \mathbb{F}_2^n$ can be written as an n-tuple $(x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$ for all $i = 1, \ldots, n$. The set of integers, real numbers and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ respectively. The addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ is denoted by '+'. The addition over $\mathbb{F}_2^n$ for all $n \geq 1$, is denoted by $\oplus$. If $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are two elements of $\mathbb{F}_2^n$, we define the scalar (or inner) product, respectively, the intersection by

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n, \mathbf{x} * \mathbf{y} = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

The cardinality of the set S is denoted by $|S|$. If $z = a + b\imath \in \mathbb{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, and $\overline{z} = a - b\imath$ denotes the complex conjugate of z, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$. Any $f \in \mathcal{B}_n$ can be expressed in *algebraic normal form* (ANF) as

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \left(\prod_{i=1}^{n} x_i^{a_i} \right), \ \mu_{\mathbf{a}} \in \mathbb{F}_2.$$

The (*Hamming*) *weight* of $\mathbf{x} \in \mathbb{F}_2^n$ is $wt(\mathbf{x}) := \sum_{i=1}^{n} x_i$. The algebraic degree of f, $\deg(f) := \max_{\mathbf{a}\in\mathbb{F}_2^n}\{wt(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0\}$. Boolean functions having algebraic degree at most 1 are said to be *affine functions*. For any two functions $f, g \in \mathcal{B}_n$, we define the (*Hamming*) *distance* $d(f, g) = |\{\mathbf{x} : f(\mathbf{x}) \neq g(\mathbf{x}), \mathbf{x} \in \mathbb{F}_{2^n}\}|$.

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at any point $\mathbf{u} \in \mathbb{F}_2^n$ is defined by

$$\mathcal{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}.$$

A function $f \in \mathcal{B}_n$ is a *bent function* if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\lambda \in \mathbb{F}_2^n$. Bent functions (defined by Rothaus [15] more than thirty years ago) hold an interest among researchers in this area since they have maximum Hamming distance

from the set of all affine Boolean functions. Several classes of bent functions were constructed by Rothaus [15], Dillon [6], Dobbertin [7], and later by Carlet [1].

The sum $\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}$ is the *crosscorrelation* of f and g at z. The *autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$. It is known [4] that a function $f \in \mathcal{B}_n$ is bent if and only if $\mathcal{C}_f(\mathbf{u}) = 0$ for all $\mathbf{u} \neq 0$.

For a detailed study of Boolean functions we refer to Carlet [2,3], and Cusick and Stănică [4].

The *nega–Hadamard transform* of $f \in \mathbb{F}_2^n$ at any vector $\mathbf{u} \in \mathbb{F}_2^n$ is the complex valued function:

$$\mathcal{N}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\imath^{wt(\mathbf{x})}.$$

A function is said to be *negabent* if the nega–Hadamard transform is flat in absolute value, namely $|\mathcal{N}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$. The sum

$$C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}}$$

is the *nega–crosscorrelation* of f and g at z. We define the *nega–autocorrelation* of f at $\mathbf{u} \in \mathbb{F}_2^n$ by

$$C_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{u})}(-1)^{\mathbf{x}\cdot\mathbf{u}}.$$

The negaperiodic autocorrelation defined by Parker and Pott [11,12] is as follows

$$n_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{u})}(-1)^{wt(\mathbf{u})}(-1)^{\mathbf{x}\cdot\mathbf{u}}.$$

It is to be noted that the difference between the above two definitions is not critical and both the defintions can be used.

As we will be referring later, we also present the definition of a symmetric Boolean function. A Boolean function is said to be symmetric if inputs of the same weight produce the same output, that is, $f(\mathbf{x}) = f(\sigma(\mathbf{x}))$, for any permutation σ.

2 Properties of Nega–Hadamard transform

It is a well known fact that if $f \in \mathcal{B}_n$, then the Walsh–Hadamard transform $\mathcal{H}_f(\lambda)$ is invertible, and so,

$$(-1)^{f(\mathbf{x})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{H}_f(\mathbf{u})(-1)^{\mathbf{x}\cdot\mathbf{u}}, \tag{1}$$

for all $\mathbf{x} \in \mathbb{F}_2^n$. The nega–Hadamard transform is also a unitary transformation. An immediate consequence of the definition of nega–Hadamard transformation of a function $f \in \mathcal{B}_n$ in [11,14] is the following:

Lemma 1. *Suppose $f \in \mathcal{B}_n$. Then*

$$(-1)^{f(\mathbf{y})} = 2^{-\frac{n}{2}}\, \imath^{-wt(\mathbf{y})} \sum_{u \in \mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})(-1)^{\mathbf{y}\cdot\mathbf{u}}, \tag{2}$$

for all $\mathbf{y} \in \mathbb{F}_2^n$.

Next, we prove a theorem that gives the nega–Hadamard transform of various combinations of Boolean functions. We shall use throughout the well-known identity (see [10])

$$wt(\mathbf{x} \oplus \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} * \mathbf{y}). \tag{3}$$

Theorem 1. *Let f, g, h be in $\mathcal{B}_n$. The following statements are true:*

(*a*) $\mathcal{N}_{\mathbf{0}}(\mathbf{u}) = -\mathcal{N}_{\mathbf{1}}(\mathbf{u}) = \omega^n\, \imath^{-wt(\mathbf{u})}$, *and* $\mathcal{N}_{h\oplus 1}(\mathbf{u}) = -\mathcal{N}_h(\mathbf{u})$, $\mathbf{u} \in \mathbb{F}_2^n$, *where* $\mathbf{0}, \mathbf{1}$ *are the constant* 0, *respectively,* 1 *functions; and,* ω *is an* 8*-th primitive root of* 1, *namely* $\omega = (1+\imath)/\sqrt{2}$. *In general, for any affine function* $\ell_{\mathbf{a},c}(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x} \oplus c$, *we have* $\mathcal{N}_{\ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c\, \omega^n\, \imath^{-wt(\mathbf{a}\oplus\mathbf{u})}$.

(*b*) *If* $h(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x})$ *on* $\mathbb{F}_2^n$, *then for* $\mathbf{u} \in \mathbb{F}_2^n$,

$$\mathcal{N}_h(\mathbf{u}) = 2^{-n/2} \sum_{\mathbf{v}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{v})\mathcal{H}_g(\mathbf{u}\oplus\mathbf{v}) = 2^{-n/2} \sum_{v\in\mathbb{F}_2^n} \mathcal{H}_f(\mathbf{v})\mathcal{N}_g(\mathbf{u}\oplus\mathbf{v}).$$

(*c*) *If* $\ell_{\mathbf{a},c}(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x} \oplus c$ *is affine, then* $\mathcal{N}_{f\oplus\ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c \mathcal{N}_f(\mathbf{a}\oplus\mathbf{u})$.

(*d*) *If* $h(\mathbf{x}) = f(A\mathbf{x}\oplus\mathbf{a})$, *then* $\mathcal{N}_h(\mathbf{u}) = (-1)^{\mathbf{a}\cdot(A\mathbf{u})}\, \imath^{wt(\mathbf{a})}\, \mathcal{N}_f(A\mathbf{u}\oplus\mathbf{a})$, *where* A *is an* $n\times n$ *orthogonal matrix over* $\mathbb{F}_2$ *(and so,* $A^TA = I_n$*).*

(*e*) *If* $h(\mathbf{x},\mathbf{y}) = f(\mathbf{x}) \oplus g(\mathbf{y}), \mathbf{x},\mathbf{y} \in \mathbb{F}_2^n$, *then* $\mathcal{N}_{f\oplus g}(\mathbf{u},\mathbf{v}) = \mathcal{N}_f(\mathbf{u})\mathcal{N}_g(\mathbf{v})$.

(*f*) *If* $f \in \mathcal{B}_n, g \in \mathcal{B}_k$, *and* $h(\mathbf{x},\mathbf{y}) = f(\mathbf{x})g(\mathbf{y})$, *then*

$$2^{k/2}\mathcal{N}_h(\mathbf{u},\mathbf{v}) = \mathcal{N}_f(\mathbf{u})A_{g1}(\mathbf{v}) + \omega^n\, \imath^{-wt(\mathbf{u})} A_{g0}(\mathbf{v}),$$
$$A_{g1}(\mathbf{v}) + A_{g0}(\mathbf{v}) = 2^{k/2}\omega^k \imath^{-wt(\mathbf{v})},$$

where $A_{g0}(\mathbf{v}) = \sum_{\mathbf{y},g(\mathbf{y})=0}(-1)^{\mathbf{y}\cdot\mathbf{v}}\, \imath^{wt(\mathbf{y})}$, $A_{g1}(\mathbf{v}) = \sum_{\mathbf{y},g(\mathbf{y})=1}(-1)^{\mathbf{y}\cdot\mathbf{v}}\, \imath^{wt(\mathbf{y})}$. *Moreover, if* $k = 1$,

$$2^{1/2}\mathcal{N}_{yf(\mathbf{x})}(\mathbf{u},v) = (-1)^v\, \imath\mathcal{N}_f(\mathbf{u}) + \omega^n\, \imath^{-wt(\mathbf{u})}$$
$$2^{1/2}\mathcal{N}_{(y\oplus 1)f(\mathbf{x})}(\mathbf{u},v) = \mathcal{N}_f(\mathbf{u}) + \omega^n(-1)^v\, \imath^{-wt(\mathbf{u})+1}.$$

Proof. Claim (*a*) follows from Lemma 1 of [19], since $\mathcal{N}_{\mathbf{0}}(\mathbf{u}) = -\mathcal{N}_{\mathbf{1}}(\mathbf{u}) = 2^{-n/2}\sum_{\mathbf{y}}(-1)^{\mathbf{u}\cdot\mathbf{y}}\, \imath^{wt(\mathbf{y})} = \omega^n\, \imath^{-wt(\mathbf{u})}$. We now show the first identity of (*b*) (the second is absolutely similar). Since

$$\mathcal{N}_f(\mathbf{v}) = 2^{-n/2} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{v}}\, \imath^{wt(\mathbf{y})}$$
$$\mathcal{H}_g(\mathbf{u}\oplus\mathbf{v}) = 2^{-n/2} \sum_{\mathbf{z}\in\mathbb{F}_2^n} (-1)^{g(\mathbf{z})\oplus\mathbf{z}\cdot(\mathbf{u}\oplus\mathbf{v})}$$

and (see [4, p. 8])

$$\sum_{\mathbf{x}}(-1)^{\mathbf{v}\cdot\mathbf{x}} = \begin{cases} 2^n & \text{if } \mathbf{v}=\mathbf{0} \\ 0 & \text{if } \mathbf{v}\neq\mathbf{0}, \end{cases}$$

we obtain (all sums are over $\mathbb{F}_2^n$)

$$\begin{aligned}\sum_{\mathbf{v}\in\mathbb{F}_2^n}\mathcal{N}_f(\mathbf{v})\mathcal{H}_g(\mathbf{u}\oplus\mathbf{v}) &= 2^{-n}\sum_{\mathbf{v},\mathbf{y},\mathbf{z}}(-1)^{f(\mathbf{y})\oplus g(\mathbf{z})+\mathbf{v}\cdot(\mathbf{y}\oplus\mathbf{z})\oplus\mathbf{u}\cdot\mathbf{z}}\imath^{wt(\mathbf{y})} \\ &= 2^{-n}\sum_{\mathbf{y},\mathbf{z}}(-1)^{f(\mathbf{y})\oplus g(\mathbf{z})\oplus\mathbf{u}\cdot\mathbf{z}}\imath^{wt(\mathbf{y})}\sum_{\mathbf{v}}(-1)^{\mathbf{v}\cdot(\mathbf{y}\oplus\mathbf{z})} \\ &= \sum_{\mathbf{y}}(-1)^{f(\mathbf{y})\oplus g(\mathbf{y})\oplus\mathbf{u}\cdot\mathbf{y}}\imath^{wt(\mathbf{y})} = 2^{n/2}\mathcal{N}_{f\oplus g}(\mathbf{u}).\end{aligned}$$

Further, (c) follows from (b), since

$$\begin{aligned}\mathcal{H}_{\ell_{\mathbf{a},c}}(\mathbf{w}) &= 2^{-n/2}\sum_{\mathbf{y}}(-1)^{\mathbf{a}\cdot\mathbf{y}\oplus\mathbf{w}\cdot\mathbf{y}\oplus c} \\ &= 2^{-n/2}(-1)^c\sum_{\mathbf{y}}(-1)^{(\mathbf{a}\oplus\mathbf{w})\cdot\mathbf{y}} \\ &= \begin{cases}(-1)^c 2^{n/2} & \text{if } \mathbf{a}=\mathbf{w} \\ 0 & \text{if } \mathbf{a}\neq\mathbf{w}.\end{cases}\end{aligned}$$

The property (d) can be derived from [11, Lemma 2] and [19, Theorem 2]. It is to be noted that [19, Theorem 2] further proves that the action of orthogonal group preserves bent–negabentness property of a Boolean function. Item (e) is straightforward. To show item (f), we write

$$\begin{aligned}2^{(n+k)/2}\mathcal{N}_h(\mathbf{u},\mathbf{v}) &= \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{F}_2^{n+k}}(-1)^{f(\mathbf{x})g(\mathbf{y})\oplus\mathbf{x}\cdot\mathbf{u}\oplus\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{x})+wt(\mathbf{y})} \\ &= \sum_{\mathbf{y},g(\mathbf{y})=1}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})}\sum_{\mathbf{x}}(-1)^{f(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}}\imath^{wt(\mathbf{x})} \\ &\quad+\sum_{\mathbf{y},g(\mathbf{y})=0}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})}\sum_{\mathbf{x}}(-1)^{\mathbf{x}\cdot u}\imath^{wt(\mathbf{x})} \\ &= 2^{n/2}\mathcal{N}_f(\mathbf{u})\sum_{\mathbf{y},g(\mathbf{y})=1}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})} \\ &\quad+2^{n/2}\omega^n\imath^{-wt(\mathbf{u})}\sum_{\mathbf{y},g(\mathbf{y})=0}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})},\end{aligned}$$

from which we obtain the desired identity. Moreover, if $k=1$, and $g(y)=y$, then $A_{g0}(v)=1, A_{g1}(v)=(-1)^v\imath$, and if $g(y)=y\oplus 1$, then $A_{g1}(v)=1, A_{g0}(v)=(-1)^v\imath$, and so

$$\begin{aligned}2^{1/2}\mathcal{N}_{yf(\mathbf{x})}(\mathbf{u},v) &= (-1)^v\imath\mathcal{N}_f(\mathbf{u})+\omega^n\imath^{-wt(\mathbf{u})} \\ 2^{1/2}\mathcal{N}_{(y\oplus 1)f(\mathbf{x})}(\mathbf{u},v) &= \mathcal{N}_f(\mathbf{u})+\omega^n(-1)^v\imath^{-wt(\mathbf{u})+1}.\end{aligned}$$

The proof of the theorem is done. □

The next result is analogous to the result on the crosscorrelation of two Boolean functions [16]. In the nega–Hadamard transform context, the basic idea of this result is explained in [5] and equation (15) of [13]. In Lemma 2 we are able to use Hadamard transform because unlike the definition in [5,13] our nega–crosscorrelation does not include the factor $(-1)^{wt(\mathbf{u})}$.

Lemma 2. *If $f, g \in \mathcal{B}_n$, then the nega–crosscorrelation*

$$C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}} = \imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}}.$$

Proof. The sum

$$\begin{aligned}\imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}} &= 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{y})}\, \imath^{wt(\mathbf{x})-wt(\mathbf{y})+wt(\mathbf{z})} \\ &\quad \times \sum_{\mathbf{u}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z})} \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}}.\end{aligned}$$

□

If we consider the case $f = g$ in the previous lemma, then we obtain

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}} &= \imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_f(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}} \\ &= \imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{N}_f(\mathbf{u})|^2(-1)^{\mathbf{u}\cdot\mathbf{z}}.\end{aligned} \tag{4}$$

This is an analogue of autocorrelation of Boolean functions. It is to be noted that since both Hadamard and nega–Hadamard transforms are unitary they are energy preserving and hence, Parseval's theorem holds for both the transformations. The classical Parseval's identity takes the form

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} (\mathcal{H}_f(\mathbf{u}))^2 = 2^n$$

for Walsh–Hadamard transform. Substituting $\mathbf{z} = \mathbf{0}$ in the equation (4), we obtain a proof of this fact for the particular case of nega–Hadamard transforms.

Corollary 1 (*nega–Parseval's identity*). *We have*

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{N}_f(\mathbf{u})|^2 = 2^n. \tag{5}$$

Lemma 3. *A Boolean function $f \in \mathcal{B}_n$ is negabent if and only if, $C_f(\mathbf{z}) = 0$ for all $\mathbf{z} \in \mathbb{F}_2^n \setminus \{0\}$.*

Proof. If f is a negabent function then $|\mathcal{N}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$. For all $\mathbf{z} \neq \mathbf{0}$, then by (4) we obtain $C_f(\mathbf{z}) = 0$. The converse also follows from the equation (4). □

An equivalent result is proved after equation (15) in [13], and in [11, Theorem 2] for the negaperiodic autocorrelation.

Remark 1. Lemma 3 provides an alternative characterization of negabent functions.

If f is an affine function, then for all $\mathbf{z} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ the nega–autocorrelation $C_f(\mathbf{z}) = 0$. This implies that any affine function is negabent. For alternative proofs we refer to [19, Lemma 1] and [11, Proposition 1].

3 Decomposition of Negabent Functions with Respect to Co-dimension One Subspaces

Suppose $1 \leq r \leq n$. Then any function $f \in \mathcal{B}_n$ can be thought of as a function from $\mathbb{F}_2^r \times \mathbb{F}_2^{n-r}$ into $\mathbb{F}_2$. For any fixed $\mathbf{v} \in \mathbb{F}_2^r$, the function $f_\mathbf{v} \in \mathcal{B}_{n-r}$ is defined as $f_\mathbf{v}(\mathbf{x}) = f(\mathbf{v}, \mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_2^{n-r}$.

Theorem 2. *Let $f \in \mathcal{B}_n$ expressed as $f : \mathbb{F}_2^r \times \mathbb{F}_2^{n-r} \to \mathbb{F}_2$. Then*

$$C_f(\mathbf{u}, \mathbf{w}) = \sum_{\mathbf{v} \in \mathbb{F}_2^r} C_{f_\mathbf{v}, f_{\mathbf{v}\oplus\mathbf{u}}}(\mathbf{w})(-1)^{\mathbf{v}\cdot\mathbf{u}}.$$

Proof. By definition

$$\begin{aligned} C_f(\mathbf{u}, \mathbf{w}) &= \sum_{\mathbf{v} \in \mathbb{F}_2^r} \sum_{\mathbf{z} \in \mathbb{F}_2^{n-r}} (-1)^{f(\mathbf{v},\mathbf{z}) \oplus f(\mathbf{v}\oplus\mathbf{u}, \mathbf{z}\oplus\mathbf{w})} (-1)^{\mathbf{v}\cdot\mathbf{u} \oplus \mathbf{z}\cdot\mathbf{w}} \\ &= \sum_{\mathbf{v} \in \mathbb{F}_2^r} (-1)^{\mathbf{v}\cdot\mathbf{u}} \sum_{\mathbf{z} \in \mathbb{F}_2^{n-r}} (-1)^{f_\mathbf{v}(\mathbf{z}) \oplus f_{\mathbf{v}\oplus\mathbf{u}}(\mathbf{z}\oplus\mathbf{w})} (-1)^{\mathbf{z}\cdot\mathbf{w}} \qquad (6) \\ &= \sum_{\mathbf{v} \in \mathbb{F}_2^r} C_{f_\mathbf{v}, f_{\mathbf{v}\oplus\mathbf{u}}}(\mathbf{w})(-1)^{\mathbf{v}\cdot\mathbf{u}}. \end{aligned}$$

□

Corollary 2. *Suppose $f \in \mathcal{B}_n$ is expressed as*

$$f(\mathbf{x}, y) = f_0(\mathbf{x})(1 \oplus y) \oplus f_1(\mathbf{x})y, \text{ for all } (\mathbf{x}, y) \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2,$$

where $f_0, f_1 \in \mathcal{B}_{n-1}$. Then

$$\begin{aligned} C_f(\mathbf{w}, 0) &= C_{f_0}(\mathbf{w}) + C_{f_1}(\mathbf{w}) \\ C_f(\mathbf{w}, 1) &= C_{f_0, f_1}(\mathbf{w}) - (-1)^{wt(\mathbf{w})} C_{f_0, f_1}(\mathbf{w}). \end{aligned}$$

The functions f and g are said to have *complementary nega–autocorrelation* if for all nonzero $\mathbf{u} \in \mathbb{F}_2^n$

$$C_f(\mathbf{u}) + C_g(\mathbf{u}) = 0.$$

The following lemma establishes a connection between the nega–autocorrelations of f, g and their nega–Hadamard transformations.

Lemma 4. *Two functions $f, g \in \mathcal{B}_n$ have complementary nega–autocorrelations if and only if*

$$|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2 \text{ for all } \mathbf{u} \in \mathbb{F}_2^n.$$

Proof. Let f, g be two functions with complementary nega–autocorrelations. Then

$$\begin{aligned} |\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 &= 2^{-n} \sum_{\mathbf{z} \in \mathbb{F}_2^n} \imath^{-wt(\mathbf{z})} (C_f(\mathbf{z}) + C_g(\mathbf{z}))(-1)^{\mathbf{z}\cdot\mathbf{u}} \\ &= 2^{-n} 2^{n+1} = 2. \end{aligned}$$

Conversely, suppose $|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{F}_2^n$. Then

$$\begin{aligned} C_f(\mathbf{z}) + C_g(\mathbf{z}) &= \imath^{wt(\mathbf{z})} \sum_{\mathbf{u} \in \mathbb{F}_2^n} (|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2)(-1)^{\mathbf{u}\cdot\mathbf{z}} \\ &= 2\imath^{wt(\mathbf{z})} \sum_{\mathbf{u} \in \mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{z}} \\ &= 2^{n+1} \imath^{wt(\mathbf{z})} \delta_0(\mathbf{z}), \end{aligned}$$

where

$$\delta_0(\mathbf{z}) = \begin{cases} 0 & \text{if } \mathbf{z} \neq \mathbf{0}; \\ 1 & \text{if } \mathbf{z} = \mathbf{0}. \end{cases} \tag{7}$$

Thus the functions f and g have complementary nega–autocorrelations. □

Theorem 3. *Suppose $h \in \mathcal{B}_{n+1}$ is expressed as*

$$h(\mathbf{x}, y) = f(\mathbf{x})(1 \oplus y) \oplus g(\mathbf{x})y, \text{ for all } (\mathbf{x}, y) \in \mathbb{F}_2^n \times \mathbb{F}_2,$$

where $f, g \in \mathcal{B}_n$. Then the following statements are equivalent:

(1) *h is negabent.*
(2) *f and g have complementary nega–autocorrelations and $C_{f_0,f_1}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ with $wt(\mathbf{u}) \equiv 1 \pmod 2$.*
(3) *$|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{F}_2^n$ and $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}$ is a real number whenever $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$.*

Proof. We show first (1) $\iff$ (2). Suppose h is a negabent function. Then $C_h(\mathbf{u}, a) = 0$ for all nonzero $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$. From Corollary 2 we obtain

$$C_h(\mathbf{u}, 0) = C_f(\mathbf{u}) + C_g(\mathbf{u}) = 0,$$

for all $\mathbf{u} \in \mathbb{F}_2^n \setminus \{0\}$ and

$$C_h(\mathbf{u}, 1) = C_{f,g}(\mathbf{u})(1 - (-1)^{wt(\mathbf{u})}) = 0,$$

which implies $C_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ with $wt(\mathbf{u}) \equiv 1 \pmod 2$.

Conversely, let us assume that the functions f and g have complementary nega–autocorrelations and $C_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ with $wt(\mathbf{u}) \equiv 1 \pmod 2$. Then by Corollary 2, $C_h(\mathbf{u}, a) = 0$ for all nonzero $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$. This implies that h is a negabent function.

We now show (1) $\iff$ (3). The nega–Hadamard transform of h at $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$ is

$$\begin{aligned}\mathcal{N}_h(\mathbf{u}, a) &= 2^{-\frac{n+1}{2}} \sum_{(\mathbf{x},y)\in\mathbb{F}_2^n\times\mathbb{F}_2} (-1)^{h(\mathbf{x},y)\oplus\mathbf{u}\cdot\mathbf{x}\oplus ay}\, \imath^{wt(\mathbf{x},y)} \\ &= 2^{-\frac{n+1}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\, \imath^{wt(\mathbf{x})} + 2^{-\frac{n+1}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{g(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}\oplus a}\, \imath^{wt(\mathbf{x})+1} \\ &= \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \imath\,(-1)^a \frac{1}{\sqrt{2}}\mathcal{N}_g(\mathbf{u}).\end{aligned}$$

Thus,

$$\mathcal{N}_h(\mathbf{u}, a) = \begin{cases} \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u}) & \text{if } a = 0; \\ \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) - \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u}) & \text{if } a = 1. \end{cases} \tag{8}$$

Since h is negabent $|\mathcal{N}_h(\mathbf{u}, a)| = 1$ for all $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$ we obtain

$$\begin{aligned}\left|\frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u})\right| &= 1, \\ \left|\frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) - \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u})\right| &= 1.\end{aligned} \tag{9}$$

If h is negabent, then by Lemma 4 and the equivalence of the first two statements proved above we obtain:

$$|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2 \text{ for all } \mathbf{u} \in \mathbb{F}_2^n.$$

Suppose for $\mathbf{u} \in \mathbb{F}_2^n$, $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$. Let $z_1 = \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u})$ and $z_2 = \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u})$. Then by equation (9) we obtain

$$\begin{gathered}|z_1 + z_2|^2 = |z_1 - z_2|^2, \text{ that is} \\ z_1\overline{z_2} = -z_2\overline{z_1}\end{gathered}$$

Therefore we have $\mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})} = \mathcal{N}_g(\mathbf{u})\overline{\mathcal{N}_f(\mathbf{u})}$, i.e., $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})} = \overline{\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}} = \overline{\left(\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}\right)}$. This proves that $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}$ is a real number.

Conversely, suppose $|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{F}_2^n$ and $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}$ is a real number whenever $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$.

Without loss of generality, we may first assume $\mathcal{N}_f(\mathbf{u}) = 0$, for some $\mathbf{u} \in \mathbb{F}_2^n$. Then by the above condition $|\mathcal{N}_g(\mathbf{u})| = \sqrt{2}$. By equation (8), $|\mathcal{N}_h(\mathbf{u}, a)| = 1$ for

all $a \in \mathbb{F}_2$. Next we consider the case when $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$. Let $\phi(\mathbf{u}) = \frac{\mathcal{N}_g(\mathbf{u})}{\mathcal{N}_f(\mathbf{u})}$. Then

$$\begin{aligned}
|\mathcal{N}_h(\mathbf{u},a)|^2 &= |\frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \imath(-1)^a\frac{1}{\sqrt{2}}\phi(\mathbf{u})\mathcal{N}_f(\mathbf{u})|^2 \\
&= \frac{1}{2}|\mathcal{N}_f(\mathbf{u})|^2|1+\imath(-1)^a\phi(\mathbf{u})|^2 \\
&= \frac{1}{2}|\mathcal{N}_f(\mathbf{u})|^2(1+|\phi(\mathbf{u})|^2) \qquad (10)\\
&= \frac{1}{2}|\mathcal{N}_f(\mathbf{u})|^2\left(1+\frac{|\mathcal{N}_g(\mathbf{u})|^2}{|\mathcal{N}_f(\mathbf{u})|^2}\right) \\
&= \frac{1}{2}(|\mathcal{N}_f(\mathbf{u})|^2+|\mathcal{N}_g(\mathbf{u})|^2) = 1.
\end{aligned}$$

Thus h is negabent. □

4 Negabent Functions Symmetric about Two Variables

Suppose $h \in \mathcal{B}_n$ is a Boolean function which is symmetric with respect to two variables, y and z say. Then there exist functions $f, g, s \in \mathcal{B}_{n-2}$ such that

$$h(\mathbf{x},y,z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) \oplus s(\mathbf{x})yz \qquad (11)$$

for all $(\mathbf{x},y,z) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. The Boolean function h is bent if and only if, f and g are bent and $s(\mathbf{x}) = 1$ for all $\mathbf{x} \in \mathbb{F}_2^{n-2}$ (see [2,3,4,20]). For negabent functions we prove the following similar result.

Theorem 4. *Suppose $h \in \mathcal{B}_n$ is expressed as $h(\mathbf{x},y,z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) \oplus s(\mathbf{x})yz$ for all $(\mathbf{x},y,z) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. The Boolean function h is negabent if and only if f and g are negabent and $s(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^n$.*

Proof. The nega–autocorrelation of h at $(0,1,1)$ is

$$\begin{aligned}
C_h(\mathbf{0},1,1) &= \sum_{\mathbf{x}\in\mathbb{F}_2^{n-2}}\sum_{y\in\mathbb{F}_2}\sum_{z\in\mathbb{F}_2}(-1)^{s(\mathbf{x})(1\oplus y\oplus z)}(-1)^{y\oplus z} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^{n-2}}(-1)^{s(\mathbf{x})}\sum_{y\in\mathbb{F}_2}(-1)^{s(\mathbf{x})y\oplus y}\sum_{z\in\mathbb{F}_2}(-1)^{s(\mathbf{x})z\oplus z} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^{n-2}}(-1)^{s(\mathbf{x})}\sum_{y\in\mathbb{F}_2}(-1)^{s(\mathbf{x})y\oplus y}(1+(-1)^{s(\mathbf{x})\oplus 1}) \\
&= 2\sum_{\mathbf{x}\in\mathbb{F}_2^{n-2},s(\mathbf{x})=1}(-1)\sum_{y\in\mathbb{F}_2}(-1)^{2y} = 4\sum_{\mathbf{x}\in\mathbb{F}_2^{n-2},s(\mathbf{x})=1}(-1) \\
&= -4|\{\mathbf{x}\in\mathbb{F}_2^{n-2} : s(\mathbf{x})=1\}|.
\end{aligned}$$

If h is a negabent function then $C_h(\mathbf{0}, 1, 1) = 0$. Therefore $|\{\mathbf{x} \in \mathbb{F}_2^{n-2} : s(\mathbf{x}) = 1\}| = 0$, which implies that $s(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^{n-2}$. Thus, if h is a negabent function and symmetric with respect to the variables y and z, then it can be expressed as

$h(\mathbf{x}, y, z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z)$, for all $(\mathbf{x}, y, z) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. The nega–Hadamard transform $\mathcal{N}_h(\mathbf{u}, a, b)$ of h at $(\mathbf{u}, a, b) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$ is

$$2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^{n-2}} \sum_{y \in \mathbb{F}_2} \sum_{z \in \mathbb{F}_2} (-1)^{f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) + \mathbf{u} \cdot \mathbf{x} \oplus ay \oplus bz} \imath^{wt(\mathbf{x}, y, z)}.$$

Expanding the above sum by substituting all possible values of $(y, z) \in \mathbb{F}_2 \times \mathbb{F}_2$ we obtain

$$\mathcal{N}_h(\mathbf{u}, a, b) = \frac{1 - (-1)^{a \oplus b}}{2} \mathcal{N}_f(\mathbf{u}) + \imath \frac{(-1)^a + (-1)^b}{2} \mathcal{N}_g(\mathbf{u}). \tag{12}$$

Therefore $\mathcal{N}_h(\mathbf{u}, a, b) \in \{\mathcal{N}_f(\mathbf{u}), \pm \imath \mathcal{N}_g(\mathbf{u})\}$ for all $(\mathbf{u}, a, b) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. This proves that both f and g are negabent. On the other hand if f and g are negabent functions then h is also negabent. This shows the converse. □

Corollary 3. *A symmetric negabent function is affine.*

Proof. Let $h \in \mathcal{B}_n$ be a symmetric negabent function. Let us suppose that h has algebraic degree greater than or equal to 2. Since h is symmetric, it is symmetric with respect to any two variables. Therefore, it is possible to express h, for at least one pair y, z of variables, as follows

$$h(\mathbf{x}, y, z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) \oplus s(\mathbf{x})yz,$$

where $s(\mathbf{x}) \neq 0$ for at least one $\mathbf{x} \in \mathbb{F}_2^{n-2}$. But this contradicts the fact that h is negabent. Hence all symmetric negabent functions are affine. □

The result of Corollary 3 gives an alternate proof of the fact proved in [17]. In fact, the case for even n can be immediately obtained following the result of Parker and Pott [11], which gives a connection between bent and negabent functions.

Theorem 5 ([11, Thm. 12]). *A function $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ is negabent if and only if $f \oplus s_2$ is bent, where $s_2(x_1, x_2, \ldots, x_{2m}) = \sum_{i<j} x_i x_j$ is the elementary symmetric function of degree 2.*

We note that s_2 is actually a homogeneous (that is, all terms of its ANF are of the same degree), symmetric and quadratic bent function.

Let $s_1(x_1, x_2, \ldots, x_{2m}) = \sum_i x_i$, the (only) symmetric linear function involving all the variables. In [18] it is shown that the only symmetric bent functions are s_2, $s_2 \oplus s_1$, $1 \oplus s_2$, $1 \oplus s_2 \oplus s_1$.

In [17], it is proved (by a long argument) that all the symmetric negabent functions are affine. Following [18,11], the result of [17] can be achieved in a few lines for even n.

Theorem 6. *Let n be even. A symmetric function $f \in \mathcal{B}_n$ is negabent if and only if it is affine.*

Proof. Suppose $f \in \mathcal{B}_n$ is a symmetric negabent function. Then $f \oplus s_2$ is a bent function. Since the direct sum of two symmetric functions is symmetric, then $f \oplus s_2$ is a symmetric bent function. The only symmetric bent functions are s_2, $s_2 \oplus s_1$, $1 \oplus s_2$, $1 \oplus s_2 \oplus s_1$ (see [18]). Therefore f can be 0, 1, s_1, $1 \oplus s_1$ and nothing else. This proves that if f is a symmetric negabent function on even number of variables then it is affine.

Conversely, it is known that all affine functions are negabent [19]. Therefore, symmetric functions on even number of variables, if affine, are negabent. □

Bent functions do not exist for odd number of input variables. Thus there is no equivalent characterization of Theorem 5 for odd dimension, and the result of [17] cannot be proved trivially as before. However, the odd (as well as the even) case has already been taken care of by Corollary 3.

5 Bent–Negabent Functions in Maiorana–McFarland Class

In this section we shall investigate bent functions which are also negabent in the Maiorana-McFarland (MM) class of bent functions, namely

$$f(\mathbf{x}, \mathbf{y}) = \pi(\mathbf{x}) \cdot \mathbf{y} \oplus g(\mathbf{x}), \ \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n \tag{13}$$

where π is a permutation satisfying $wt(\mathbf{x} \oplus \mathbf{y}) = wt(\pi(\mathbf{x}) \oplus \pi(\mathbf{y}))$ (we call π a *weight-sum invariant* permutation), for all $\mathbf{x}, \mathbf{y}$, and g is an arbitrary Boolean function, both on $\mathbb{F}_2^n$. We remark that if π is orthogonal, that is, $\pi(\mathbf{x}) = A \cdot \mathbf{x}$ with A orthogonal ($A^T A = I_n$), then it satisfies the imposed condition (since $wt(\pi(\mathbf{x}) \oplus \pi(\mathbf{y})) = wt(A(\mathbf{x} \oplus \mathbf{y}))$, it suffices to show that $wt(A\mathbf{z}) = wt(\mathbf{z})$; for that, consider $wt(A\mathbf{z}) = (A\mathbf{z})^T \cdot (A\mathbf{z}) = \mathbf{z}^T (A^T A)\mathbf{z} = wt(\mathbf{z})$). It could be interesting to see if there are such weight-sum invariant permutations outside of the linear orthogonal group generated ones.

Theorem 7. *A function as in (13) on $\mathbb{F}_2^{2n}$ is bent–negabent if and only if g is bent.*

Proof. We evaluate

$$\begin{aligned}
\mathcal{N}_f(\mathbf{u}, \mathbf{v}) &= 2^{-n} \sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{F}_2^{2n}} (-1)^{\pi(\mathbf{x}) \cdot \mathbf{y} \oplus g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u} \oplus \mathbf{y} \cdot \mathbf{v}} \imath^{wt(\mathbf{x}) + wt(\mathbf{y})} \\
&= 2^{-n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \imath^{wt(\mathbf{x})} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{\pi(\mathbf{x}) \cdot \mathbf{y} \oplus \mathbf{y} \cdot \mathbf{v}} \imath^{wt(\mathbf{y})} \\
&= 2^{-n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \imath^{wt(\mathbf{x})} 2^{n/2} \omega^n \imath^{-wt(\pi(\mathbf{x}) \oplus \mathbf{v})} \\
&= 2^{-n/2} \omega^n \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \imath^{wt(\mathbf{x}) - wt(\pi(\mathbf{x}) \oplus \mathbf{v})}.
\end{aligned}$$

Now, using the fact that π is a weight-sum invariant permutation, and by (3), we obtain

$$\begin{aligned}
&wt(\pi(\mathbf{x}) \oplus \mathbf{v}) = wt(\mathbf{x} \oplus \pi^{-1}(\mathbf{v})),\\
&wt(\mathbf{x}) - wt(\pi(\mathbf{x}) \oplus \mathbf{v}) = -wt(\pi^{-1}(\mathbf{v})) + 2wt(\mathbf{x} * \pi^{-1}(\mathbf{v})), \text{ and}\\
&\imath^{2wt(\mathbf{x}*\pi^{-1}(\mathbf{v}))} = (-1)^{\mathbf{x}\cdot\pi^{-1}(\mathbf{v})},
\end{aligned}$$

which implies that

$$\begin{aligned}
\mathcal{N}_f(\mathbf{u},\mathbf{v}) &= 2^{-n/2}\omega^n\, \imath^{-wt(\pi^{-1}(\mathbf{v}))} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{g(\mathbf{x})\oplus\mathbf{x}\cdot(\mathbf{u}\oplus\pi^{-1}(\mathbf{v}))}\\
&= \omega^n\, \imath^{-wt(\pi^{-1}(\mathbf{v}))}\mathcal{H}_g(\mathbf{u}\oplus\pi^{-1}(\mathbf{v})).
\end{aligned}$$

Consequently,

$$|\mathcal{N}_f(\mathbf{u},\mathbf{v})| = |\mathcal{H}_g(\mathbf{u}\oplus\pi^{-1}(\mathbf{v}))|,$$

which implies our claim. □

The following corollary follows easily from our theorem, since bent functions exist for any degree up to half of the (even) dimension. We remark that Theorem 10 of [11] gives an upper bound of $n-1$ on the degree of a bent–negabent function, but not an existence result.

Corollary 4. *If f as in (13) is bent–negabent with π weight-sum invariant, then the degree of f is bounded by $n/2$. Moreover, there exist bent–negabent functions in the MM class of any degree between 2 and $n/2$.*

Acknowledgements. The authors are thankful to the anonymous reviewers whose comments have improved the technical as well as the editorial quality of the paper. Ankita Chaturvedi thanks the University Grants Commission of India for supporting her research.

References

1. Carlet, C.: Two new classes of bent functions. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 77–101. Springer, Heidelberg (1994)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P. (eds.) Boolean Methods and Models. Cambridge Univ. Press, Cambridge, http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html
3. Carlet, C.: Vectorial Boolean functions for cryptography. In: Crama, Y., Hammer, P. (eds.) Boolean Methods and Models. Cambridge Univ. Press, Cambridge, http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html
4. Cusick, T.W., Stănică, P.: Cryptographic Boolean functions and Applications. Elsevier/Academic Press (2009)
5. Danielsen, L.E., Gulliver, T.A., Parker, M.G.: Aperiodic Propagation Criteria for Boolean Functions. Inform. Comput. 204(5), 741–770 (2006)

6. Dillon, J.F.: Elementary Hadamard difference sets. In: Proceedings of Sixth S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, pp. 237–249 (1975)
7. Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 61–74. Springer, Heidelberg (1995)
8. Dobbertin, H., Leander, G.: Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions. Des. Codes Cryptography 49, 3–22 (2008)
9. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1983)
10. MacWilliams, F.J., Sloane, N.J.A.: The theory of error–correcting codes. North-Holland, Amsterdam (1977)
11. Parker, M.G., Pott, A.: On Boolean functions which are bent and negabent. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.-Y. (eds.) SSC 2007. LNCS, vol. 4893, pp. 9–23. Springer, Heidelberg (2007)
12. Parker, M.G., Pott, A.: Personal Communications
13. Riera, C., Parker, M.G.: One and two-variable interlace polynomials: A spectral interpretation. In: Ytrehus, Ø. (ed.) WCC 2005. LNCS, vol. 3969, pp. 397–411. Springer, Heidelberg (2006)
14. Riera, C., Parker, M.G.: Generalized bent criteria for Boolean functions. IEEE Trans. Inform. Theory 52(9), 4142–4159 (2006)
15. Rothaus, O.S.: On bent functions. Journal of Combinatorial Theory Series A 20, 300–305 (1976)
16. Sarkar, P., Maitra, S.: Cross–Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes. Theory Comput. Systems 35, 39–57 (2002)
17. Sarkar, S.: On the symmetric negabent Boolean functions. In: Roy, B., Sendrier, N. (eds.) INDOCRYPT 2009. LNCS, vol. 5922, pp. 136–143. Springer, Heidelberg (2009)
18. Savicky, P.: On the bent Boolean functions that are symmetric. European J. Comb. 15, 407–410 (1994)
19. Schmidt, K.U., Parker, M.G., Pott, A.: Negabent functions in the Maiorana–McFarland class. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 390–402. Springer, Heidelberg (2008)
20. Zhao, Y., Li, H.: On bent functions with some symmetric properties. Discrete Appl. Math. 154, 2537–2543 (2006)

Synchronization of Boolean Dynamical Systems: A Spectral Characterization

Jérémy Parriaux[1], Philippe Guillot[2], and Gilles Millérioux[1]

[1] Nancy University, CNRS,
Research Center for Automatic Control of Nancy (CRAN UMR 7039), France
jeremy.parriaux@esstin.uhp-nancy.fr,
gilles.millerioux@esstin.uhp-nancy.fr
[2] Université Paris 8,
Laboratoire Analyse, Géométrie et Applications (LAGA UMR 7539), France
philippe.guillot@univ-paris8.fr

Abstract. In this paper a spectral characterization of the synchronization property of Boolean dynamical systems is provided. Conditions on the spectrum of the next-state function are derived for two systems coupled in a unidirectional way - also called master-slave configuration - to guarantee self-synchronization. Two kinds of self-synchronization are discussed: the statistical one and the finite one. Next, some conditions are stated for a specific input sequence to allow the system to be self-synchronizing. Some of the results are based on the notion of influence of variables, a notion that is extended to vectorial Boolean functions for the purpose of the paper. A potential application to cryptography is finally given.

1 Introduction

Dynamical systems are commonly used to model natural or engineering based processes. We can distinguish two kinds of systems. The continuous ones, $\mathbb{R}$ valued and discrete ones, finite-set valued. The latter can be either an approximation of a continuous system or can be intrinsically discrete. Let us stress that the terminology *continuous* or *discrete* refers to the state variables of the system regardless the time which can be continuous or discrete. Among a wide variety of discrete dynamical systems, the class of Boolean Dynamical Systems (BDS for short) is of special interest. In this paper, we focus on non-autonomous BDS, that is with input. The specificity of BDS lies in that the internal state, the input and the output are Boolean variables and therefore the transition and output functions are Boolean functions.

In this paper we deal with the issue of synchronization of BDS which is the process through which two systems are brought to the same state. Although several structural conditions to guarantee synchronization have been provided in the open literature, few works deal with BDS. Moreover, these studies address the synchronization issue in the time. In this paper we propose a spectral point of view. The interest of the spectral approach lies in that the composition of

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 373–386, 2010.

functions can be expressed in terms of product of matrices well suited for design purpose. Spectral characterization is also well appropriate in the perspective of ensuring special cryptographic properties when the dynamical systems under consideration are involved in a ciphering setup.

More precisely we investigate the problem of self-synchronization. By self-synchronization, it is intended a dynamical behavior which do no longer depend on the initial condition after a transient time. Besides the spectral characterization, the novelty of the study lies in that the problem is viewed through the notion of influence of variables. Roughly speaking, influence describes the ability of a subset of the input variables of a function to change its output. Here the set of variables under consideration is the initial condition of the dynamical system. For the purpose of the paper we also had to extend this notion to vectorial Boolean functions.

The layout is the following. In Section 2, we recall some background on Boolean functions and tools of spectral analysis in particular Walsh transform. Section 3 is devoted to the problem statement, namely the issue of self-synchronization between two dynamical systems coupled in a unidirectional way. Distinction between statistical and finite time self-synchronization is made. Section 4 deals with the Walsh transform of the iterated function of a dynamical system as a prerequisite for deriving the main result. In Section 5, the notion of self-synchronizing sequence is developed. The main result of the paper is stated in Section 6 wherein, based on the notion of influence, we derive conditions on the spectrum of the next-state function for a BDS to be self-synchronizing. Finally Section 7 is devoted to illustrative examples. An example potentially interesting for cryptographic applications involving the so called Self-Synchronizing Stream Ciphers (SSSC for short) is provided.

2 Preliminaries and Definitions

In this section, we recall the basics about spectral analysis of Boolean functions which is the main tool used in this paper. Let $\mathbb{F}_2$ denotes the two elements field. For any positive integer n, the n–dimensional vector space over $\mathbb{F}_2$ is denoted $\mathbb{F}_2^n$. A Boolean function f is a mapping $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. If f is a Boolean function, we denote by $\widehat{f}$ its Fourier transform, which is by definition the real valued mapping $\mathbb{F}_2^n \longrightarrow \mathbb{R}$ defined, for any n–dimensional binary vector u, by

$$\widehat{f}(u) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{x \cdot u}, \tag{1}$$

where $x \cdot u = x_1 u_1 + \cdots + x_n u_n$. This transform is invertible and the inverse is given by:

$$\widehat{\widehat{f}} = 2^n f \tag{2}$$

Let us recall the Parseval's theorem (see [1]):

Theorem 1 (Parseval's theorem). *For any Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, and any vector $u \in \mathbb{F}_2^n$, the following relation holds:*

$$\sum_{u \in \mathbb{F}_2^n} \widehat{f^2}(u) = 2^n \sum_{x \in \mathbb{F}_2^n} f^2(x). \tag{3}$$

When dealing with Boolean functions, we rather resort to the Walsh transform which gets nicer properties in most cases. The Walsh transform of a Boolean function f is simply the Fourier transform of its sign function f_χ where $f_\chi = (-1)^{f(x)} = 1 - 2f(x)$ that is,

$$\widehat{f_\chi}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x \cdot u} \tag{4}$$

As shown in [1], the correspondence between the Fourier and the Walsh transforms is given by

$$\forall u \in \mathbb{F}_2^n, \quad \widehat{f_\chi}(u) = 2^n \delta_0(u) - 2\widehat{f}(u), \tag{5}$$

where $\delta_0(u)$ is the Kronecker symbol, equals 1 if u is the n–dimensional zero vector, and equals 0 elsewhere.

An (n, m) vectorial Boolean function, or simply an (n, m)–function, is a function over the vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Any of the output components defines a Boolean function. Therefore, an (n, m)–function f is nothing but a m–dimensional vector where each component is a n–variable Boolean function. The j^{th} coordinate is denoted by f_j. The Walsh matrix of any (n, m)–function is the $2^m \times 2^n$ dimensional matrix $W_f = \left(w^f_{u,v}\right)$ so that (see [2]):

$$\forall u \in \mathbb{F}_2^m,\ \forall v \in \mathbb{F}_2^n,\ w^f_{u,v} = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot f(x)+v \cdot x} \tag{6}$$

In other words, the rows indexed by $u \in \mathbb{F}_2^m$ of this matrix are the Walsh transforms of the linear combination of the functions f_i defined by $x \longmapsto u \cdot f(x)$. The coefficients of the Walsh matrix of a function is called the spectrum of the function.

N.B. Matrices indexes may be without ambiguity either an integer or a binary vector representing the same integer in natural binary coding. Thus, if u and v are vectors of same dimension, we may write $u < v$. It means that the number represented by u is smaller than the one represented by v.

An interesting property relates the Walsh matrices of composed functions.

Proposition 1 (see [2]). *If f is an (n, m)–function and g is an (p, n)–function then*

$$W_{f \circ g} = \frac{1}{2^n} W_f \times W_g. \tag{7}$$

3 Problem Statement

Let us consider a compound system involving two BDS coupled in a unidirectional way, a setup called master-slave configuration. The system obeys the following equations

$$\begin{cases} x_{k+1} = F(x_k, u_k) \\ y_k \quad\;\; = G(x_k, u_k) \end{cases} \qquad \text{(Master equation)} \tag{8}$$

$$\begin{cases} \widehat{x}_{k+1} = f(\widehat{x}_k, y_k) \\ \widehat{u}_k \quad\;\; = g(\widehat{x}_k, y_k) \end{cases} \qquad \text{(Slave equation)} \tag{9}$$

where x_k and $\widehat{x}_k$ are n dimensional vectors. The subscript k stands for the discrete time. The $(n+1, n)$–functions F and f are called the next-state functions. The $(n+1, 1)$–functions G and g are called the output functions. The input and output of (8) (respectively (9)) are u_k and y_k (respectively y_k and $\widehat{u}_k$). The situation is depicted in Figure 1. We are interested in self-synchronization. Before proceeding further, let us introduce some formal definitions.

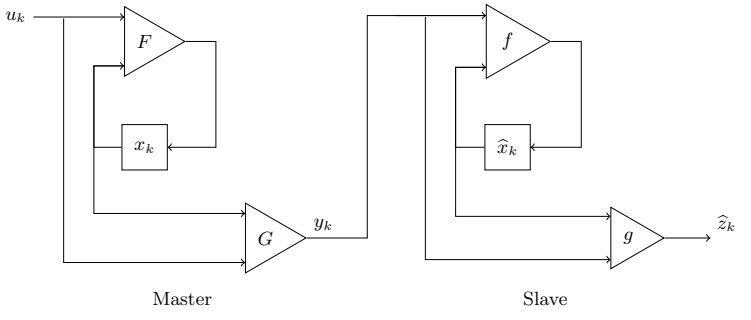


Fig. 1. Overall system

Definition 1 (Synchronizing sequence). *A sequence* (u) *is synchronizing for* (8)–(9) *if there exists an integer* k_u *so that for all initial states* x_0 *and* $\widehat{x}_0$*:*

$$\forall k \geq k_u,\ x_k = \widehat{x}_k \tag{10}$$

Remark 1. This definition can be generalized by adding a constant delay r so that (10) turns into $\forall k \geq k_u,\ x_k = \widehat{x}_{k+r}$.

Definition 2 (Finite time synchronization). *The overall system* (8)–(9) *is finite time synchronizing if the minimum value* k_u *is upper bounded when* u *stands in the set of all input sequences. The upper bound is called the synchronization delay.*

Remark 2. If (u) is a random sequence then, (u) turns into (U) and k_u turns into K_U which is a random variable.

Definition 3 (Statistical synchronization). *A system is statistically synchronizing if* $\lim_{k\to+\infty} \mathrm{Prob}(K_U \leq k) = 1$.

In the sequel, we will focus on the slave system. The synchronizing properties of this subsystem are entirely defined by those of the $(n+1, n)$–function f. Therefore, the previous definitions may be transposed as follow:

Definition 4 (Self-Synchronizing sequence). *A sequence* (y) *is self-synchronizing for* f *if there exists an integer* k_y *so that for all initial state* x_0 *and* $\widehat{x}_0$

$$\forall k \geq k_y,\ x_k = \widehat{x}_k \tag{11}$$

Definition 5 (Finite time self-synchronization). *The function* f *is finite time self-synchronizing if the minimum value* k_y *is upper bounded when* y *stands in the set of all input sequences. The upper bound is called the self-synchronization delay of* f.

Definition 6 (Statistical self-synchronization). *A function* f *is statistically self-synchronizing if* $\lim_{k\to+\infty} \mathrm{Prob}(K_Y \leq k) = 1$, *where* K_Y *is the random synchronization delay for the random sequence* (Y).

For our purpose, we must define, for any positive integer i, the iterated function ϕ_i that expresses the internal state after $i+1$ iterations by means of the initial internal state and the input sequence. More precisely, for the sequence $(y) = (y_0, \ldots, y_i) \in \mathbb{F}_2^{i+1}$ and $x \in \mathbb{F}_2^n$, the value $\phi_i(y, x)$ is:

$$\phi_i(y, x) = f(y_i, f(y_{i-1}, f(\ldots, f(y_0, x)\cdots))) \tag{12}$$

This function plays a central role in the sequel.

4 Walsh Transform of the Iterated Function

In this section, the Walsh spectrum of the iterated function ϕ_i is expressed by means of the spectrum of the next-state function f. We then observe the consequences on the synchronization properties of f.

Let us denote by f^0 (respectively f^1) the (n, n)–function which is the restriction of f to the input bit $y = 0$ (respectively to $y = 1$). For a given fixed input sequence $y = (y_0, \ldots, y_i)$, we denote by ϕ_i^y the (n, n)–function that expresses the internal state after $i+1$ iterations: $\phi_i^y : x \longmapsto \phi_i(y, x)$. We express the spectrum of the function ϕ_i^y.

Proposition 2. *The Walsh matrix of* ϕ_i^y *is*

$$W_{\phi_i^y} = \frac{1}{2^{n+i}} W_{f^{y_i}} W_{f^{y^{i-1}}} \times \cdots \times W_{f^{y_0}}. \tag{13}$$

Proof. The proof is a direct consequence of Proposition 1. □

For two vectors $u = (u_0, \ldots, u_i)$ and $v = (v_0, \ldots, v_{n-1})$, their concatenation, denoted $u|v$ is by definition the $(n+i+1)$–dimensional vector

$$u|v = (u_0, \ldots, u_i, v_0, \ldots, v_{n-1}).$$

Proposition 3. *Let* $v,\ t \in \mathbb{F}_2^n,\ u \in \mathbb{F}_2^{u+1},\ z = u|v$ *and* $\left(w_{t,v}^{\phi_i^y}\right) = W_{\phi_i^y}$. *The entries of the Walsh matrix of the iterated function* ϕ_i *are defined by*

$$w_{t,z}^{\phi_i} = w_{t,u|v}^{\phi_i} = \sum_{y \in \mathbb{F}_2^{i+1}} (-1)^{u \cdot y} w_{t,v}^{\phi_i^y} \tag{14}$$

Proof. By definition of the Walsh coefficients,

$$\begin{aligned} w_{t,z}^{\phi_i} = w_{t,u|v}^{\phi_i} &= \textstyle\sum_{x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^{i+1}} (-1)^{t \cdot \phi_i(y,x) + (u|v) \cdot (y|x)} \\ &= \textstyle\sum_{y \in \mathbb{F}_2^{i+1}} \sum_{x \in \mathbb{F}_2^n} (-1)^{t \cdot \phi_i(y,x) + u \cdot y + v \cdot x} \qquad = \sum_{y \in \mathbb{F}_2^{i+1}} (-1)^{u \cdot y} w_{t,v}^{\phi_i^y} \end{aligned}$$

□

According to (13), the Walsh matrix of ϕ_i can be expressed as sums and differences of the Walsh matrices $W_{\phi_i^y}$ obtained for all the possible sequences (y) of length $i+1$. Therefore, we get the expression of the spectrum of ϕ_i as a function of the spectrum of f.

5 Self-synchronizing Sequences

In this section we are interested in characterizing the sequences (y) that self-synchronize the function based on the spectrum of the function ϕ_i^y.

Proposition 4. *The Walsh matrix of the iterated function is*

$$W_{\phi_i^y} = \begin{pmatrix} 2^n & 0 \cdots & 0 \\ \pm 2^n & 0 \cdots & 0 \\ \vdots & \vdots & \vdots \\ \pm 2^n & 0 \cdots & 0 \end{pmatrix} \tag{15}$$

if and only if (y) *is a self-synchronizing sequence for this function.*

Proof. By definition, if (y) is a self-synchronizing sequence $\phi_i^y(x)$ does not depend on x thus, ϕ_i^y is a constant function. The converse can be derived by applying (2) to the rows of the above matrix (which are the Walsh transforms of the linear combinations of the component functions f_j. □

The matrix $W_{\phi_i^y}$ can easily be worked out with (13).

Remark 3. If (y) is a self-synchronizing sequence for the function f then, any other sequence that contains (y) as a subsequence is also self-synchronizing for f.

Proposition 5. *If f has at least one self-synchronizing sequence then f is statistically self-synchronizing.*

Proof. A self-synchronizing sequence has a finite length, therefore, its probability of occurrence is one in a sequence whose length tends to infinity. □

These results can be used to check in the spectral domain whether a given sequence is self-synchronizing or not. But more importantly it gives some conditions on the Walsh spectrum of the function that can be used to build self-synchronizing systems that have the form (9).

6 Influence of Variables

Roughly speaking, influence reveals the ability of a variable to change the output of a function. Let us stress that the notion of variable influence has been used in several papers (e.g. [3], [4], [5] to mention a few). For reasons explained later on, we must revisit the existing formal definitions of such a notion because they are not suited for our purpose.

6.1 Influence of a Single Variable

Let f be a boolean function of the variable x. The influence of one variable x_i over a Boolean function f is defined as the probability that the value of $f(x)$ changes if the value of the component x_i is changed, the other components being set randomly. This definition may be expressed in an equivalent way.

Definition 7. *Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ be a Boolean function and $i \in \{1, \ldots, n\}$ a set of integers. Let e_i be the n–dimensional vector whose components are zero except the i^{th} one which equals 1. The influence of x_i on f is:*

$$I_f(i) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} \left[f(x) + f(x + e_i) \right]$$

Remark 4. This is related to the so called auto-correlation function of f which is $r_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+u)}$ that is, $I_f(i) = 2^{n-1} + \frac{1}{2} r_f(e_i)$.

6.2 Influence of a Set of Variables

There exists several ways to extend Definition 7. None is more natural than the others. The choice of the right definition depends on what need to be studied. The influence of a subset[1] S of components of x can be defined as the probability that the value of $f(x)$ changes if one of the variables in S changes too. It does not take into account the number of possibilities of choosing the values of the variables that change the output of the function. A more suitable definition for our purpose

[1] Note that a variable may be identified to its index. Thus for short S may be also considered as a set of indexes in $\{1, \ldots, n\}$.

should involve the balancedness of the restricted function obtained by fixing the variables not in the set S. Next, the expression of the influence of a set containing more than one element is a complex function of its spectral representation and is therefore not suitable for the proposed approach. We therefore rather introduce a new definition of the influence that takes these points into account. The support of a vector u is by definition: $\mathrm{supp}(u) = \{i \in \{1, \ldots, n\} \mid u_i \neq 0\}$.

Definition 8. *Let $f(x)$ be a Boolean function of n variables, S be a set of k components of x. The influence $I_f(S)$ is:*

$$I_f(S) = \frac{1}{2^n(2^k-1)} \sum_{x \in \mathbb{F}_2^n} \sum_{u \in \mathbb{F}_2^n | u \neq 0,\ \mathrm{supp}(u) \subset S} [f(x) + f(x+u)] \tag{16}$$

In other words, the influence of a set of variables is the mean of the probabilities that $f(x)$ changes when x is uniformly randomly chosen, the mean being computed for all possible changes of the value of the variables in S.

Remark 5. When the set S contains one element, then Definitions 7 and 8 are equivalent.

6.3 Spectral Expression of the Influence

The influence of a set of variables over a Boolean function f can simply be expressed by means of its spectral representation.

Proposition 6. *Let $f(x)$ be a Boolean function of n variables, S be a set of k components of x. The influence $I_f(S)$ is:*

$$I_f(S) = \frac{2^{k-1}}{2^{2n}(2^k-1)} \sum_{v \in \mathbb{F}_2^n | \ \mathrm{supp}(v) \cap S \neq \emptyset} \widehat{f_\chi}^2(v) \tag{17}$$

Proof. For any vector u, let $f^u : x \longmapsto f(x) - f(x+u)$. It is easy to see that $f^u(x) = 0$ if $f(x) = f(x+u)$ and $f^u(x) = \pm 1$ if $f(x) \neq f(x+u)$. This implies that $[f^u(x)]^2 = f(x) + f(x+u)$. Therefore, by using (3),

$$I_f(S) = \frac{1}{2^{2n}(2^k-1)} \sum_{v \in \mathbb{F}_2^n} \sum_{u \in \mathbb{F}_2^n | u \neq 0,\ \mathrm{supp}(u) \subset S} \left[\widehat{f^u}(v)\right]^2. \tag{18}$$

By expressing $\widehat{f^u}(v)$ by means of $\widehat{f}(v)$, we get

$$\widehat{f^u}(v) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{v \cdot x}(1 - (-1)^{v \cdot u}) = (1 - (-1)^{v \cdot u})\widehat{f}(v),$$

By using this expression of $\widehat{f^u}(v)$ in (18), we get

$$I_f(S) = \frac{1}{2^{2n}(2^k-1)} \sum_{v \in \mathbb{F}_2^n} \widehat{f}^2(v) \sum_{u \in \mathbb{F}_2^n | u \neq 0,\ \mathrm{supp}(u) \subset S} [1 - (-1)^{v \cdot u}]^2,$$

and thus:

$$I_f(S) = \frac{1}{2^{2n-2}(2^k-1)} \sum_{v/\,\mathrm{supp}(v)\cap S\neq\emptyset} \widehat{f}^2(v),$$

and finally using (5) the desired result stands. □

Remark 6. This definition of the influence of variables is very close, up to a factor that depends on the cardinality of S, to the definition of the so called *variable variation* given in [4].

Proposition 7. *Let f be a Boolean function.*

1. *f is bent if and only if for all non-empty subset S of variable indexes, one has $I_f(S) = \frac{1}{2}$,*
2. *f does not depend on the variables in the subset S if and only if $I_f(S) = 0$.*

Proof. 1. *If f is bent, then $\forall u \in \mathbb{F}_2^n$, $\widehat{f_\chi}(u) = \pm 2^{n/2}$. Then replacing this expression in (17), we get*

$$I_f(S) = \frac{2^{k-1}\times 2^n}{2^{2n}(2^k-1)} \sum_{v/\,\mathrm{supp}(v)\cap S\neq\emptyset} 1 = \frac{2^{k-1}\times 2^n}{2^{2n}(2^k-1)}(2^n - 2^{n-k}) = \frac{1}{2}$$

Conversely, if for all non-empty subset of variable indexes S of k elements, one has $I_f(S) = 1/2$, then, by replacing in relation (17), one gets

$$\frac{2^{k-1}}{2^{2n}(2^k-1)} \sum_{v|\,\mathrm{supp}(v)\cap S\neq\emptyset} \widehat{f_\chi}^2(v) = \frac{1}{2}.$$

By Parseval's Theorem, and as $\mathrm{supp}(v)\cap S = \emptyset \iff \mathrm{supp}(v) \subset \overline{S}$, where $\overline{S}$ denotes the complementary set of S,

$$2^{2n} - \sum_{v|\,\mathrm{supp}(v)\subset\overline{S}} \widehat{f_\chi}^2(v) = 2^{2n-k}(2^k-1),$$

Thus:

$$\sum_{v|\,\mathrm{supp}(v)\subset\overline{S}} \widehat{f_\chi}^2(v) = 2^{2n} - 2^{2n-k}(2^k-1) = 2^{2n-k} \tag{19}$$

When applying this relation with $S = \{1,\ldots,n\}$, the sum (19) has only one term which is $\widehat{f_\chi}(0)^2 = 2^{2n-n} = 2^n$. The other values are obtained by induction on the weight of vector u. Let v be a non-zero vector. Let us choose S such that $\overline{S} = \mathrm{supp}(u)$. One can split the sum of relation (19) into the term $\widehat{f_\chi}^2(v)$ and the $2^{n-k}-1$ others terms which all equal 2^n by the induction hypothesis as they all have weight strictly lower than the weight of v. Thus, $\widehat{f_\chi}^2(u) + (2^{n-k}-1)\cdot 2^n = 2^{2n-k}$ and the result holds.

2. *If f is constant with respect to the variables in S, $\forall x, \forall v \in \mathrm{supp}(S)$, $f(x) + f(x+v) = 0$ thus, $I_f(S) = 0$. Conversely, $I_f(S) = 0$ implies that for all v the terms $f(x)+f(x+v)$ equal 0 since $I_f(S)$ is a sum of positive terms.* □

6.4 Extension of the Influence to Vectorial Boolean Functions

In this section, we extend the definition of the influence to vectorial Boolean functions in order to characterize the self-synchronization property of f.

Definition 9. *The influence of a set of variables S over a vectorial Boolean function f is the mean of the influence of S over each coordinate function f_j.*

$$I_f(S) = \frac{1}{q}\sum_{j=1}^{q} I_{f_j}(S) \tag{20}$$

Proposition 8. *If f does not depend on the variables in S then, the influence is $I_f(S) = 0$.*

Proof. This is a simple consequence of Proposition 7. □

6.5 Self-synchronization vs. Influence

We aim at relating the self-synchronization property of the function f stated in Definition 5 and 6 to the influence of the initial state on the corresponding iterated function ϕ_i. Let S_x denote the subset of variables that corresponds to the initial state x.

Proposition 9. *The function f is finite time self-synchronizing if and only if, there exists an integer i large enough so that for any finite sequence (y) of length $i+1$, the iterated function $\phi_i(y,x)$ does not depend on the internal state component x. In other words, the variable x of $\phi_i(y,x)$ has no longer influence after a transient time that is, $I_{\phi_i}(S_x) = 0$*

Proposition 10. *The function f is statistically self-synchronizing if and only if, there exists an integer i large enough so that for at least one sequence (y) of length $i+1$, the iterated function $\phi_i(y,x)$ does not depend on the internal state component x. In other words, there is at least one input sequence (y) so that the variable x of $\phi_i^y(x)$ has no influence over ϕ_i^y thus, $I_{\phi_i^y}(S_x) = 0$.*

It can be inferred from (14) that this implies for W_{ϕ_i} to be sparse. The only possible non-zero coefficients are located on the column v so that $\mathrm{supp}(v) \cap S = \emptyset$.

7 Examples

7.1 Academic Example

We now show how to use the previous results to build a $(n+1, n)$–function f that is statistically self-synchronizing. Let $f : \mathbb{F}_2 \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$, and f^0 (respectively f^1) the restriction of f to $y = 0$ (respectively $y = 1$). A statistically self-synchronizing function f can be obtained by selecting the appropriate functions f^0 and f^1 so that there exists an admissible way to multiply the corresponding

Walsh matrices W_{f^0} and W_{f^1} (or their powers) yielding (15). From this perspective, we can consider a lower triangular matrix with zeros on the diagonal except the entry located at row 0 and column 0. Such a matrix has the interesting property that the successive right multiplications with any other matrix tends to produce a matrix of form (15). Therefore we can select f^0 such that its Walsh matrix has the aforementioned structure, f^1 being any vectorial Boolean function. Note that this choice is arbitrary and the role of f^0 and f^1 can be reversed.

Let us provide a constructive approach to find out a suitable (n,n)–function f^0. First, let us recall that the u^{th} row of W_{f^0} is the Walsh transform of the Boolean function defined by $x \longmapsto u \cdot f^0(x)$. That is, the u^{th} row is the Walsh transform of the linear combination of the coordinate functions f_j^0 such that the components u_j equal 1. Let e_j be the canonical vector whose components are 0 except the j^{th} one which equals 1. Considering the rows $u = e_j$ for $j \in \{1,\ldots,n\}$ is equivalent to select each coordinate function f_j^0. Thus, the other rows can be obtained by calculating the Walsh transform of the linear combinations of the functions f_j^0. Interestingly, the functions that depend only on the first k variables have zeros after the first 2^k coefficients.

Proposition 11. *Let f be a n–variable Boolean function. The function f depends only on the first j^{th} variables ($j \leq n$) if and only if*

$$\forall u,\ \mathrm{supp}(u) \notin \{1,\ldots,j\},\ \widehat{f_\chi}(u) = 0$$

Proof. Let us express the Walsh transform of a n–variable function f that indeed depends only on the first j^{th} variables. It can be expressed, for $u \in \mathbb{F}_2^j$ and $v \in \mathbb{F}_2^{n-j}$, as

$$\widehat{f_\chi}(u|v) = \sum_{y \in \mathbb{F}_2^{n-j}} (-1)^{v\cdot y} \sum_{x \in \mathbb{F}_2^j} (-1)^{f(x|0)+u\cdot x}.$$

This implies that $\widehat{f_\chi}(u|v) = 0$ if $v \neq 0$, which proves that Conversely, for $x \in \mathbb{F}_2^j$ and $y \in \mathbb{F}_2^{n-j}$, one has $f_\chi(x|y) = \frac{1}{2^n}\widehat{\widehat{f_\chi}}(x|y) = \frac{1}{2^n}\sum_{u,v}\widehat{f_\chi}(u|v)(-1)^{x\cdot u+v\cdot y}$. As it is assumed that, for $v \neq 0$, one has $\widehat{f_\chi}(u|v) = 0$, we deduce $f(x|y) = \frac{1}{2^n}\sum_u \widehat{f_\chi}(u|0)(-1)^{u\cdot x}$. It is clear that this expression does not depend on y and the result holds. □

This proposition implies that if the coordinate functions f_j^0 are chosen so that it depends only on the first $j-1$ variables then, W_{f^0} is of the form (15). This is true since the rows $u < e_j$ are Walsh transforms of linear combinations of functions that depend on the first $j-1$ variables. Note that the function f_0^0 has to be constant, its value is therefore either 0 or 1.

We propose to construct a $(3,3)$–function f^0 so that its Walsh matrix has the desire structure of an upper triangular matrix. According to the aforementioned considerations, a function f^0 which fulfills the required constraints can be

$$f^0 = \begin{cases} f_0^0 = 0 \\ f_1^0 = x_0 \\ f_2^0 = x_1 + x_0x_1 \end{cases} \tag{21}$$

Its Walsh transform is

$$W_{f^0} = \begin{pmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & -4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & -4 & 4 & 4 & 0 & 0 & 0 & 0 \\ -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ -4 & 4 & 4 & 4 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{22}$$

As pointed out before, there are no particular restriction on the function f^1. The sole lower triangular structure of W_{f^0} suffices to guarantee that any sequence that contains three 0s self-synchronizes the system.

This is one approach to build self-synchronizing functions. But as it can be seen the lower triangular structure of W_{f^0} implies a very specific structure to f^0. It would now be interesting to find out other constructions that release the constraint on f^0.

7.2 Application to Self-synchronizing Stream Ciphers

In this section, we are interested in the self-synchronizing property for cryptographic purposes and more exactly for the design of a so called Self-Synchronizing Stream Cipher (SSSC for short). The reader may refer to [6], [7] for examples of SSSC proposed through the eSTREAM European project devoted to stream ciphers. At the transmitter side, the canonical equations governing an SSSC read

$$\begin{cases} x_k = \varphi_\ell(y_k, \ldots, y_{k-\ell}) \\ z_k = h(x_k, y_k) \\ y_k = z_k + u_k \end{cases} \tag{23}$$

and at the receiver side, the equations read

$$\begin{cases} \widehat{x}_k = \varphi_\ell(y_k, \ldots, y_{k-\ell}) \\ \widehat{z}_k = g(\widehat{x}_k, y_k) \\ \widehat{u}_k = \widehat{z}_k + y_k \end{cases} \tag{24}$$

The sequences (z) and $(\widehat{z})$ are the respective key-streams, x_k and $\widehat{x}_k$ are the respective internal states. The ciphering is performed by the exclusive-OR between the key-stream and the plain-text while the deciphering is performed by the exclusive-OR between the key-stream and the cipher-text. Let us note that (23) and (8) can not directly be identified. It is clear that proper decryption is achieved whenever $\widehat{z}_k = z_k$. Actually, since φ_ℓ depends at both ends on the same arguments, such a condition is always fulfilled. It is nothing but a synchronization condition.

We propose to resort to the dynamical system (9) for delivering the key-stream instead of a static function like φ_ℓ. The objective of resorting to a recursive approach is to get a more complex ciphering function with a same computational

cost. However not all dynamical systems are admissible. Indeed, in (9), f must have the self-synchronization property. Assuming that (9) is finite time self-synchronizing, the state vector $\widehat{x}_k$ must have to be precisely expressed as a function φ_ℓ that does not depend on $\widehat{x}_{k-\ell}$. It must read

$$\begin{cases} \widehat{x}_k = \phi_\ell(y_k, \ldots, y_{k-\ell}, \widehat{x}_{k-\ell}) = \varphi_\ell(y_k, \ldots, y_{k-\ell}) \\ \widehat{z}_k = g(\widehat{x}_k, y_k) \end{cases}, \tag{25}$$

where ϕ_ℓ is the iterated function. It has been stressed in [8] and [9] that this is related to the flatness property borrowed from control theory.

If f has the statistical self-synchronization property, it means that ℓ is not bounded and this may increase the complexity of the next-state function f causing the diffusion/confusion properties of the cipher to increase. Besides, if ℓ is not bounded, the canonical representation cannot be obtained in an explicit way. That prevents from any practical implementation. We illustrate the statistical self-synchronizing property. Let us turn back to the example of Section 7.1. It has been pointed out that f^1 can be arbitrary. We define for example f^1 as

$$f^1 = \begin{cases} f_0^1 = x_0x_1 + x_1x_2 + x_0x_1x_2 \\ f_1^1 = x_0x_1 + x_2 \\ f_2^1 = x_1x_2 + x_0 \end{cases} \tag{26}$$

Consequently, the function f is defined as

$$f(y, x) = (y + 1)f^0(x) + yf^1(x) \tag{27}$$

Below is given the third iterated function ϕ_2.

$$\phi_2 = \begin{cases} (\phi_2)_0 = x_0x_2y_{k-2}y_{k-1}y_k + x_0x_1x_2y_{k-2}y_{k-1}y_k \\ (\phi_2)_1 = x_0x_1y_{k-2}y_{k-1} + x_0x_2y_{k-2}y_{k-1} + x_1x_2y_{k-2}y_{k-1} \\ \quad + x_0x_1x_2y_{k-2}y_{k-1} + x_0y_k + x_0y_{k-2}y_k + x_2y_{k-2}y_k \\ \quad + x_1x_2y_{k-2}y_k + x_0y_{k-1}y_k + x_0y_{k-2}y_{k-1}y_k + x_0x_1y_{k-2}y_{k-1}y_k \\ \quad + x_2y_{k-2}y_{k-1}y_k + x_0x_2y_{k-2}y_{k-1}y_k \\ (\phi_2)_2 = x_0x_1y_{k-2} + x_1x_2y_{k-2} + x_0x_1x_2y_{k-2} + x_1y_{k-1} + x_0x_1y_{k-1} \\ \quad + x_0y_{k-2}y_{k-1} + x_1y_{k-2}y_{k-1} + x_0x_1y_{k-2}y_{k-1} + x_0x_2y_{k-2}y_{k-1} \\ \quad + x_1x_2y_{k-2}y_{k-1} + x_0x_1y_{k-2}y_k + x_1x_2y_{k-2}y_k + x_0x_1x_2y_{k-2}y_k \\ \quad + x_1y_{k-1}y_k + x_0x_1y_{k-1}y_k + x_0y_{k-2}y_{k-1}y_k + x_1y_{k-2}y_{k-1}y_k \\ \quad + x_0x_2y_{k-2}y_{k-1}y_k \end{cases} \tag{28}$$

Such a simple example illustrates the relevance of resorting to a recursive approach. Indeed we can easily imagine the complexity of implementing the canonical form instead of the recursive equations when ℓ is large. Besides, as stressed above, when ℓ is not bounded, an explicit expression cannot be obtained.

8 Conclusion

In this paper a spectral characterization of the synchronization property of Boolean dynamical systems has been provided. Conditions on the spectrum of

the next-state function have been derived for two systems coupled in a unidirectional way to guarantee self-synchronization. Two kinds of self-synchronization have been considered: the statistical one and the finite one. Next some conditions have been stated for a specific input sequence to allow the system to be self-synchronizing. Some of the results have been based on the notion of influence of variables, a notion that have been extended to vectorial Boolean functions for the purpose of the paper. A potential application to cryptography has finally been given as an illustrative example. To obtain a complete cryptosystem setup, further work will investigate relevant classes of boolean functions as well as cryptanalysis aspect.

References

1. Boolean Functions for Cryptography and Error-Correcting Codes. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge Press (2010)
2. Vectorial Boolean Functions for Cryptography. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge Press (2010)
3. Kahn, J., Kalai, G., Linial, N.: The influence of variables on boolean functions. In: SFCS 1988: Proceedings of the 29th Annual Symposium on Foundations of Computer Science, Washington, DC, USA, pp. 68–80. IEEE Computer Society, Los Alamitos (1988)
4. Kindler, G., Safra, S.: Noise-resistant boolean-functions are juntas (2003), http://www.math.tau.ac.il/~safra/PapersAndTalks/nibfj.ps
5. Marichal, J.-L.: The influence of variables on pseudo-boolean functions with applications to game theory and multicriteria decision making. Discrete Applied Mathematics 107(1-3), 139–164 (2000)
6. Daemen, J., Paris, K.: The self-synchronzing stream cipher moustique. Technical report, e-Stream Project (2006), http://www.ecrypt.eu.org/stream/p3ciphers/mosquito/mosquito_p3.pdf
7. Daemen, J., Lano, J., Preneel, B.: Chosen ciphertext attack on sss. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/044 (June 2005), http://www.ecrypt.eu.org/stream/papers.html/044.pdf
8. Millérioux, G., Guillot, P., Amigó, J.M., Daafouz, J.: Flat dynamical systems and self-synchronizing stream ciphers (2008), http://hal.archives-ouvertes.fr/docs/00/33/18/33/PDF/FlatDS_SSSC.pdf
9. Millérioux, G., Guillot, P.: Self-synchronizing stream ciphers and dynamical systems: state of the art and open issues. International Journal of Bifurcation and Chaos 20(9) (September 2010)
10. Maurer, U.M.: New approaches to the design of self-synchronizing stream cipher. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 458–471. Springer, Heidelberg (1991)
11. Keller, N.: On the influence of variables on boolean functions in product spaces (May 2009), http://arxiv.org/PS_cache/arxiv/pdf/0905/0905.4216v1.pdf

Some Constructions of Almost-Perfect, Odd-Perfect and Perfect Polyphase and Almost-Polyphase Sequences

Evgeny I. Krengel

Kedah Electronics Engineering, Zelenograd, Korpus 445, Moscow 124498, Russia
evgeniy.krengel@kedah.ru

Abstract. In the paper, some new almost-perfect (AP), odd-perfect (OP) and perfect polyphase and almost-polyphase sequences derived from the Frank and Milewski sequences are presented. The considered almost-polyphase sequences are polyphase sequences with some zero elements. In particular, we constructed AP 2^{t+1}- and 2^{t+2}-phase sequences of length $2 \cdot 4^t$ and 4^{t+1}, OP 2^{t+1}- and 2^{t+2}-phase sequences of length 4^t and $2 \cdot 4^t$, OP 2^{t+1}- and 2^{t+2} - phase sequences of length $4^t(p^m + 1)$, $(p^m - 1) \equiv 0 \pmod{2 \cdot 4^t}$ with 4^t zeroes and length $2 \cdot 4^t(p^m + 1)$, $(p^m - 1) \equiv 0 \pmod{4^{t+1}}$ with $2 \cdot 4^t$ zeroes, and perfect 2^{t+1}- and 2^{t+2} - phase sequences of length $4^{t+1}(p^m + 1)$ with 4^{t+1} zeroes and $2 \cdot 4^{t+1}(p^m + 1)$ with $2 \cdot 4^{t+1}$ zeroes. It is shown that the phase alphabet size of the obtained OP and perfect almost-polyphase sequences is much smaller in comparison with the known OP and perfect polyphase sequences of the same length and the alphabet size of some new OP polyphase sequences is minimum.

1 Introduction

Polyphase and almost-polyphase sequences with good periodical autocorrelation properties and small phase alphabet size are widely used in digital communication and radar engineering [1-4]. In many applications it is important to have sequences with perfect, almost-perfect or odd-perfect autocorrelation functions. A polyphase sequence $\mathbf{x} = \{x_i\}$ with a phase alphabet size Q is a sequence whose element $x_i \in \exp(2\pi ik/Q)$, $0 \le k < Q$. Accordingly a sequence is called a perfect if all its out-of-phase autocorrelation coefficients are zero, an almost-perfect (AP) if all its out-of-phase autocorrelation coefficients except one are 0 and an odd-perfect (OP) if all its out-of-phase odd-periodic autocorrelation coefficients are 0 [1,4].

Perfect polyphase sequences include Q-phase Frank sequences of length Q^2 [5], $2N$-phase (N even) or N-phase (N odd) Zadoff-Chu sequences of length N [3,6], Q^{u+1}-phase Milewski sequences of length Q^{2u+1} [7], and their various modifications and combinations [3]. Unfortunately, the perfect polyphase sequences with small alphabet sizes can be built only for a few lengths. This drawback can be overcome by adding zeroes in sequences. In the result perfect polyphase

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 387–398, 2010.

sequences with one or some zeroes whose phase alphabet size doesn't depend on their length have been constructed. In [4] such perfect sequences are called the perfect almost-polyphase sequences. Following [4], we say that a polyphase sequence with zeroes is an almost-polyphase sequence if its number of zeroes is much smaller than the sequence length. Note that in this case the sequence has peak-factor close to 1 [2].

Among perfect almost-polyphase sequences are ternary Ipatov and Hoholdt-Justesen sequences [2,8] of length $(p^{mk}-1)/(p^m-1)$,p odd prime, k odd and $(2p^{mk}-1)/(2^m-1)$, k odd accordingly, quadriphase Lee sequences [9] with one zero element and length $(p^m+1) \equiv 2 \pmod 4$, 8-phase Lüke sequences [10] with one zero element and length $(p^m+1) \equiv 4 \pmod 8$, 8-phase sequences with two zeroes and length $2(p^m+1) \equiv 4 \pmod 8$ [11], etc. [12,13,14].

AP and OP polyphase and almost-polyphase sequence sets are also well known. In particular, there are AP binary sequence set of length $2(p^m+1)$, p odd prime discovered by Wolfmann [15], Langevin [16], Pott and Bradley [17] and AP ternary (APT) sequences of length $2(q^k-1)/(q-1)$ proposed by Langevin [18]. In 2001 Lüke built a new class of AP quadriphase sequences of length $p^j+1 \equiv 2 \pmod 4$, p odd prime [19]. Later, APT sequences of length $4(p^{km}-1)/(p^m-1)$, $(p^m-1) \equiv 0 \pmod 4$ and in particular, APT sequences of length $4(p^m+1)$ with four zeroes were found [20]. According to [20,21], the above APT sequences of length N generate OP ternary (OPT) sequences of length $N/2$. In particular, the APT sequences of length $2(p^m+1)$ and $4(p^m+1)$, $(p^m-1) \equiv 0 \pmod 4$ with two and four zeroes generate the OPT sequences of length p^m+1 and $2(p^m+1)$ with one and two zeroes.

In 2006 Zeng, Hu and Liu presented a novel method for constructing AP polyphase sequences based on shift sequences of m-sequences [22]. In particular, several new families of AP quadriphase sequences of lengths $J(p^m+1)$, $(p^m-1) \equiv 0 \pmod J$ where $J = 4, 8$ were obtained.

There is another method for constructing perfect and OP polyphase sequences. It is even-odd transformation (EOT) translating every perfect polyphase sequence to an odd-perfect sequence of the same length and vice versa [23].

In the paper, on the basis of the Frank and Milewski sequences we present the following new AP, OP and perfect polyphase and almost-polyphase sequences:

- AP and OP Q-phase sequences of length $Q^2/2$ and $Q^2/4$. Here and further Q is even.
- AP and OP $Q^2/2$-phase sequences of length $Q^3/2$ and $Q^3/4$ when $Q/2$ odd and Q^{u+1}-phase sequences of length $Q^{2u+1}/2$ and $Q^{2u+1}/4$ when $Q/2$ even or $u > 1$.
- AP Q-phase sequences of length $Q^2(p^m+1)/2, (p^m-1) \equiv 0 \pmod{Q^2/2}$.
- AP $Q^2/2$-phase sequences of length $Q^3(p^m+1)/2, (p^m-1) \equiv 0 \pmod{Q^3/2}$ when $Q/2$ odd and Q^{u+1}-phase sequences of length $Q^{2u+1}(p^m+1)/2, (p^m-1) \equiv 0 \pmod{Q^{2u+1}/2}$ when $Q/2$ even or $u > 1$.
- OP Q-phase sequences of length $Q^2(p^m+1)/4, (p^m-1) \equiv 0 \pmod{Q^2/2}$ with $Q^2/4$ zeroes.
- OP $Q^2/2$-phase sequences of length $Q^3(p^m+1)/4, (p^m-1) \equiv 0 \pmod{Q^3/2}$

with $Q^3/4$ zeroes when $Q/2$ odd and Q^{u+1}-phase sequences of length $Q^{2u+1}(p^m+1)/4, (p^m-1) \equiv 0 \pmod{Q^{2u+1}/2}$ with $Q^{2u+1}/4$ zeroes when $Q/2$ even or $u > 1$.

- Perfect 2^{t+1}- and 2^{t+2} - phase sequences of length $4^{t+1}(p^m+1)$ with 4^{t+1} zeroes, $(p^m-1) \equiv 0 \pmod{2 \cdot 4^t}$ and length $2 \cdot 4^{t+1}(p^m+1)$ with $2 \cdot 4^{t+1}$ zeroes, $(p^m-1) \equiv 0 \pmod{4^{t+1}}$. In particular, perfect 4-phase sequences of length $16(p^m+1), (p^m-1) \equiv 0 \pmod 8$ with 16 zeroes and also 8-phase sequences of length $32(p^m+1), (p^m-1) \equiv 0 \pmod{16}$ with 32 zeroes and length of $64(p^m+1), (p^m-1) \equiv 0 \pmod{32}$ with 64 zeroes.

The remainder of the paper is organized as follows. Section 2 contains some notations and definitions necessary for sequence constructions. In Section 3 we construct AP and OP polyphase sequences of length $Q^2/2$, $Q^{2u+1}/2$ and $Q^2/4$, $Q^{2u+1}/4$ accordingly. Section 4 describes constructions of AP polyphase and almost-polyphase sequences of length $Q^2(p^m+1)/2$, $(p^m-1) \equiv 0 \pmod{Q^2/2}$ and $Q^{2u+1}(p^m+1)/2$,$(p^m-1) \equiv 0 \pmod{Q^{2u+1}/2}$ and also OP almost-polyphase sequences of length $Q^2(p^m+1)/4$ and $Q^{2u+1}(p^m+1)/4$. In Section 5 we construct perfect 2^{t+1}- and 2^{t+2} - phase sequences of length $4^{t+1}(p^m+1)$,$(p^m-1) \equiv 0 \pmod{2 \cdot 4^t}$ and $2 \cdot 4^{t+1}(p^m+1)$,$(p^m-1) \equiv 0 \pmod{4^{t+1}}$ with 4^{t+1} and $2 \cdot 4^{t+1}$ zeroes accordingly. Section 6 includes some examples of the sequence constructions. Section 7 concludes the paper.

2 Preliminaries

Notations:

- $Tr_m^n(\alpha) = \sum_{i=0}^{n/m-1} \alpha^{p^{im}}$, the trace function of an element $\alpha \in GFp^n)$ to $GF(p^m)$;
- $ind_\beta z$, the index (logarithm) function z to base β ;
- $\theta_x(l) = \sum_{i=0}^{N-1} x_i x_{i+l}^*$, the periodic (even) autocorrelation function (ACF) of a sequence $\mathbf{x} = \{x_i\}$ with length N. Here x_i^* denotes the complex conjugate of x_i;
- $\widehat{\theta_x}(l) = \sum_{i=0}^{N-l-1} x_i x_{i+l}^* + \sum_{i=N-l}^{N-1} x_i \bar{x}_{i+l-N}^*$, the odd-periodic ACF of a sequence $\mathbf{x} = \{x_i\}$;
- $\theta_{xy}(l) = \sum_{i=0}^{N-1} x_i y_{i+l}^*$, the periodic (even) cross-correlation function (CCF) of sequences $\mathbf{x} = \{x_i\}$ and $\mathbf{y} = \{y_i\}$ with length N.

The even-odd transformation (EOT) with an integer parameter t of any sequence $\mathbf{s} = \{s_j\}$ of length N is given by [23]

$$s_j\langle t\rangle = s_j \exp(i\pi j(2t+1)/N) , \qquad j = 0, 1, 2 \ldots, N-1, i = \sqrt{-1}. \tag{1}$$

Let $\theta_{rs}(\tau)$ and $\hat{\theta}_{rs}(\tau)$ be the even and odd-periodic CCF of sequences $\mathbf{r}$ and $\mathbf{s}$ of length N. Let $\theta_{r\langle t\rangle s\langle t\rangle}(\tau)$ and $\hat{\theta}_{r\langle t\rangle s\langle t\rangle}(\tau)$ be the even and odd-periodic CCF of sequences $\mathbf{r}\langle t\rangle$ and $\mathbf{s}\langle t\rangle$ of length N. Then according to [23],

$$|\theta_{r\langle t\rangle s\langle t\rangle}(\tau)| = |\hat{\theta}_{rs}(\tau)| \tag{2}$$

and

$$|\hat{\theta}_{r\langle t\rangle s\langle t\rangle}(\tau)| = |\theta_{rs}(\tau)|. \tag{3}$$

Note that in the case $\mathbf{r} = \mathbf{s}$ the EOT coincides with the binary to P-phase (BTP) transform introduced by Lüke in [10].

A Frank sequence $\mathbf{f}^r = \{f_n^r\}$ is a perfect Q-phase sequence of length $N = Q^2$ with elements [5,3]

$$f_n^r = \exp(2\pi irjk/Q) = \alpha^{rjk}, 0 \le j, k < Q, \tag{4}$$

where $0 \le n = jQ + k \le Q^2 - 1$, $(r, Q) = 1$, $\alpha = \exp(2\pi i/Q)$, Q - an integer.

A Zadoff-Chu sequence $\mathbf{c}^r = \{c_j^r\}$ is a perfect polyphase sequence of length N with elements [6,3]

$$c_j^r = \begin{cases} \exp(i\pi r(j+1)j/N), & N \text{ odd} \\ \exp(i\pi rj^2/N), & N \text{ even} \end{cases} \quad 0 \le j < N,\ (r, N) = 1. \tag{5}$$

A Milewski sequence $\dot{\mathbf{m}}^r = \{\dot{m}_n^r\}$ is a perfect Q^{u+1}-phase sequence of length $N = Q^{2u+1}$ with elements [7]

$$\dot{m}_n^r = \dot{m}_{jQ^u+k}^r = d_{j(\mathrm{mod}Q)}^r \beta^{rjk}, \quad \beta = e^{2\pi i/Q^{u+1}}, \tag{6}$$

where $\mathbf{d}^r = \{d_s^r\}$, $0 \le s < Q$ is a Zadoff-Chu sequence of length $Q, j = 0, 1, \ldots,$ $Q^{u+1} - 1$, $k = 0, 1, \ldots, Q^u - 1, (r, Q) = 1$.

A modulatable Frank sequence $\breve{\mathbf{f}}^r = \{\breve{f}_n^r\}$ is a perfect polyphase sequence of length $N = Q^2$ with elements [3]

$$\breve{f}_n^r = \breve{b}_k f_{jQ+k}^r,$$

where $\breve{b}_k, 0 \le k < Q$, are arbitrary complex numbers with absolute values of 1. Correspondingly, a modulatable Milewski sequence $\breve{\mathbf{m}}^r = \{\breve{m}_n^r\}$ is a perfect polyphase sequence of length Q^{2u+1} with elements [3]

$$\breve{m}_n^r = \hat{b}_k \dot{m}_{jQ^u+k}^r,$$

where $\hat{b}_k, k = 0, 1, \ldots, Q^u - 1$, are arbitrary complex numbers with absolute values of 1.

Let $N = sm^2$ and s be square free. Then according to Mow's conjecture and its extension [4], the minimum alphabet size for perfect and odd-perfect polyphase sequences of length N is

$$P_{\min} = \begin{cases} 2sm, & \text{for even } s \text{ and old } m \\ sm, & \text{else} \end{cases} \tag{7}$$

and

$$P_{\min,\mathrm{odd}} = \begin{cases} sm, & \text{for even } s \text{ and old } m \\ 2sm, & \text{else} \end{cases}. \tag{8}$$

3 AP and OP Polyphase Sequences Derived from the Frank and Milewski Sequences

Let $\mathbf{x}$ be a perfect polyphase sequence of length $N = 2^g l$, l odd and the phase alphabet size P. According to (1), the EOT with parameter $2t + 1 = l$ of the sequence $\mathbf{x}$ is an OP sequence $\mathbf{y}$ of length N with the phase alphabet size $\mathrm{LCM}(P, 2^{g+1})$. Then using the OP sequence $\mathbf{y}$ we can build an AP sequence $\mathbf{w} = \mathbf{y} \cdot \bar{\mathbf{y}}$ of length $2N$, where $\bar{y}_j = -y_j$. Now let us apply the EOT to the Frank and Milewski perfect polyphase sequences. Note that Frank sequences possess the minimum phase alphabet size for any Q whereas the Milewski sequences have the minimum alphabet size only when Q is a product of different primes.

Obviously, the phase alphabet sizes of the OP and AP sequences derived from the Frank and Milewski sequences of odd length are $2Q$ and $2Q^{u+1}$ accordingly. For even length the situation is more complicated. Suppose $Q = 2^d s$, s odd. The alphabet sizes of the OP(AP) sequences derived from the Frank and Milewski sequences by the EOT are $\mathrm{LCM}(Q, 2^{2d+1}) = Q2^{d+1}$ and $\mathrm{LCM}(Q^{u+1}, 2^{(2u+1)d+1}) = Q2^{du+1}$ accordingly. Then for $Q = 2^d$ we get the OP(AP) 2^{2d+1}-phase and $2^{d(2u+1)+1}$-phase sequences. At the same time according to (8), $P_{\min,\mathrm{odd}}$ for OP polyphase sequences of length 2^{2d} and $2^{d(2u+1)}$ is 2^{d+1} and $2^{du+d/2+1}$ if d even or $2^{du+(d+3)/2}$ otherwise. It follows that the alphabet size of these OP(AP) sequences is much greater than $P_{\min,\mathrm{odd}}$.

However there are two other methods for constructing AP and OP polyphase sequences with much smaller alphabet size. The first method consists of finding such modulatable Frank and Milewski sequences whose EOT have the minimum alphabet size. It is possible for all Frank sequences and for those Milewski sequences that have the minimum alphabet size. The second method is based on a decomposition of the Frank and Milewski sequences of even length. In the paper we consider the second method since it does not need the EOT.

Theorem 1. *Let* $\mathbf{f}^r = \{f_n^r\}, 0 \le n < N$ *be a* Q*-phase Frank sequence of length* $N = Q^2$, $Q \ge 4$ *even. Let* $\delta^r = \{\delta_n^r\}$, $0 \le n < N/2$ *be a sequence of length* $Q^2/2$ *with elements* $\delta_n^r = f_{2n+1}^r$ *. Let* $\eta^r = \{\eta_n^r\}$ *and* $\varphi^r = \{\varphi_n^r\}$ *,* $0 \le n < N/4$ *be sequences of length* $Q^2/4$ *with elements* $\eta_n^r = f_{2n}^r$ *and* $\varphi_n^r = f_{2n+N/2}^r$ *accordingly. Then*

1. $\eta^r = \varphi^r$*;*
2. δ^r *is an AP* Q*-phase sequence of length* $Q^2/2$*;*
3. η^r *and* φ^r *are* $Q/2$*-phase Frank sequences of length* $Q^2/4$*.*

Proof. Suppose $Q = 2t$. From (4) it follows that $\eta^r = \varphi^r$. For the sequence η^r we have $2n = Qj_1 + k$, $k = 2k_1$, $0 \le j_1, k_1 < Q/2$. Then $\eta_n^r = f_{2n}^r = \exp(2\pi i r k_1 j_1/t)$. Since $n = tj_1 + k_1, 0 \le n < t^2$, $0 \le k_1, j_1 < t$, the sequence $\eta^r(\varphi^r)$ is a $Q/2$-phase Frank sequence of length $Q^2/4$. Now, since $\mathbf{f}^r$ is the perfect sequence with $\theta(0) = N$ and $\eta^r(\varphi^r)$ is the perfect sequence with $\theta(0) = N/4$, we conclude that δ^r is an AP Q-phase sequence of length $Q^2/2$. □

From $\delta_n^r = -\delta_{n+N/4}^r, 0 \le n < N/4$ we get that a sequence $\{f_{2n+1}^r\}$, $0 \le n < N/4$ is an OP Q-phase sequence of length $Q^2/4$. Besides, according to (8), the obtained OP sequences have the minimum phase alphabet size. In particular, the 4- and 8-phase Frank sequences of length 16 and 64 generate the AP (OP) 4- and 8-phase sequences of length 8(4) and 32(16) accordingly. Note that the AP 4-phase sequence of length 8 was found early in the result of an exhaustive computer search [22].

Theorem 2. *Let $\dot{\mathbf{m}}^r = \{\dot{m}_n^r\}, 0 \le n < N$ be a Q^{u+1}-phase Milewski sequence of length $N = Q^{2u+1}$, Q even. Let $\varepsilon^r = \{\varepsilon_n^r\}$, $0 \le n < N/2$ be a sequence of length $Q^{2u+1}/2$ with elements $\varepsilon_n^r = \dot{m}_{2n+1}^r$. Let $\mu^r = \{\mu_n^r\}$, $\omega^r = \{\omega_n^r\}$, $0 \le n < N/4$ be sequences of length $Q^{2u+1}/4$ with elements $\mu_n^r = \dot{m}_{2n}^r$ and $\omega_n^r = \dot{m}_{2n+N/2}^r$ accordingly. Then*

1. $\mu^r = \omega^r$;
2. if $Q/2$ odd and $u = 1$, then ε^r is an AP $Q^2/2$-phase sequence of length $Q^3/2$ and μ^r (ω^r) is a perfect Q^2-phase sequence of length $Q^3/4$;
3. if $Q/2$ even or $u > 1$, then ε^r is an AP Q^{u+1}-phase sequence of length $Q^{2u+1}/2$ and μ^r (ω^r) is a perfect $Q^{u+1}/2$-phase sequence of length $Q^{2u+1}/4$.

Proof. The proof is similar to the one given in [7]. From (6) we easily find that $\mu^r = \omega^r$. Consider an array $\hat{\mathbf{M}}^r = (\hat{m}_{jk}^r)$, where $\hat{m}_{jk}^r = d_{j(\mathrm{mod}Q)}\beta^{rjk}$, $j = 0, 1, \ldots, Q^{u+1} - 1, \quad k = 0, 1, \ldots, Q^u - 1$. Obviously, $\hat{\mathbf{M}}^r$ being unfolded row by row is associated with the sequence $\dot{\mathbf{m}}^r$. According to [7], the columns of the array $\hat{\mathbf{M}}^r$ are pairwise orthogonal. Then an array $(\tilde{m}_{jk}^r)$,where $\tilde{m}_{jk}^r = \hat{m}_{j,2k}^r$, $j = 0, 1, \ldots, Q^{u+1}/2 - 1, \quad k = 0, 1, \ldots, Q^u/2 - 1$ can be associated with the sequence μ^r. Clearly, its columns are pairwise orthogonal too. Let $D = Q^{u+1}/2$ and $F = Q^u/2$. It follows that $\theta_\mu(l) = 0$, $l \ne 0 \pmod F$. If $l = cF, c \ne 0 \pmod D$ then

$$\theta_\mu(l) = \sum_{j=0}^{D-1}\sum_{k=0}^{F-1} \hat{m}_{j,2k}^r \hat{m}_{j+c,2k}^{r*} = \sum_{j=0}^{D-1}\sum_{k=0}^{F-1} d_j^r \beta^{rj2k} d_{j+c}^{r*} \beta^{-r(j+c)2k}$$
$$= \Big(\sum_{j=0}^{D-1} d_j^r d_{j+c}^{r*}\Big)\Big(\sum_{k=0}^{F-1} \beta^{-2rck}\Big). \qquad (9)$$

There are two cases: when $c \ne 0 \pmod Q$ and when $c \equiv 0 \pmod Q$.

Case $c \ne 0 \pmod Q$. Then the first factor in the right part of the expression (9) is zero because d_n^r is the perfect sequence.

Case $c \equiv 0 \pmod Q$. Then β^{-2rc} is an Fth root of unity. On the other hand, $\beta^{-2rc} \ne 1$ since $c \ne 0 \pmod D$. Therefore, the second factor of the right part (9) is also zero. It follows that μ_n^r is a perfect sequence. Then by the above, ε^r is an AP sequence of length $Q^{2u+1}/2$. From (5) and (6) it follows that if $Q/2$ odd and $u = 1$ then the sequences ε^r and μ^r are $Q^2/2$- and Q^2-phase sequences. Otherwise, the sequences ε^r and μ^r are Q^{u+1}- and $Q^{u+1}/2$-phase sequences. □

From $\varepsilon_n^r = -\varepsilon_{n+N/2}^r$, $0 \le n < N/4$ it follows that a sequence $\{\varepsilon_n^r\}$, $0 \le n < N/4$ is an OP sequence of length $Q^{2u+1}/4$. There are two cases: when $Q \neq 2$ and when $Q = 2$.

The case $Q \neq 2$. It can be shown that when $Q/2 = p_1 p_2 ... p_n$ is a product of different odd primes the obtained perfect and OP polyphase sequences of length $Q^{2u+1}/4$ have the minimum phase alphabet size (7,8). In the converse case the alphabet size of these sequences is an integer multiple of $P_{\min}$ and $P_{\min,\text{odd}}$. Our analysis shows that these perfect sequences are the products either of two modulatable Milewski sequences or a modulatable Milewski sequence and the Zadoff-Chu sequence $1\, i$.

The case $Q = 2$. When $u = 1$ the sequence μ_n^r is the 4-phase Zadoff-Chu sequence $1, i$ of length 2 and the sequence ε^r is 1,-1,-1,1. On the contrary, when $u > 1$, by construction it follows that μ_n^r is the 2^u-phase Milewski sequence of length 2^{2u-1} while ε^r is AP 2^{u+1}-phase sequence of length 2^{2u}. The obtained AP and OP 2^{u+1}-phase sequences are new and possess the minimum alphabet size. For example, the 8-phase Milewski sequence of length 32 generates the 4-phase Milewski sequence of length 8 and the AP (OP) 8-phase sequence of length 16 (8). Note also that the same OP 2^{u+1}-phase sequences can be obtained by applying the EOT to some modulatable Milewski sequences of length 2^{2u-1}.

Thus by Theorem 1 and Theorem 2, we can construct the new AP (OP) 2^{t+1}- and 2^{t+2}-phase sequences of length $2{\cdot}4^t$ and 4^{t+1} (4^t and $2{\cdot}4^t$) with the minimum phase alphabet size. Besides, these AP sequences are balanced.

4 Some AP and OP Polyphase and Almost-Polyphase Sequences Derived from Shift Sequences

Let $p > 2$ be a prime, α be a primitive element of $GF(p^n)$, and β be a primitive element of $GF(p^m)$, where $n = mk$, $m \ge 1$,$k > 1$. Let $\mathbf{b}$ be an m-sequence over *GF(p)* of length $p^n - 1$ with elements $b_i = Tr_1^n(\alpha^i)$, $0 \le i < p^n$-1. Fold $\mathbf{b}$ into a decomposition array $\mathbf{B}$ by columns [24] with $T = (p^n - 1)/(p^m - 1)$ rows and p^m-1 columns. Its rows are either null rows or cyclic shifts of an m-sequence of length p^m-1 over *GF(p)*. A shift sequence is defined by

$$\mathbf{e} = \{e_i\} = \begin{cases} \infty, & \text{if } Tr_m^n(a^i) = 0 \\ ind_\beta(Tr_m^n(a^i)), & \text{if } Tr_m^n(a^i) \neq 0 \end{cases}, \tag{10}$$

where $0 \le i < p^n$ -1. The first T of its elements give all these cyclic shifts relatively to the m-sequence of length $p^m - 1$ and ∞ point to a null rows.

In [22] a method for constructing the AP polyphase sequences by using shift sequences of m-sequences was proposed. Shortly, the method can be described as follows. Let $\mathbf{e}$ be the shift sequence of the m-sequence $\mathbf{b}$ with $n = 2m, m \ge 1$. Let $\mathbf{z} = \{z_i\}$ be an AP polyphase sequence of length h, $h|(p^m - 1)$ with $\theta(0) = -\theta(h/2) = h$ and the phase alphabet size γ. Let $\mathbf{v} = \{v_i\}$ be a perfect polyphase sequence of length $h/2$ with $\theta(0) = h/2$ and the phase alphabet size ν. Let $\mathbf{v}_1 = \mathbf{v} \cdot \mathbf{v}$ be twice repeated sequence $\mathbf{v}$. Form an $T \times h$ array $\mathbf{W}$ whose

i-th row is a cyclic shift of the sequence $\mathbf{z}$ by $e_i \pmod h$ when $e_i \neq \infty$ or the sequence $\mathbf{v}_1$ in the converse case. Let $\mathbf{w}$ be a sequence associated with the array $\mathbf{W}$. Then according to [22], the sequence $\mathbf{w}$ of length hT is an AP polyphase sequence with the alphabet size $\mathrm{LCM}(\gamma, \nu)$.

Let $\mathbf{z}$ and $\mathbf{v}$ be the AP and perfect sequences produced by Theorem 1 or 2. As a result, we get some new AP Q-phase sequences of lengths $Q^2(p^m+1)/2$, $(p^m-1) \equiv 0 \pmod{Q^2/2}$ and AP $Q^2/2$-phase sequences of length $Q^3(p^m+1)/2$, $(p^m-1) \equiv 0 \pmod{Q^3/2}$ if $Q/2$ odd and $u=1$ and Q^{u+1}-phase sequences of length $Q^{2u+1}(p^m+1)/2$,$(p^m-1) \equiv 0 \pmod{Q^{2u+1}/2}$ otherwise.

Note that the similar method for constructing APT sequences of length Th was proposed in [20]. The generalization of this method for a case of AP almost-polyphase sequences is given by the following theorem.

Theorem 3. *Let $p > 2$ be a prime, $n = mk, m \geq 1, k > 1$, and $\mathbf{b}$ be an m-sequence over GF(p) of length $p^n - 1$ with the shift sequence $\mathbf{e} = \{e_i\}$ of length $T = (p^n-1)/(p^m-1)$. Let $\mathbf{z} = \{z_i\}$ be an AP polyphase or almost-polyphase sequence of length h, $h|(p^m-1)$ with autocorrelation peak R and let $z_i = -z_{i+h/2}$, $0 \leq i < h/2$. Let $\mathbf{W}$ be an $T \times h$ array whose i-th row is a cyclic shift of the sequence $\mathbf{z}$ by $e_i \pmod h$ if $e_i \neq \infty$ or the null sequence in the converse case. Then a sequence $\mathbf{w}$ associated with the array $\mathbf{W}$ is an AP almost-polyphase sequence of length $N = Th$ with autocorrelation peak Rp^{n-m} and $(p^n(h-R) + Rp^{n-m} - h)/(p^m-1)$ zeroes.*

By Theorem 3, $w_i = w_{i+N/2}$. It follows that a sequence $\{w_i\}, 0 \leq i < N/2$ is an OP almost-polyphase sequence of length $N/2$.

Consider the case when $n = 2m$. By Theorem 1 and 3, we get the AP Q-phase sequences of length $Q^2(p^m+1)/2$ with $Q^2/2$ zeroes. Accordingly, by Theorem 2 and 3, we have the AP $Q^2/2$-phase sequences of length $Q^3(p^m+1)/2$ with $Q^3/2$ zeroes if $Q/2$ odd and $u=1$ and Q^{u+1}-phase sequences of length $Q^{2u+1}(p^m+1)/2$ with $Q^{2u+1}/2$ zeroes otherwise. Note that length of the associated OP sequences is twice less.

Thus, when Q is a power of two and $u > 1$, we get the new AP 2^{t+1}- and 2^{t+2}-phase sequences of length $2 \cdot 4^t(p^m+1)$, $(p^m-1) \equiv 0 \pmod{2 \cdot 4^t}$ and length $4^{t+1}(p^m+1)$, $(p^m-1) \equiv 0 \pmod{4^{t+1}}$ with $2 \cdot 4^t$ and 4^{t+1} zeroes accordingly and OP 2^{t+1}- and 2^{t+2}- phase sequences of length $4^t(p^m+1)$ and length $2 \cdot 4^t(p^m+1)$ with 4^t and $2 \cdot 4^t$ zeroes accordingly.

5 Perfect Sequences Derived from Multiple Mix

Recently, a method for constructing perfect sequences of length $4N$ based on mixing of perfect and OP sequences with length N and the same autocorrelation peak R has been presented [14]. Shortly, the method for constructing perfect sequences is the following. Let sequences $\mathbf{a} = \{a_j\}$ and $\mathbf{b} = \{b_j\}, 0 \leq j < N$ be accordingly arbitrary perfect and OP sequences of length N with the same autocorrelation peak R. By concatenation, form two sequences $\acute{\mathbf{a}} = \mathbf{a} \cdot \mathbf{a}$ and $\acute{\mathbf{b}} = \mathbf{b} \cdot \bar{\mathbf{b}}$ of length $2N$ where $\bar{\mathbf{b}} = \{\bar{b}_j\}, \bar{b}_j = -b_j$. Then a sequence $\mathbf{f} = \{f_n\}, 0 \leq n < 4N$ given by the following rule

$$f_n = \begin{cases} \acute{a}_j, & n = 2j \\ \acute{b}_j, & n = 2j+1 \end{cases}, 0 \le j < 2N \tag{11}$$

is a perfect sequence of length $4N$. In most cases to compose pairs of the sequences **a** and **b** the EOT (BTP) transform is used. The relevant sequences can be connected by the EOT directly or indirectly through their decimations or cyclic shifts. But there might be cases when the pairs are not connected by any transform. In the paper we are interested in just such cases.

Let $n = 2m$. It is easy to show that then $8|(p^m - 1)$. Since $4|(p^m - 1)$, by [9,21] we can form pairs of the perfect almost-quadriphase Lee sequences of length $p^m + 1$ and the OPT sequences of length $p^m + 1$ with one zero. After the first mixing we have the perfect almost-quadriphase sequences of length $4(p^m + 1)$ with 4 zeroes [13]. Further, since $8|(p^m - 1)$, we can compose relevant pairs of the obtained above perfect almost-quadriphase sequences of length $4(p^m + 1)$ and the OP almost-quadriphase sequences of the same length with 4 zeroes. In the result of next mixing we get new perfect almost-quadriphase sequences of length $16(p^m + 1)$ with 16 zeroes.

Consider the case when $16|(p^m - 1)$. As in the previous case, we can also get the new perfect almost-quadriphase sequences of length $16(p^m + 1)$ with 16 zeroes. Further, since $4|(p^m - 1)$, let us form relevant pairs of the perfect 8-phase sequences of length $2(p^m + 1)$ with two zeroes [11] and OPT sequences of length $2(p^m + 1)$ with two zeroes [20]. Mixing them, we get perfect 8-phase sequences of length $8(p^m + 1)$ with 8 zeroes. Since $16|(p^m - 1)$, on the basis of these perfect sequences and the above OP 8-phase sequences of length $8(p^m + 1)$ we can construct new perfect 8-phase sequences of length $32(p^m + 1)$ with 32 zeroes.

Now let $32|(p^m - 1)$. Obviously, this case includes two previous cases. Also, we can form pairs of the above obtained perfect almost-quadriphase sequences of length $16(p^m + 1)$ with 16 zeroes and the OP 8-phase sequences of length $16(p^m + 1)$ with 16 zeroes obtained in Section 4. Applying to them the mix method we get new perfect 8-phase sequences of length $64(p^m + 1)$ with 64 zeroes. In this case the total number of the mixes is three.

Further, in the case $64|(p^m - 1)$ we can form pairs of the new perfect 8-phase sequences of length $32(p^m + 1)$ and the above obtained OP 16-phase sequences of length $32(p^m + 1)$ with 32 zeroes. After mixing we have new perfect 16-phase sequences of length $128(p^m + 1)$ with 128 zeroes. In general, when $(p^m - 1) \equiv 0 \pmod{2 \cdot 4^t}$ we get new perfect 2^{t+1} - phase sequences of length $4^{t+1}(p^m + 1)$ with 4^{t+1} zeroes and when $(p^m - 1) \equiv 0 \pmod{4^{t+1}}$ we get 2^{t+2}-phase sequences of length $2 \cdot 4^{t+1}(p^m + 1)$ with $2 \cdot 4^{t+1}$ zeroes.

Let $m = 2^k$. Then it can easily be checked that $(p^m - 1) \equiv 0 \pmod{2^{k+2}}$. This means that we can build perfect 4-phase sequences of length $16(p^{2s} + 1)$ and also perfect 8-phase sequences of length $32(p^{4s} + 1)$ and $64(p^{8s} + 1)$, $s = 1, 2, 3, \ldots$.

6 Examples

Example 1. Let $n = 4, m = 2, p = 3$, and $x^4 + x + 2$ be a primitive polynomial of degree 4 over $GP(3)$. In this case $p^m - 1 = 8$ and $p^m + 1 = 10$. According to [21], calculate the OPT sequence $1, 1, 1, 1, -1, 0, 1, 1, -1, 1$ of length 10. The perfect almost-quadriphase Lee sequence of length 10 is $1, i, -1, -i, -1, 0, -1, -i, -1, i$ [4,9]. After the first mixing we obtain the perfect almost-quadriphase sequence 1,1,*i*,1,-1,1, -*i*, 1, -1,-1, 0,0, -1, 1, -*i*, 1, -1, -1, *i*, 1, 1, -1, *i*, -1, -1, -1, -*i*, -1, -1, 1, 0, 0, -1, -1,-*i*, -1, -1, 1, *i*, -1 of length 40 with 4 zeroes.

Now on the basis of the AP almost-quadriphase sequence 1, 1, *i*, -*i*, -1,-1, -*i*, *i* of length 8 and Theorem 3, we construct the OP almost-quadriphase sequence 1, *i*, *i*, -*i*, 1, 0, -*i*, -1, 1, *i*, 1, -*i*, -*i*, *i*, *i*, 0, *i*, -1, *i*, -*i*, *i*, -1, -1, 1, -*i*, 0, 1, -*i*, -*i*, -1, -*i*, -1, -1, 1, -1, 0, 1, *i*, -1, -1 of length 40. After the next mixing we get the perfect almost-quadriphase sequence 1,1,1,*i*,*i*,*i*,1,-*i*,-1,1,1,0,-*i*,-*i*,1,-1,-1,1,-1,*i*,0,1,0,-*i*,-1,-*i*,1,*i*,-*i*,*i*,1,0,-1,*i*,-1,-1,*i*,*i*,1,-*i*,1,*i*,-1,-1,*i*,-1,-1,1,-1,-*i*,-1,0,-*i*, 1,-1,-*i*,-1,-*i*,1,-1,0,-*i*,0,-1,-1,-1,-1,1,-*i*,-1,-1,0,-1,1,1,*i*,*i*,-1,-1,-1,1,-1,1,-*i*,*i*,-*i*,1,*i*,-1,-1,0,-*i*, *i*, 1, 1,-1,-1,-1,-*i*,0,-1,0,*i*,-1,*i*,1,-*i*, -*i*,-*i*,1,0,-1,-*i*,-1,1,*i*,-*i*,1,*i*,*i*,1,-*i*,-1,1,*i*,1,-1,-1,-1,*i*,-1,0,-*i*, -1,-1, *i*,-1,*i*,1,1,0,*i*,0,1,-1,1,-1,-1,-*i*,*i*,1,-1,0,-1,-1,1,-*i*,*i*,1,-1,1 of length 160 with 16 zeroes. Note that according to (7,8), the minimum alphabet size for the perfect and OP polyphase sequences of length 160 and 40 is 40. The combined perfect polyphase sequences of length 160 produced by the multiplication of 8-phase Milewski sequences of length 32 and 5-phase Zadoff-Chu sequences of length 5 have just such alphabet size. Also there is 320-phase Zadoff-Chu sequences of length 160.

Example 2. Let $n = 8, m = 4$, and $p = 3$. In this case $p^m - 1 = 80$ and $p^m + 1 = 82$. Since $16|80$, perfect almost-quadriphase sequences of length $16 * 82 = 1312$ with 16 zeroes and perfect almost 8-phase sequences of length 2624 with 32 zeroes accordingly can be constructed. There exist perfect polyphase sequences with the same lengths. Namely, there are combined perfect 328-phase sequences of length 1312, 2624-phase Zadoff-Chu sequences of length 1312, combined perfect 328-phase sequences of length 2624 and the 5248-phase Zadoff-Chu sequence of length 2624. Note that the minimum alphabet size for the perfect polyphase sequences with length 1312 and 2624 is 328.

Example 3. Let $p = 193$ and $m = 1$. Then $p-1 = 192, p+1 = 194$ and $64|192$. Using Theorem 1, we can construct perfect almost-quadriphase sequences of length 3104 with 16 zeroes and perfect almost 8-phase sequences of length 12416 with 64 zeroes. Further, using Theorem 2, we can construct perfect almost 8-phase sequences of length 6208 with 32 zeroes and perfect almost 16-phase sequences of length 24832 with 128 zeroes. There are also perfect polyphase sequences with the same lengths like perfect combined 776-phase sequences and 6208 -phase Zadoff-Chu sequences of length 3104, perfect combined 776-phase sequences and 12416-phase Zadoff-Chu sequences of length 6208, perfect combined 1552-phase sequences and 24832-phase Zadoff-Chu sequences of length 12416, and perfect combined 1552-phase sequences and 49664-phase Zadoff-Chu sequences of length

24832. Note that the minimum alphabet sizes for the perfect polyphase sequences of length $3104, 6208, 12416$, and 24832 are $776, 776, 1552$, and 1552 accordingly.

7 Conclusions

The constructions described in this paper allow to get some new AP, OP and perfect polyphase and almost-polyphase sequence sets of different nature and structure. None the less all these sequences are connected with each other as they are based on the Frank, Zadoff-Chu, and Milewski perfect sequences [3].

The phase alphabet size of the constructed perfect and OP almost-polyphase sequences is much smaller in comparison with the known perfect and OP polyphase sequences with the same length. Moreover, some of the new OP polyphase sequences possess the minimum alphabet size.

The presented results allow to conjecture that the perfect polyphase sequences generate the OP polyphase sequences with the minimum alphabet size if and only if their alphabet size is minimum.

Due to their good autocorrelation, the considered sequences can be used in communication systems for synchronization and channel estimation as well as in radar and sonar systems for ranging.

Acknowledgment

The author thanks the anonymous referees for their valuable comments and suggestions.

References

1. Golomb, S.W., Gong, G.: Signal Design for Good Correlation: for Wireless Communication,Cryptography and Radar. Cambridge University Press, Cambridge (2005)
2. Ipatov, V.P.: Periodic discrete signals with optimal correlation properties. Moscow, "Radio i svyaz" (1992), ISBN-5-256-00986-9
3. Fan, P., Darnell, M.: Sequence Design for Communications Applications. Research Studies Press Ltd., London (1996)
4. Lüke, H.D., Schotten, H.D., Hadinejad-Mahram, H.: Binary and quadriphase sequences with optimal autocorrelation properties: survey. IEEE Transactions on Information Theory IT-49(12), 3271–3282 (2001)
5. Frank, R.L.: Phase coded communication system. U.S. Patent 3,099,795, July 30 (1963)
6. Chu, D.C.: Polyphase codes with good periodic correlation properties. IEEE Transactions on Information Theory IT-18, 531–533 (1972)
7. Milewski, A.: Periodic sequences with optimal properties for channel estimation and fast start-up equalization. IBM Jornal of Research and Development 27(5), 425–431 (1983)
8. Hoholdt, T., Justesen, J.: Ternary sequences with perfect periodic auto-correlation. IEEE Transactions on Information Theory IT-29(4), 597–600 (1983)

9. Lee, C.E.: Perfect q-ary sequences from multiplicative characters over GF(p). Electron. Lett. 3628(9), 833–835 (1992)
10. Lüke, H.D.: BTP-transform and perfect sequences with small phase alphabet. IEEE Transactions Aerosp. Syst. 32, 497–499 (1996)
11. Krengel, E.I.: Some new 8-phase perfect sequences with two zeroes. In: Proceedings of the second International Symposium on Sequence Design and Its Application in Communications (IWSDA 2005), Shimonoseki, Japan, October 10-14, pp. 35–38 (2005)
12. Schotten, H.D., Lüke, H.D.: New perfect and w-cyclic-perfect sequences. In: Proc. 1996 IEEE International Symp. on Information Theory, pp. 82–85 (1996)
13. Krengel, E.I.: New polyphase perfect sequences with small alphabet. Electron. Lett. 44(17), 1013–1014 (2008)
14. Krengel, E.I.: A method of construction of perfect sequences. Radiotehnika 11, 15–21 (2009)
15. Wolfmann, J.: Almost perfect autocorrelation sequences. IEEE Transactions on Information Theory IT–38(4), 1412–1418 (1992)
16. Langevin, P.: Almost perfect binary functions. Applicable Algebra in Engineering, Communication and Computing 4, 95–102 (1993)
17. Pott, A., Bradley, S.: Existance and nonexistence of almost-perfect autocorrelation sequences. IEEE Transactions on Information Theory IT-41(1), 301–304 (1995)
18. Langevin, P.: Some sequences with good autocorrelation properties. In: Finite Fields, vol. 168, pp. 175–185 (1994)
19. Lüke, H.D.: Almost-perfect quadriphase sequences. IEEE Transactions on Information Theory IT-47, 2607–2608 (2001)
20. Krengel, E.I.: Almost-perfect and odd-perfect ternary sequences. In: Helleseth, T., Sarwate, D., Song, H.-Y., Yang, K. (eds.) SETA 2004. LNCS, vol. 3486, pp. 197–207. Springer, Heidelberg (2005)
21. Lüke, H.D., Schotten, H.D.: Odd-perfect almost binary correlation sequences. IEEE Trans. Aerosp. Electron. Syst. 31, 495–498 (1996)
22. Zeng, X.Y., Hu, L., Liu, Q.C.: A novel method for constructing almost perfect polyphase sequences. In: Ytrehus, Ø. (ed.) WCC 2005. LNCS, vol. 3969, pp. 346–353. Springer, Heidelberg (2006)
23. Mow, W.H.: Even-odd transformation with application to multi-user CW radars. In: Proceedings 1996 IEEE 4th International Symposium on Spread Spectrum Techniques and Applications Proceedings, Mainz, Germany, September 22-25, pp. 191–193 (1996)
24. Baumert, L.D.: Cyclic difference sets. Springer, Berlin (1971)

Almost p-Ary Perfect Sequences

Yeow Meng Chee[1], Yin Tan[1,⋆], and Yue Zhou[2,⋆⋆]

[1] Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371 Singapore
ymchee@ntu.edu.sg, itanyinmath@gmail.com

[2] Department of Mathematics, Otto-von-Guericke-University Magdeburg, 39106 Magdeburg, Germany
yue.zhou@st.ovgu.de

Abstract. A sequence $\mathbf{a} = (a_0, a_1, a_2, \cdots, a_n)$ is said to be an almost p-ary sequence of period $n+1$ if $a_0 = 0$ and $a_i = \zeta_p^{b_i}$ for $1 \le i \le n$, where ζ_p is a primitive p-th root of unity and $b_i \in \{0, 1, \cdots, p-1\}$. Such a sequence $\mathbf{a}$ is called perfect if all its out-of-phase autocorrelation coefficients are zero; and is called nearly perfect if its out-of-phase autocorrelation coefficients are all 1, or are all -1. In this paper, on the one hand, we construct almost p-ary perfect and nearly perfect sequences; on the other hand, we present results to show they do not exist with certain periods. It is shown that almost p-ary perfect sequences correspond to certain relative difference sets, and almost p-ary nearly perfect sequences correspond to certain direct product difference sets. Finally, two tables of the existence status of such sequences with period less than 100 are given.

Keywords: almost p-ary sequences, almost p-ary perfect sequences, almost p-ary nearly perfect sequences, relative difference set, direct product difference set.

1 Introduction

Let $\mathbf{a} = (a_0, a_1, a_2, \cdots, a_n)$ be a complex sequence of period $n+1$. We call $\mathbf{a}$ an *m-ary sequence* if $a_i = \zeta_m^{b_i}$, where ζ_m is a primitive m-th root of unity and $b_i \in \{0, 1, \cdots, m-1\}$ for $0 \le i \le n$. In particular, the sequence $\mathbf{a}$ is called an *almost m-ary sequence if* $a_0 = 0$. For an (almost) m-ary sequence $\mathbf{a}$ with period $n+1$, the *autocorrelation coefficients* of $\mathbf{a}$ are the elements in the set

$$\{C_t(\mathbf{a}) = \sum_{i=0}^{n} a_i \overline{a_{i+t}} : 0 \le t \le n\},$$

⋆ Research of Yeow Meng Chee and Yin Tan is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03 and by the Nanyang Technological University under Research Grant M58110040.

⋆⋆ Research of Yue Zhou is partially supported by China Scholarship Council.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 399–415, 2010.

where $\bar{\cdot}$ is the complex conjugate and all subscripts are computed modulo $n+1$. For all $t \not\equiv 0 \mod (n+1)$, the $C_t(\mathbf{a})'$s are called *out-of-phase* autocorrelation coefficients, and *in-phase* autocorrelation coefficients otherwise.

Motivated by applications in engineering, sequences with small out-of-phase coefficients are of particular interests. Usually, the complex sequence $\mathbf{a}$ is expected to have a *two-level autocorrelation function*, i.e. all out-of-phase autocorrelation coefficients are a constant γ. For an almost m-ary sequence $\mathbf{a}$, we call $\mathbf{a}$ *perfect* if it has a two-level autocorrelation function and $\gamma = 0$. Moreover, we call $\mathbf{a}$ *nearly perfect* if out-of-phase autocorrelation coefficients γ all satisfy $\gamma = 1$, or all they satisfy $\gamma = -1$. We refer to [7] for a well-rounded survey on perfect binary sequences, to [9] for results of perfect and nearly perfect p-ary sequence, where p is an odd prime. In the following we briefly introduce the relationship between (almost) binary (with entries ± 1) perfect sequences and (Conference) Hadamard matrices.

A matrix H with entries ± 1 and order v is called a *Hadamard matrix* if $HH^T = vI$; and a matrix C with entries $0, \pm 1$ and order v is called a *Conference matrix* if $CC^T = (v-1)I$, where I is the identity matrix. It is well known that perfect binary (with entries ± 1) sequences of period v are equivalent to cyclic difference sets (see [7, Section 2]). In particular, when $v \equiv 0 \mod 4$, the perfect binary sequences are equivalent to circulant Hadamard matrices, or cyclic Hadamard difference sets (see [12, Section 1.1]). More precisely, let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ be a binary perfect sequence of period v. Let $H = (h_{i,j})_{i,j=0}^{v-1}$ be a circulant matrix (H is called *circulant* if $h_{i+1,j+1} = h_{i,j}$ for all i, j) defined by $h_{0,j} = a_j$ for $j \in \mathbb{Z}_v$, then H is a circulant Hadamard matrix of order v. Similarly, let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ be an almost binary perfect sequence, i.e. $a_0 = 0$ and $a_i = \pm 1$ for $1 \le i \le v-1$. Then the circulant matrix $C = (h_{i,j})_{i,j=0}^{v-1}$ defined by $h_{0,j} = a_j$ for $j \in \mathbb{Z}_v$ is a circulant Conference matrix. The famous circulant Hadamard matrices conjecture is that there do not exist circulant Hadamard matrices if $v > 4$. In contrast to this still open problem, an elegant and elementary proof in [13] shows that there do not exist circulant Conference matrices: It seems that the mathematical behavior of binary perfect sequences and almost binary perfect sequences are quite different, which is one motivation of our paper. In this paper, we study the properties of general almost p-ary perfect sequences, where p is a prime. It turns out that almost p-ary perfect sequences of period $n+1$ are equivalent to $(n+1, p, n, (n-1)/p)$ relative difference sets in $\mathbb{Z}_{n+1} \times \mathbb{Z}_p$ relative to $\mathbb{Z}_p$ (Theorem 1).

The lack of examples of almost p-ary perfect sequences motivates our research in almost p-ary nearly perfect sequences. It is shown that periodic almost p-ary nearly perfect sequences correspond to certain direct product difference sets (Theorem 6).

This paper is organized as follows. In Section 2, we give necessary definitions and results. The discussions about almost p-ary perfect and nearly perfect sequences are given in Section 3 and 4 respectively. In Appendix, we give two tables of the existence status of almost p-ary perfect and nearly perfect sequences

with period less than 100. Our results generalize those about perfect and nearly perfect p-ary sequences which have been done by Ma and Ng in [9].

2 Preliminaries

In this section, we give necessary definitions and results used in this paper.

2.1 Relative Difference Sets, Characters and Group Rings

To facilitate the study of difference sets by using group rings and character theory, we use the multiplicatively written group $G = \langle g | g^n = 1 \rangle$ instead of the additively written group $\mathbb{Z}_n$. We refer to [10] for the basic facts of group rings and [8] for character theory on finite fields. In the following, we identify a subset A of G with a group ring element $\sum_{a \in A} a$ of $\mathbb{C}[G]$ and we still denote it by A. For any integer t, we define $A^{(t)} = \sum_{a \in A} a^t$. For a group ring element $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$, we define $|A| = \sum_{g \in G} a_g$.

Let G be an abelian group of order mn and let N be a subgroup of order n. A k-subset R of G is said to be an (m, n, k, λ) *relative difference set* (RDS) in G relative to N if all elements not in N can be represented exactly λ times as the form

$$r_1 r_2^{-1},\ r_1, r_2 \in R \text{ and } r_1 \neq r_2,$$

and no element in N can be represented as this form. In the language of group rings, R is an (m, n, k, λ) relative difference set in G relative to N if and only if

$$RR^{(-1)} = k + \lambda(G - N).$$

A k-subset D of a group G is said to be a (v, k, λ) *difference set* (DS) if all non-identity elements of G can be represented exactly λ times as the form

$$d_1 d_2^{-1},\ d_1, d_2 \in D, d_1 \neq d_2.$$

We refer to [2] for details on difference sets. Relative difference sets can be regarded as the "lifting" of difference sets.

Result 1. *[11, Lemma 1.1.12] Let R be an abelian (m, n, k, λ)-RDS in G relative to N, where N is a subgroup of G of order n. Let L be a subgroup of N of order l and let $\rho : G \to G/L$ be the natural epimorphism. Then $\rho(R)$ is an $(m, \frac{n}{l}, k, l\lambda)$-RDS in G/L relative to N/L. Moreover, if $L = N$, then $\rho(R)$ is an $(m, k, n\lambda)$ difference set in G/L.*

The following result provides a useful method to prove a k-subset R of G to be an (m, n, k, λ)-RDS.

Result 2. *Let G be an abelian group of order mn and let N be a subgroup of G of order n. A k-subset R is an (m, n, k, λ)-RDS in G relative to N if and only if*

$$\chi(R)\overline{\chi(R)} = \begin{cases} n & \text{if } \chi \text{ is not principal on } N, \\ k - n\lambda & \text{if } \chi \text{ is principal on } N \text{ but nonprincipal on } G, \\ k^2 & \text{if } \chi \text{ is principal on } G, \end{cases} \tag{1}$$

where χ is a character of G.

A prime p is said to be *self-conjugate* modulo w if $p^j \equiv -1 \mod (w')$ for some j, where w' is the maximal p-free part of w, i.e. the maximal factor of w which is relative prime to p. A composite integer m is said to be self-conjugate modulo w if every prime divisor of m is self-conjugate modulo w. The self-conjugate condition is quite useful in determining the existence of RDSs. The following two results are used later; see [11].

Result 3. *Let p be a prime and ζ_w be a primitive w-th root of unity in $\mathbb{C}$.*

1. *If $w = p^e$, then the decomposition of the ideal (p) into prime ideals is $(p) = (1 - \zeta_w)^{\phi(w)}$.*
2. *If $(w, p) = 1$, then the prime ideal decomposition of the ideal (p) is $(p) = \pi_1 \cdots \pi_g$, where $\pi_i's$ are distinct prime ideals. Furthermore, $g = \phi(w)/f$ where f is the order of p modulo w. The field automorphism $\zeta_w \rightarrow \zeta_w^p$ fixes the ideals π_i.*
3. *If $w = p^e w'$ with $(w', p) = 1$, then the prime ideal (p) decomposes as $(p) = (\pi_1 \cdots \pi_g)^{\phi(p^e)}$, where $\pi_i's$ are distinct prime ideals and $g = \phi(w')/f$. If t is an integer not divisible by p and $t \equiv p^s \mod (w')$ for a suitable integer s, then the field automorphism $\zeta_w \rightarrow \zeta_w^t$ fixes the ideals π_i.*

2.2 Two Important Lemmas

The following two lemmas are crucial to the proof of our results in Section 3 and 4. They deal with the cases whether the self-conjugate condition is satisfied or not. We record them here for the convenience of the reader.

Lemma 1. *[9] Let q be a prime and α be a positive integer. Let K be an abelian group such that either q does not divide $|K|$ or the Sylow q-subgroup of K is cyclic. Let L be any subgroup of K and $Y \in \mathbb{Z}[K]$ where the coefficients of Y lie between a and b where $a < b$. Suppose*

1. *q is self-conjugate modulo $\exp(K)$;*
2. *$q^r | \chi(Y)\overline{\chi(Y)}$ for all $\chi \notin L^\perp$ and $q^{r+1} \nmid \chi(Y)\overline{\chi(Y)}$ for some $\chi \notin L^\perp$;*
3. *$\chi(Y) \neq 0$ for some $\chi \notin L^\perp \cup Q^\perp$ where $Q = K$ if $q \nmid |K|$ and Q is the subgroup of K of order q otherwise. Here $L^\perp$ denotes the subset of the character group which is non-principal on L.*

Then

1. *if $q \nmid |K|$, r is even and $q^{\frac{r}{2}} \leq b - a$; and*
2. *if Sylow q-subgroup of K is cyclic, $q^{\lfloor \frac{r}{2} \rfloor} \leq 2(b - a)$ when L is a proper subgroup of $|K|$ and $q^{\lfloor \frac{r}{2} \rfloor} \leq b - a$ when $L = K$.*

Lemma 2. *[1] Let $G = \langle \alpha \rangle \times H$ be an abelian group of exponent $v = uw$, where $\mathrm{ord}(\alpha) = u, \exp(H) = w$ and $(u, w) = 1$. Suppose $y \in \mathbb{Z}[G]$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ such that*

1. *$\chi(y)\overline{\chi(y)} = n$ for all characters χ of G such that $\chi(\alpha) = \zeta_u$, where n is an integer relative prime to w; and*
2. *σ fixes every prime ideal divisor of $n\mathbb{Z}[\zeta_v]$.*

If $\sigma(\zeta_v) = \zeta_v^t$, *then*

$$y^{(t)} = \pm\beta y + \sum_{i=1}^{r} \langle \alpha^{u/p_i} \rangle x_i,$$

where $\beta \in G, x_1, \cdots, x_r \in \mathbb{Z}[G]$ *and* $p_1, \cdots, p_r$ *are all prime divisors of* u.

Furthermore, if u *is even, then the sign* $\pm$ *can be chosen arbitrarily by choosing appropriate* β.

2.3 Direct Product Difference Sets

We conclude this section by introducing the direct product difference sets. They were first defined in [4], but studied only the case $\lambda_1 = 0, \lambda_2 = 0$. The general definition of direct product difference sets is given in [9].

Let $G = H \times N$, where the order of H and N are m and n respectively. A k-subset R is said to be an $(m, n, k, \lambda_1, \lambda_2, \mu)$ *direct product difference set* (DPDS) in G relative to H and N if

$$r_1 r_2^{-1},\ r_1, r_2 \in R, r_1 \neq r_2$$

represent

1. all non-identity elements in H exactly λ_1 times;
2. all non-identity elements in N exactly λ_2 times;
3. all non-identity elements in $G \backslash H \cup N$ exactly μ times.

In the group ring language, R is an $(m, n, k, \lambda_1, \lambda_2, \mu)$-DPDS in G relative to H and N if and only if

$$RR^{(-1)} = (k - \lambda_1 - \lambda_2 + \mu) + (\lambda_1 - \mu)H + (\lambda_2 - \mu)N + \mu G. \tag{2}$$

3 Almost p-Ary Perfect Sequences

In this section we construct almost p-ary perfect sequences, and prove that they do not exist with certain periods. First we fix some notations which will be frequently used. Let p be a prime and let $G = H \times P$, where $H = \langle h \rangle, P = \langle g \rangle, \mathrm{ord}(h) = n + 1$ and $\mathrm{ord}(g) = p$. Let ζ_p be a primitive p-th root of unity and $\mathbf{a} = \{0, a_1, \cdots, a_n\}$ be an almost p-ary sequence of period $n + 1$, where $a_i = \zeta_p^{b_i}$ with $b_i \in \{0, 1, \cdots, p - 1\}$. For the convenience of expression, we define $a_0 = 0$.

Now we consider the following n-subset R of G

$$R = \{g^{b_i} h^i | i = 1, 2, \cdots, n\}. \tag{3}$$

Obviously,

$$RR^{(-1)} = n + \sum_{t=1}^{n} \sum_{\substack{j=1 \\ j \not\equiv -t \mod (n+1)}}^{n} g^{b_{j+t} - b_j} h^t. \tag{4}$$

Lemma 3. *Let χ be a character of P and extend $\chi : \mathbb{Z}[G] \longrightarrow \mathbb{Q}(\zeta_p)[H]$ to be a ring epimorphism such that $\chi(x) = x$ for all $x \in H$. Then*

$$\chi(R)\chi(R^{(-1)}) = \begin{cases} \sum_{t=0}^{n} C_t(\boldsymbol{a})^{\sigma} h^t & \text{if } \chi \text{ is nonprincipal on } P, \\ 1 + (n-1)H & \text{if } \chi \text{ is principal on } P, \end{cases} \tag{5}$$

where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $\sigma(\zeta_p) = \chi(g)$.

Proof. If χ is principal on P, then $\chi(R)\chi(R^{(-1)}) = (H-1)^2 = 1 + (n-1)H$. Otherwise, suppose $\chi(g) = \sigma(\zeta_p)$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, the results follow from (4). □

We remind the reader that $\mathbf{a}$ is an almost p-ary PS of period $n+1$ if its out-of-phase autocorrelation coefficients are all zero and $C_0(\mathbf{a}) = n$.

Theorem 1. *Let $\mathbf{a}$ be an almost p-ary sequence of period $n+1$, then $\mathbf{a}$ is an almost p-ary perfect sequence if and only if R is an $(n+1, p, n, (n-1)/p)$-RDS in G relative to P, i.e.*

$$RR^{(-1)} = n + \frac{n-1}{p}(G - P), \tag{6}$$

where R is defined in (3).

Proof. By Lemma 3, for all characters χ of P,

$$\chi(RR^{(-1)}) = \begin{cases} n & \text{if } \chi \text{ is nonprincipal on } P, \\ 1 + (n-1)H & \text{if } \chi \text{ is principal on } P. \end{cases}$$

Now the result is followed by Result 2. □

By Theorem 1, we get a necessary condition for the existence of almost p-ary PSs with period $n+1$.

Corollary 1. *If there exists an almost p-ary perfect sequence of period $n+1$, then $p \mid n-1$.*

In the following we give an example of almost p-ary PSs from the classical affine difference sets.

Example 1. Let $\mathbb{F} := \mathbb{F}_q$ be the field of order q and $q = w^f$ be a prime power. Let α be a primitive element of the field $\mathbb{K} = \mathbb{F}_{q^2}$ and let G be the multiplicative group of $\mathbb{K}$. Clearly $G \cong \mathbb{Z}_{q^2-1}$. It is well known that the subset

$$D = \{\alpha^i | \mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha^i) = 1\}$$

of $\mathbb{K}$ is a cyclic $(q+1, q-1, q, 1)$-RDS in G relative to N, where $N \leqslant G$ and $N \cong \mathbb{Z}_{q-1}$ (see [11, Theorem 2.2.12]). Let p be a prime divisor of $q-1$ with $\gcd(p, q+1) = 1$ and let $M \leqslant N, M \cong \mathbb{Z}_{\frac{q-1}{p}}$. Let $\rho : G \longrightarrow G/M$ be the natural epimorphism, then $\rho(R)$ is a $(q+1, p, q, \frac{q-1}{p})$-RDS in G/M relative to N/M. It is clear that $G/M \cong \mathbb{Z}_{q+1} \times \mathbb{Z}_p$ and $N/M \cong \mathbb{Z}_p$. By Theorem 1, there exists an almost p-ary PS of period $q+1$ whenever q is a prime power and $p | q-1, \gcd(p, q+1) = 1$.

Next we give several nonexistence results to show that almost p-ary PSs do not exist with certain periods.

Result 4. *[5] Abelian splitting $(n+1, 2, n, (n-1)/2)$-relative difference sets do not exist.*

By Theorem 1, we have the following result.

Theorem 2. *There do not exist almost binary perfect sequences of period $n+1$ for any n.*

Result 5. *[6] Let R be an abelian $(n+1, n-1, n, 1)$-RDS in G relative to N, then n should be a prime power for $n \leq 10,000$.*

Using the technique in [9], we have the following result. Note that $\gcd(p, q) = 1$, where p is a prime divisor of n and q is a prime divisor of $n+1$. We use the notation $p^r \parallel n$ to denote p^r strictly divide n, namely $p^r \mid n$ but $p^{r+1} \nmid n$.

Theorem 3. *Let R be an $(n+1, p, n, \frac{n-1}{p})$-RDS in G relative to P. Assume that there exists a prime divisor $q \neq p$ of n and q is self-conjugate modulo $p \cdot u$, where $u \mid n+1$. Let $q^r \parallel n$, then r is even and $q^{\frac{r}{2}} \leq \frac{n+1}{u}$.*

Proof. Let $\rho : G \to K := G/\langle h^u \rangle$ be the natural epimorphism. By (6),

$$\rho(R)\rho(R^{(-1)}) = n + \frac{n-1}{p}(\frac{n+1}{u}K - \rho(P)).$$

It is clear that the coefficients of $\rho(R)$ lie between 0 and $\frac{n+1}{u}$. Let χ be a nonprincipal character of K, we have

$$\chi(\rho(R))\overline{\chi(\rho(R))} = \begin{cases} n \text{ if } \chi \text{ is nonprincipal on } \rho(P), \\ 1 \text{ if } \chi \text{ is principal on } \rho(P). \end{cases}$$

Now set $L = \rho(P)$ and $Y = \rho(R)$, where L and Y are defined in Lemma 1. It is routine to verify that the conditions in Lemma 1 are satisfied for L and Y here. Therefore we complete the proof. □

The following two results can be easily followed from Theorem 3.

Corollary 2. *Assume that there exists a prime divisor $q \neq p$ of n such that q is self-conjugate modulo $p(n+1)$, then there do not exist $(n+1, p, n, \frac{n-1}{p})$-RDSs in G relative to P. In other words, there do not exist almost p-ary perfect sequences of period $n+1$.*

Corollary 3. *Assume that there exists a prime divisor $q \neq p$ of n such that q is self-conjugate modulo p. If $q^{2s+1} \parallel n$, then there do not exist $(n+1, p, n, \frac{n-1}{p})$-RDSs in G relative to P. In other words, there do not exist almost p-ary perfect sequences of period $n+1$.*

The above results depend on the self-conjugate condition. Usually it is difficult to determine the existence status of almost p-ary PSs if this condition is not satisfied. However, in some cases we can determine whether the almost p-ary PSs exist or not when n is small. We briefly introduce the main idea of this method here. An (m, n, k, λ)-RDS is called *regular* if $k^2 \neq \lambda mn$. Let D be a RDS in G and let t be an integer with $\gcd(t, |G|) = 1$. We call t a *multiplier* of D if $D^{(t)} = Dg$ for some $g \in G$. It is well known that Rg is also a RDS for any $g \in G$. The following result tells us that we may assume R satisfying $R^{(t)} = R$ if R is regular.

Result 6. *[11] Let R be a regular (m, n, k, λ)-RDS and let t be a multiplier of D. Then there exists at least one translate Rg such that $(Rg)^{(t)} = Rg$.*

Let Ω be the set of orbits of G under the group automorphism $x \mapsto x^t$. Since $R^{(t)} = R$, we see that R is the union of elements in Ω, namely

$$R = \bigcup_{\omega \in \Phi} \omega,$$

where $\Phi \subseteq \Omega$. A natural way to construct R is to combine the elements in Ω. On the one hand, if there do not exist a subset Φ of Ω such that $|\bigcup_{\omega\in\Phi} \omega| = |R|$, then clearly R do not exist. On the other hand, to construct R, we may find suitable Φ with $|\bigcup_{\omega\in\Phi} \omega| = |R|$ and verify whether $\bigcup_{\omega\in\Phi} \omega$ is a RDS. Next result gives a way to find multipliers of RDSs.

Theorem 4. *Let R be an $(n+1, p, n, \frac{n-1}{p})$-RDS in $G = H \times P = \langle h\rangle \times \langle g\rangle \cong \mathbb{Z}_{n+1} \times \mathbb{Z}_p$ relative to P, where p is an odd prime. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$ be the prime decomposition of n. For $1 \leq i \leq l$, let $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/Q)$ defined by $\sigma_i(\zeta) = \zeta^{p_i}$, where ζ is a primitive $(n+1)p$-th root of unity. Assume that $\bigcap_{i=1}^{l} \langle\sigma_i\rangle \neq \{1\}$ and let $\varphi \in \bigcap_{i=1}^{l} \langle\sigma_i\rangle$. If $\varphi(\zeta) = \zeta^{\alpha}$, then α is a multiplier of R.*

Proof. By (6), we have $RR^{(-1)} = n + \frac{n-1}{p}(G - P)$. Let χ be a character of G such that $\chi(g) = \zeta_p$, then $\chi(R)\overline{\chi(R)} = n$. By Result 3, the prime ideal factorization of (n) in $\mathbb{Z}[\zeta_{(n+1)p}]$ is

$$(n) = (p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}) = \prod_{i=1}^{l} (P_{1,i} \cdots P_{s_i,i})^{r_i},$$

where $s_i = \phi((n+1)p)/f_i$ and $f_i = \mathrm{ord}_{(n+1)p}(p_i)$. By Result 3 (ii) and $\gcd(n, (n+1)p) = 1$, we know that σ_i fixes the prime ideals $P_{j,i}$ for $1 \leq j \leq s_i$. Therefore, φ fixes all prime ideals $P_{j,i}$ for $1 \leq j \leq s_i$ and $1 \leq i \leq l$. By Lemma 2,

$$R^{(\alpha)} = \pm\beta R + Px,$$

where $\beta \in G$ and $x \in \mathbb{Z}[G]$. Let χ_0 be the principal character of G, then

$$n = \chi_0(R^{(\alpha)}) = \chi_0(\pm\beta R + Px) = \pm n + p|x|.$$

It follows that $|x| = 0$ as $\gcd(p, n) = 1$. Next we show that x must be 0. Note that $|R| = |G/P| - 1$ and we can assume that

$$R = \sum_{i=1}^{n} g^{b_i} h^i,$$

where $0 \le b_i \le p-1$. Therefore we have $RP = G - P$. Now

$$\begin{aligned} R^{(\alpha)}R^{(-\alpha)} &= (\beta R + Px)(\beta R + Px)^{(-1)} \\ &= RR^{(-1)} + \beta x^{(-1)}RP^{(-1)} + \beta^{-1}xR^{(-1)}P + p\,xx^{(-1)}P \\ &= n + (\tfrac{n-1}{p} + \beta x^{(-1)} + \beta^{-1}x)G - (\tfrac{n-1}{p} + \beta x^{(-1)} - pxx^{(-1)} + x\beta^{-1})P. \end{aligned}$$

On the other hand, note that $\gcd(\alpha, |G|) = 1$, we have

$$R^{(\alpha)}R^{(-\alpha)} = (RR^{(-1)})^{(\alpha)} = (n + \frac{n-1}{p}(G-P))^{(\alpha)} = n + \frac{n-1}{p}(G-P).$$

Therefore,

$$\begin{cases} \beta x^{(-1)} + \beta^{-1}x & = 0, \\ \beta x^{(-1)} - pxx^{(-1)} + x\beta^{-1} & = 0. \end{cases}$$

From above we have $xx^{(-1)} = 0$, which implies that $x = 0$. It follows that $R^{(\alpha)} = \beta \cdot R$ for some $\beta \in G$. The proof is completed. □

Next we give an example to disprove the existence of an almost p-ary PS by applying Theorem 4.

Example 2. There do not exist almost 7-ary PS with period 23.

Proof. First it can be verified that almost 7-ary PSs with period 23 do not satisfy the conditions of Theorem 3. By Theorem 1, it is equivalent to prove that there do not exist $(23, 7, 22, 3)$-RDS, say R, in $G = \mathbb{Z}_{23} \times \mathbb{Z}_7$ relative to $\mathbb{Z}_7$. It can be checked that 2 is a multiplier of R by Theorem 4. Using MAGMA [3], we compute the orbits of G under the group automorphism $x \mapsto x^2$. The results are in the following table.

We checked that the only possible combination of orbits such that the cardinality is 22 and find it is not a RDS. Then we finish the proof. □

Using similar argument, we get the following result.

Table 1. Orbits of G under $x \mapsto x^2$

Length of orbit	number
1	1
3	2
11	2
33	4

Theorem 5. *There do not exist almost p-ary PSs of period $n+1$, where $p|n-1$ and $n \in \{22, 28, 45, 52\}$.*

Remark 1. The method in Example 2 cannot determine the existence of RDSs if the number of orbits gets larger. Indeed, in this case usually there exist many combinations of the orbits such that the size of the sum of these orbits equal to the cardinality of the RDS, and therefore it is impossible to verify all of them whether is an RDS one by one. For example, when $n = 77$ and $p = 19$ in Theorem 4, it can be verified that 49 is a multiplier of the corresponding $(78, 19, 77, 19)$-RDS. The orbits of $G = \mathbb{Z}_{78} \times \mathbb{Z}_{19}$ under the group automorphism $x \mapsto x^{49}$ is $1^6 3^{36} 6^{228}$, where i^j implies that there are j orbits with length i. It can be computed that the number of the combinations of the orbits such that the size of the sum of them equal to $|R| = 77$ is

$$\sum_{i=0}^{12} \binom{228}{12-i} \left(\binom{36}{1+i}\binom{6}{2} + \binom{36}{i}\binom{6}{5} \right) \approx 2^{75}.$$

In Table 2, we have the following open cases to be determined. They cannot be excluded by using the above method.

Question 1. Whether almost p-ary PSs exist for $n = 50, 76, 77, 94, 99, 100$, where odd prime $p \mid n-1$.

Table 2 in Appendix lists the existence status of p-ary PSs of period $n+1$ for $3 \le n \le 100$ and p is a prime divisor of $n-1$. The question mark "?" in the table is used to denote an undecided case.

4 Almost p-Ary Nearly Perfect Sequences

Let $G, H, P, \mathbf{a}$ be the same as those in the last section. The sequence $\mathbf{a}$ is called an *almost p-ary nearly perfect sequence (NPS) of type I (II)* if the out-of-phase autocorrelation coefficients are all $-1(1)$. Similar to Theorem 1, we have the following result.

Theorem 6. *Let $\mathbf{a} = (0, a_1, a_2, \cdots, a_n)$ be an almost p-ary sequence of period $n+1$, where $a_i = \zeta_p^{b_i}$ and $0 \le b_i \le p-1$ for $1 \le i \le n$. Let $R = \sum_{i=1}^{n} g^{b_i} h^i$. Then*

1. *$\mathbf{a}$ is an almost p-ary NPS of type I if and only if R is an $(n+1, p, n, \frac{n}{p}-1, 0, \frac{n}{p})$ direct product difference set in G relative to H and P.*
2. *$\mathbf{a}$ is an almost p-ary NPS type II if and only if R is an $(n+1, p, n, \frac{n-2}{p}+1, 0, \frac{n-2}{p})$ direct product difference set in G relative to H and P.*

From Theorem 6 we have the following necessary condition for the existence of almost p-ary NPSs.

Corollary 4. (1) *If there exists an almost p-ary NPS of period $n+1$ of type I, then $p \mid n$.* (2) *If there exists an almost p-ary NPS of period $n+1$ of type II, then $p \mid n-2$.*

Next we construct a family of almost p-ary NPSs of type I.

Example 3. Let q be a prime and let p be a prime divisor of $q-1$. Let H be the additive group of the finite field $\mathbb{F}_q$ and let N be the multiplicative group of $\mathbb{F}_q$. Let $G = H \times N \cong \mathbb{Z}_q \times \mathbb{Z}_{q-1}$. Define

$$R = \{(x, x) | x = 0, 1, \cdots, q-2\}.$$

Clearly R is a $(q, q-1, q-1, 0, 0, 1)$ direct product difference set in G relative to H and N (see [11, Example 5.3.2]). By (2),

$$RR^{(-1)} = q + (G - H - N). \tag{7}$$

Let $\rho : G \to G/M$ be the natural epimorphism, where $M \leqslant N$ and $M \cong Z_{\frac{q-1}{p}}$. Then by (7), we have $\rho(R)\rho(R^{(-1)}) = q - N/M + \frac{q-1}{p}(G/M - N/M)$, which follows that $\rho(R)$ is a $(q, p, q-1, \frac{q-1}{p} - 1, 0, \frac{q-1}{p})$-DPDS in $G/M \cong \mathbb{Z}_q \times \mathbb{Z}_p$ relative to $H/M \cong \mathbb{Z}_q$ and $N/M \cong \mathbb{Z}_p$. By Theorem 6 (1), there exists an almost p-ary NPS of type I with period q.

In the following we present results to show almost p-ary NPSs of type I do not exist with certain periods.

Lemma 4. *Let n be an odd integer and $b_i \in \{0, 1, \cdots, n-1\}$ for $1 \leq i \leq n$. Assume that $b_i \neq b_j$ when $i \neq j$, then $|\{b_{i+1} - b_i | i = 1, 2, \cdots, n-1\}| < n-1$ ($b_i - b_j$ is computed modulo n).*

Proof. Let $S = \{b_{i+1} - b_i | i = 1, 2, \cdots, n-1\}$. Clearly $|S| \leq n-1$. Now assume that $|S| = n-1$, then $S = \{1, \ldots, n-1\}$ as $b_i \neq b_j$ for $i \neq j$. Therefore, $\sum_{i=1}^{n-1}(b_{i+1} - b_i) = \sum_{i=1}^{n-1} i \equiv \frac{n(n-1)}{2} \equiv 0 \mod n$ as n is odd. On the other hand, $\sum_{i=1}^{n-1}(b_{i+1} - b_i) = b_n - b_1$. The contradiction arises as $b_i \not\equiv b_j \mod n$. □

Theorem 7. *Let $G = H \times P = \langle h \rangle \times \langle g \rangle = \mathbb{Z}_{n+1} \times \mathbb{Z}_n$ and let R be an $(n+1, n, n, 0, 0, 1)$-DPDS in G relative to H and P. Then R does not exist if n is an odd integer. Therefore, for any odd prime p, there do not exist almost p-ary NPSs of type I with period $p+1$.*

Proof. Since $|R| = |G/P| - 1$ and no elements in P can be represented as the differences of elements in R, we can assume that $R = \sum_{i=1}^{n} g^{b_i} h^i$ and $b_i \in \{0, 1, \ldots, n-1\}$. Similarly, as there are also no elements in H can be represented as the differences of elements in R and $|P| = |R| = n$, we have $\{b_i | i = 1, \ldots, n\} = \{0, 1, \ldots, n-1\}$. Now

$$n + 1 + (G - H - P) = RR^{(-1)} = n + \sum_{t=1}^{n} \sum_{\substack{i=1 \\ i \not\equiv -t \mod (n+1)}}^{n} g^{b_{i+t} - b_i} h^t.$$

It follows that for each $t \neq 0$,

$$\{b_{i+t} - b_i : 1 \leq i \leq n | i \not\equiv -t \mod (n+1)\} = \{1, \ldots, n-1\}.$$

However, by letting $t = 1$ and we see the above equation cannot hold by Lemma 4. We finish the proof. □

By Lemma 1, we have the following nonexistence result.

Theorem 8. *Let q be a prime divisor of $n+1$ such that $q^r \| n+1, q \neq p$. Assume that q is self-conjugate modulo $p \cdot u$ for a divisor u of $n+1$. Let $G = H \times P = \langle h \rangle \times \langle g \rangle \cong \mathbb{Z}_{n+1} \times \mathbb{Z}_p$ and let $K = G/\langle h^u \rangle \cong \mathbb{Z}_u \times \mathbb{Z}_p$. If there exists an almost p-ary NPS of type I with period $n+1$, then*

1. *If $q \nmid |K|$, r is even and $q^{\frac{r}{2}} \leq \frac{n+1}{u}$; and*
2. *If $q \mid |K|$, $q^{\lfloor \frac{r}{2} \rfloor} \leq 2\frac{n+1}{u}$.*

Proof. By Theorem 6, we can assume that there is an $(n+1, p, n, \frac{n}{p} - 1, 0, \frac{n}{p})$-DPDS R in G relative to H and P. Then $RR^{(-1)} = (n+1) - H + \frac{n}{p}(G - P)$. Let $\rho : G \to K$ be the natural epimorphism. Clearly the coefficients of $\rho(R) \in \mathbb{Z}[K]$ lie between 0 and $\frac{n+1}{u}$. Since q is self-conjugate modulo $\exp(K) = p \cdot u$ and for any nonprincipal character χ of K,

$$\chi(\rho(R))\overline{\chi(\rho(R))} = \begin{cases} n+1 & \text{if } \chi \text{ is nonprincipal on both } \rho(P) \text{ and } \rho(H), \\ 1 & \text{if } \chi \text{ is nonprincipal on } \rho(H), \\ 0 & \text{if } \chi \text{ is nonprincipal on } \rho(P). \end{cases}$$

Take $L = \rho(P)$ and $K = \rho(R)$ in Lemma 1, then obviously $q^r | \chi(\rho(R))(\overline{\chi(\rho(R))})$ for $\chi \notin \rho(P)^\perp$ and $q^{r+1} \nmid \chi(\rho(R))(\overline{\chi(\rho(R))})$ for $\chi \notin \rho(H)^\perp \cup \rho(P)^\perp$. If $q \mid |K|$, it is also easy to see $\chi(\rho(R)) \neq 0$ because $\chi(\rho(R))\overline{\chi(\rho(R))} = n+1$ for $\chi \notin \rho(Q)^\perp \cup \rho(P)^\perp$, where Q is the subgroup of K of order q. Now the result follows from Lemma 1. □

Corollary 5. *If there exists a prime divisor q of $n+1$ with $q^{2s+1} \| n+1$ and q is self-conjugate modulo p, then there do not exist almost p-ary NPSs of type I with period $n+1$.*

Proof. Take $u = 1$ in Theorem 8 and note that $|K| = p$. By Theorem 8, the result follows as $q \nmid p$ for every prime divisor q of $n+1$. □

Corollary 6. *Let q be a prime divisor of $n+1$ with q is self-conjugate modulo $(n+1)p$. Assume that $q^r \mid n+1$ for $r \geq 4$ if $q = 2$. Then there do not exist almost p-ary NPSs of type I with period $n+1$.*

For almost p-ary NPSs of type II with period $n+1$, we only find the example with $p = 2$ and $n = 2$, namely $\mathbf{a} = \{0, 1, 1\}$. We have done a computer search for $p = 3$ and $n \in \{2, 5, 8, 11, 14, 17\}$, and however, no example is found. We leave it as the following open question.

Question 2. Do almost p-ary NPSs of type II with period $n+1$ exist?

In Appendix, Table 3 lists the existence status of the almost p-ary NPSs of type I with period $n+1$ for $2 \leq n \leq 100$, where p is a prime divisor of n. The question mark "?" in the table is used to denote an undecided case.

Acknowledgement

The authors are grateful to the invaluable discussions with Professor Alexander Pott which enables this work. They also thank the anonymous referees for their valuable suggestions.

Part of this work was done during the second author's visit at the Otto-von-Guericke- University. He would like to thank the hospitality of the Institute of Algebra and Geometry.

References

1. Arasu, K.T., Ma, S.L.: Abelian difference sets without self-conjugacy. Des. Codes Cryptography 15(3), 223–230 (1998)
2. Beth, T., Jungnickel, D., Lenz, H.: Design theory, 2nd edn. Cambridge University Press, New York (1999)
3. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system I: The user language. Journal of Symbolic Computation 24(3-4), 235–265 (1997), http://www.sciencedirect.com/science/article/B6WM7-45M2XHC-7/2/1774bb42b9fe09d31c90f383c419c7d2
4. Ganley, M.J.: Direct product difference sets. Journal of Combinatorial Theory, Series A 23(3), 321–332 (1977), http://www.sciencedirect.com/science/article/B6WHS-4D7D14S-XS/2/4f3316fe57bc9e1b6b685433891ca6aa
5. Jungnickel, D.: On automorphism groups of divisible designs, II: group invariant generalised conference matrices. Archiv der Mathematik 54(2) (February 1990)
6. Jungnickel, D., Pott, A.: Computational non-existence results for abelian affine difference sets. Congressus Numerantium 68, 91–98 (1989)
7. Jungnickel, D., Pott, A.: Perfect and almost perfect sequences. Discrete Applied Mathematics 95(1-3), 331–359 (1999)
8. Lidl, R., Niederreiter, H.: Finite fields, Encyclopedia of Mathematics and its Applications, 2nd edn., vol. 20. Cambridge University Press, Cambridge (1997)
9. Ma, S.L., Ng, W.S.: On nonexistence of perfect and nearly perfect sequences. Int. J. Inf. Coding Theory 1(1), 15–38 (2009)
10. Passman, D.S.: The algebraic structure of group rings. John Wiley & Sons, New York (1977)
11. Pott, A.: Finite Geometry and Character Theory. LNM, vol. 1601. Springer, Heidelberg (1995)
12. Schmidt, B.: Characters and cyclotomic fields in finite geometry. LNM, vol. 1797. Springer, Berlin (2002)
13. Stanton, R., Mullin, R.C.: On the nonexistence of a class of circulant balanced weighing matrices. SIAM Journal on Applied Mathematics 30, 98–102 (1976)

Appendix

Table 2. Existence Status of Perfect Sequences

n	p	Existence Status	n	p	Existence Status
3	2	not exist by Theorem 2	4	3	exist by Example 1
5	2	not exist by Theorem 2	6	5	not exist by Corollary 3 with q=2
7	2	not exist by Theorem 2	7	3	exist by Example 1
8	7	exist by Example 1 2	9	2	not exist by Theorem 2
10	3	not exist by Corollary 3 with q=2	11	2	not exist by Theorem 2
11	5	exist by Example 1	12	11	not exist by Result 5
13	2	not exist by Theorem 2	13	3	exist by Example 1
14	13	not exist by Corollary 3 with q=2	15	2	not exist by Theorem 2
15	7	not exist by Corollary 3 with q=3	16	3	exist by Example 1
16	5	exist by Example 1	17	2	not exist by Theorem 2
18	17	not exist by Corollary 3 with q=2	19	2	not exist by Theorem 2
19	3	exist by Example 1	20	19	not exist by Result 5
21	2	not exist by Theorem 2	21	5	not exist by Corollary 3 with q=3
22	3	not exist by Corollary 3 with q=2	22	7	not exist by Theorem 5
23	2	not exist by Theorem 2	23	11	exist by Example 1
24	23	not exist by Result 5	25	2	not exist by Theorem 2
25	3	exist by Example 1	26	5	not exist by Corollary 3 with q=2
27	2	not exist by Theorem 2	27	13	exist by Example 1
28	3	not exist by Theorem 5	29	2	not exist by Theorem 2
29	7	exist by Example 1	30	29	not exist by Corollary 3 with q=2
31	2	not exist by Theorem 2	31	3	exist by Example 1
31	5	exist by Example 1	32	31	exist by Example 1
33	2	not exist by Theorem 2	34	3	not exist by Corollary 3 with q=2
34	11	not exist by Corollary 3 with q=2	35	2	not exist by Theorem 2
35	17	not exist by Corollary 3 with q=5	36	5	not exist by Corollary 2 with q=2
36	7	not exist by Corollary 2 with q=3	37	2	not exist by Theorem 2
37	3	exist by Example 1	38	37	not exist by Corollary 3 with q=2
39	2	not exist by Theorem 2	39	19	not exist by Corollary 3 with q=3
40	3	not exist by Corollary 3 with q=2	40	13	not exist by Corollary 3 with q=2
41	2	not exist by Theorem 2	41	5	exist by Example 1
42	41	not exist by Corollary 3 with q=2	43	2	not exist by Theorem 2
43	3	exist by Example 1	43	7	exist by Example 1
44	43	not exist by Result 5	45	2	not exist by Theorem 2
45	11	not exist by Theorem 5	46	3	not exist by Corollary 3 with q=2
46	5	not exist by Corollary 3 with q=2	47	2	not exist by Theorem 2
47	23	exist by Example 1			
48	47	not exist by Result 5	49	2	not exist by Theorem 2
49	3	exist by Example 1	50	7	?
51	2	not exist by Theorem 2	51	5	not exist by Corollary 3 with q=3
52	3	not exist by Theorem 5	52	17	not exist by Corollary 3 with q=13
53	2	not exist by Theorem 2	53	13	exist by Example 1

Table 2. (*continued*)

54	53	not exist by Corollary 3 with q=2	55	2	not exist by Theorem 2
55	3	not exist by Corollary 3 with q=5	56	5	not exist by Corollary 3 with q=2
56	11	not exist by Corollary 3 with q=2	57	2	not exist by Theorem 2
57	7	not exist by Corollary 3 with q=3	58	3	not exist by Corollary 3 with q=2
58	19	not exist by Corollary 3 with q=2	59	2	not exist by Theorem 2
59	29	exist by Example 1	60	59	not exist by Result 5
61	2	not exist by Theorem 2	61	3	exist by Example 1
61	5	exist by Example 1	62	61	not exist by Corollary 3 with q=2
63	2	not exist by Theorem 2	63	31	not exist by Corollary 3 with q=3
64	3	exist by Example 1	64	7	exist by Example 1
65	2	not exist by Theorem 2	66	5	not exist by Corollary 3 with q=2
66	13	not exist by Corollary 3 with q=2	67	2	not exist by Theorem 2
67	3	exist by Example 1	67	11	exist by Example 1
68	67	not exist by Result 5	69	2	not exist by Theorem 2
69	17	not exist by Corollary 3 with q=3	70	3	not exist by Corollary 3 with q=2
70	23	not exist by Corollary 3 with q=5	71	2	not exist by Theorem 2
71	5	exist by Example 1	71	7	exist by Example 1
72	71	not exist by Result 5	73	2	not exist by Theorem 2
73	3	exist by Example 1	74	73	not exist by Result 5
75	2	not exist by Theorem 2	75	37	not exist by Corollary 3 with q=3
76	3	?	77	2	not exist by Theorem 2
77	19	?	78	7	not exist by Corollary 3 with q=3
78	11	not exist by Corollary 3 with q=2	79	2	not exist by Theorem 2
79	39	exist by Example 1	80	79	not exist by Result 5
81	2	not exist by Theorem 2	81	5	exist by Example 1
82	3	not exist by Corollary 3 with q=2	83	2	not exist by Theorem 2
83	41	exist by Example 1	84	83	not exist by Result 5
85	2	not exist by Theorem 2	85	3	not exist by Corollary 3 with q=5
85	7	not exist by Corollary 3 with q=5	86	5	not exist by Corollary 3 with q=2
85	17	not exist by Corollary 3 with q=2	87	2	not exist by Theorem 2
87	43	not exist by Corollary 3 with q=3	88	3	not exist by Corollary 3 with q=2
88	29	not exist by Corollary 3 with q=2	89	2	not exist by Theorem 2
89	11	exist by Example 1	90	89	not exist by Corollary 3 with q=3
91	2	not exist by Theorem 2	91	3	exist by Example 1
91	5	exist by Example 1	92	91	not exist by Result 5
93	2	not exist by Theorem 2	93	23	not exist by Corollary 3 with q=7
94	3	not exist by Corollary 3 with q=2	94	31	?
95	2	not exist by Theorem 2	95	47	not exist by Corollary 3 with q=5
96	5	not exist by Corollary 3 with q=2	96	19	not exist by Corollary 3 with q=2
97	2	not exist by Theorem 2	97	3	exist by Example 1
98	97	not exist by Corollary 3 with q=2	99	2	not exist by Theorem 2
99	7	?	100	3	?
100	11	?			

Table 3. Existence Status of Nearly Perfect Sequences

n	p	Existence Status	n	p	Existence Status
2	2	exist by example 3	3	3	not exist by Theorem 7 with q=3
4	2	exist by example 3	5	5	not exist by Corollary 5 with q=2
6	2	exist by example 3	6	3	exist by example 3
7	7	not exist by Theorem 7 with q=7	8	2	not exist by Corollary 6 with q=3
9	3	not exist by Corollary 5 with q=2	10	2	exist by example 3
10	5	exist by example 3	11	11	not exist by Theorem 7 with q=11
12	2	exist by example 3	12	3	exist by example 3
13	13	not exist by Corollary 5 with q=2	14	2	not exist by Corollary 5 with q=3
14	7	not exist by Corollary 5 with q=3	15	3	not exist by Corollary 6 with q=2
15	5	not exist by Corollary 6 with q=2	16	2	exist by example 3
17	17	not exist by Corollary 5 with q=2	18	2	exist by example 3
18	3	exist by example 3	19	19	not exist by Theorem 7 with q=19
20	2	not exist by Corollary 5 with q=3	20	5	not exist by Corollary 5 with q=3
21	3	not exist by Corollary 5 with q=2	21	7	?
22	2	exist by example 3	22	11	exist by example 3
23	23	not exist by Theorem 7 with q=23	24	2	not exist by Corollary 6 with q=5
24	3	not exist by Corollary 6 with q=5	25	5	not exist by Corollary 5 with q=2
26	2	not exist by Corollary 5 with q=3	26	13	?
27	3	?	28	2	exist by example 3
28	7	exist by example 3	29	29	not exist by Corollary 5 with q=2
30	2	exist by example 3	30	3	exist by example 3
30	5	exist by example 3	31	31	not exist by Theorem 7 with q=31
32	2	not exist by Corollary 5 with q=3	33	3	not exist by Corollary 5 with q=2
33	11	not exist by Corollary 5 with q=2	34	2	not exist by Corollary 5 with q=5
	17	not exist by Corollary 5 with q=5	35	5	?
35	7	not exist by Corollary 6 with q=3	36	2	exist by example 3
36	3	exist by example 3	37	37	not exist by Theorem 7 with q=37
38	2	not exist by Corollary 5 with q=3	38	19	not exist by Corollary 5 with q=3
39	3	not exist by Corollary 5 with q=2	39	13	not exist by Corollary 5 with q=2
40	2	exist by example 3	40	5	exist by example 3
41	41	not exist by Corollary 5 with q=2	42	2	exist by example 3
42	3	exist by example 3	42	7	exist by example 3
43	43	not exist by Theorem 7 with q=43	44	2	not exist by Corollary 5 with q=5
44	11	?	45	3	not exist by Corollary 5 with q=2
45	5	not exist by Corollary 5 with q=2	46	2	exist by example 3
46	23	exist by example 3	47	47	not exist by Theorem 7 with q=47
48	2	not exist by Corollary 6 with q=7	48	3	not exist by Corollary 6 with q=7
49	7	not exist by Corollary 6 with q=5	50	2	not exist by Corollary 5 with q=3
50	5	not exist by Corollary 5 with q=3	51	3	?
51	17	not exist by Corollary 5 with q=13	52	2	exist by example 3
52	13	exist by example 3	53	53	not exist by Corollary 5 with q=2

Table 3. (*continued*)

54	2	not exist by Corollary 5 with q=5	54	3	not exist by Corollary 5 with q=5
55	5	not exist by Corollary 5 with q=2	55	11	not exist by Corollary 5 with q=2
56	2	not exist by Corollary 5 with q=3	56	7	not exist by Corollary 5 with q=3
57	3	not exist by Corollary 5 with q=2	57	19	not exist by Corollary 5 with q=2
58	2	exist by example 3	58	29	exist by example 3
59	59	not exist by Theorem 7 with q=59	60	2	exist by example 3
60	3	exist by example 3	60	5	exist by example 3
61	61	not exist by Corollary 5 with q=2	62	2	not exist by Corollary 5 with q=7
62	31	not exist by Corollary 6 with q=3	63	3	not exist by Corollary 6 with q=2
63	7	?	64	2	not exist by Corollary 5 with q=5
65	5	not exist by Corollary 5 with q=2	65	13	not exist by Corollary 5 with q=2
66	2	exist by example 3	66	2	exist by example 3
66	11	exist by example 3	67	67	not exist by Theorem 7 with q=67
68	2	not exist by Corollary 5 with q=3	68	17	not exist by Corollary 5 with q=3
69	3	not exist by Corollary 5 with q=2	69	23	not exist by Corollary 5 with q=5
70	2	exist by example 3	70	5	exist by example 3
70	7	exist by example 3	71	71	not exist by Theorem 7 with q=71
72	2	exist by example 3	72	3	exist by example 3
73	73	not exist by Theorem 7 with q=73	74	2	not exist by Corollary 5 with q=3
74	37	not exist by Corollary 5 with q=3	75	3	?
75	5	not exist by Corollary 5 with q=15	76	2	not exist by Corollary 5 with q=7
76	19	?	77	7	?
77	11	not exist by Corollary 5 with q=2	78	2	exist by example 3
78	39	exist by example 3	79	79	not exist by Theorem 7 with q=79
80	2	not exist by Corollary 6 with q=3	80	5	not exist by Corollary 6 with q=3
81	3	not exist by Corollary 6 with q=2	82	2	exist by example 3
82	41	exist by example 3	83	83	not exist by Theorem 7 with q=83
84	2	not exist by Corollary 5 with q=5	84	3	not exist by Corollary 5 with q=5
84	7	not exist by Corollary 5 with q=5	85	5	not exist by Corollary 5 with q=2
85	17	not exist by Corollary 5 with q=2	86	2	not exist by Corollary 5 with q=3
86	43	not exist by Corollary 5 with q=3	87	3	not exist by Corollary 5 with q=11
87	29	not exist by Corollary 5 with q=11	88	2	exist by example 3
88	11	exist by example 3	89	89	not exist by Corollary 5 with q=5
90	2	exist by example 3	90	3	exist by example 3
90	5	exist by example 3	91	91	not exist by Theorem 7 with q=91
92	2	not exist by Corollary 5 with q=3	92	23	?
93	3	not exist by Corollary 5 with q=2	93	31	?
94	2	not exist by Corollary 5 with q=5	94	47	not exist by Corollary 5 with q=5
95	5	not exist by Corollary 5 with q=2	95	19	not exist by Corollary 5 with q=2
96	2	exist by example 3	96	3	exist by example 3
97	97	not exist by Corollary 5 with q=2	98	2	not exist by Corollary 5 with q=11
98	7	?	99	3	not exist by Corollary 6 with q=5
99	11	?	100	2	exist by example 3

Sequences, Bent Functions and Jacobsthal Sums

Tor Helleseth and Alexander Kholosha

The Selmer Center
Department of Informatics, University of Bergen
P.O. Box 7800, N-5020 Bergen, Norway
{Tor.Helleseth,Alexander.Kholosha}@uib.no

Abstract. The p-ary function $f(x)$ mapping $\mathrm{GF}(p^{4k})$ to $\mathrm{GF}(p)$ and given by $f(x) = \mathrm{Tr}_{4k}\left(ax^d + bx^2\right)$ with $a, b \in \mathrm{GF}(p^{4k})$ and $d = p^{3k} + p^{2k} - p^k + 1$ is studied with the respect to its exponential sum. In the case when either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$ with $b \neq 0$, this sum is shown to be three-valued and the values are determined. For the remaining cases, the value of the exponential sum is expressed using Jacobsthal sums of order $p^k + 1$. Finding the values and the distribution of those sums is a long-lasting open problem.

Keywords: Cyclotomic number, Jacobsthal sum, p-ary bent function, polynomial over finite field, Walsh transform.

1 Introduction

Niho in [1, Theorem 3-7] and Helleseth in [2] studied the cross correlation between two binary m-sequences that differ by the decimation $2^{3k} - 2^{2k} + 2^k + 1$. They proved that the cross-correlation function is four-valued and found the distribution. In [3], Helleseth and Kholosha constructed a p-ary weakly regular binomial bent function that has an exponent of this type in its first term (the second term is a square). This gave the infinite class of nonquadratic generalized bent functions built over the fields of an arbitrary odd characteristic. In this paper, we take $n = 4k$, an odd prime p and examine p-ary functions having the form $f(x) = \mathrm{Tr}_n\left(ax^d + bx^2\right)$ with $a, b, x \in \mathrm{GF}(p^n)$ and $d = p^{3k} + p^{2k} - p^k + 1$. Functions of this type with a and b being nonzero belong to the class of *binomials*. Note that d is cyclotomic equivalent to the Niho exponent (with 2 changed to p) and that $\gcd(d, p^n - 1) = 2$ since $d = (p^{2k} - 1)(p^k + 1) + 2$.

Given a function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$, the direct and inverse *Walsh transform* operations on f are defined at a point by the following respective identities:

$$S_f(y) = \sum_{x \in \mathrm{GF}(p^n)} \omega^{f(x) - \mathrm{Tr}_n(yx)} \quad \text{and} \quad \omega^{f(x)} = \frac{1}{p^n} \sum_{y \in \mathrm{GF}(p^n)} S_f(y) \omega^{\mathrm{Tr}_n(yx)}$$

* This work was supported by the Norwegian Research Council and partially by the grant NIL-I-004 from Iceland, Liechtenstein and Norway through the EEA and Norwegian Financial Mechanisms.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 416–429, 2010.

where $\mathrm{Tr}_n() : \mathrm{GF}(p^n) \to \mathrm{GF}(p)$ denotes the absolute trace function, $\omega = e^{\frac{2\pi i}{p}}$ is the complex primitive p^{th} root of unity and elements of $\mathrm{GF}(p)$ are considered as integers modulo p.

According to [4], $f(x)$ is called a *p-ary bent function* (or *generalized bent function*) if all its Walsh coefficients satisfy $|S_f(y)|^2 = p^n$. A bent function $f(x)$ is called *regular* (see [4, Definition 3] and [5, p. 576]) if for every $y \in \mathrm{GF}(p^n)$ the normalized Walsh coefficient $p^{-n/2}S_f(y)$ is equal to a complex p^{th} root of unity, i.e., $p^{-n/2}S_f(y) = \omega^{f^*(y)}$ for some function f^* mapping $\mathrm{GF}(p^n)$ into $\mathrm{GF}(p)$. A bent function $f(x)$ is called *weakly regular* if there exists a complex u having unit magnitude such that $up^{-n/2}S_f(y) = \omega^{f^*(y)}$ for all $y \in \mathrm{GF}(p^n)$. Recently, weakly regular bent functions were shown to be useful for constructing certain combinatorial objects such as partial difference sets, strongly regular graphs and association schemes (see [6,7]). This justifies why the classes of (weakly) regular bent functions are of independent interest. For a comprehensive reference on monomial and quadratic p-ary bent functions we refer reader to [8].

Taking $a = b = 1$, results in a weakly regular bent function and the exact value of its Walsh transform coefficients (and value distribution) can be found.

Theorem 1 ([3]). *Let $n = 4k$. Then p-ary function $f(x)$ mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ and given by*

$$f(x) = \mathrm{Tr}_n\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)$$

is a weakly regular bent function. Moreover, for $y \in \mathrm{GF}(p^n)$ the corresponding Walsh transform coefficient of $f(x)$ is equal to

$$S_f(y) = -p^{2k}\omega^{\mathrm{Tr}_k(x_0)/4} \ ,$$

where x_0 is a unique root in $\mathrm{GF}(p^k)$ of the polynomial

$$y^{p^{2k}+1} + (y^2+X)^{(p^{2k}+1)/2} + y^{p^k(p^{2k}+1)} + (y^2+X)^{p^k(p^{2k}+1)/2} \ .$$

In particular, if $y^2 \in \mathrm{GF}(p^{2k})$ then $x_0 = -\mathrm{Tr}_k^{2k}(y^2)$. Also, every value $-p^{2k}\omega^i$ with $i = \{1, \ldots, p-1\}$ occurs $p^{2k-1}(p^{2k}+1)$ times in the Walsh spectrum of $f(x)$ and $-p^{2k}$ occurs $(p^{2k-1}-1)(p^{2k}+1)+1$ times.

The general case when $a, b \in \mathrm{GF}(p^n)$ is much more complicated. It seems to be hard to find the Walsh transform coefficients of $f(x)$ at an arbitrary point, so here we calculate the exponential sum of $f(x)$, i.e., $S_f(0)$. This is equal to the cross-correlation function between two sequences of length $(p^n-1)/2$ obtained by the decimation of an m-sequence by d and 2 or can be seen as a codeword weight in the corresponding p-ary linear code. We relate this value to the number of zeros, a particular polynomial has in a cyclic subgroup of order $p^{2k}+1$ of the multiplicative group of $\mathrm{GF}(p^n)$. Moreover, we show that if either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$ with $b \neq 0$ then the exponential sum of $f(x)$ is three-valued. Some steps towards finding the distribution of these values are made but the exact distribution remains an open problem. For the remaining

options for choosing (a, b), we show that $S_f(0)$ can be expressed using the Jacobsthal sum of order $p^k + 1$ which has the number of possible values growing with k. In Sections 2 and 3, we calculate the cyclotomic numbers of order $p^k + 1$ in $\mathrm{GF}(p^{2k})^*$ and prove the estimate of Artin-Hasse type for the Jacobsthal sums of order $p^k + 1$. These are used to find few important properties of $S_f(0)$.

2 Cyclotomic Numbers of Order $p^k + 1$

Let ν be a primitive element of $\mathrm{GF}(p^{2k})$ and let C_t $(t = 0, \ldots, p^k)$ denote the *cyclotomic classes* of order $p^k + 1$ in $\mathrm{GF}(p^{2k})^*$, i.e., $C_t = \{\nu^{(p^k+1)i+t} \mid i = 0, \ldots, p^k - 2\}$. The number of elements $x \in C_i$ such that $x + 1 \in C_j$ is called the *cyclotomic number* and denoted (i, j). Since $-1 \in C_0$ in our case, we can also take $x - 1$ in the definition of the cyclotomic numbers. Note that since the cyclotomic numbers of order $p^k + 1$ are *uniform* (see [9]), their values can easily be determined. Nevertheless, in the following lemma, we give a straightforward proof using the technique suggested for the binary case in [10, Sec. 5].

Lemma 1. *For any $i, j = 0, \ldots, p^k$, the cyclotomic numbers of order $p^k + 1$ in $\mathrm{GF}(p^{2k})$ are*

$$(i, j) = \begin{cases} 1, & \text{if} \quad i \neq j \text{ and } ij \neq 0 \\ p^k - 2, & \text{if} \quad i = j = 0 \\ 0, & \text{otherwise} \ . \end{cases}$$

Proof. Note that $\mathrm{GF}(p^{2k})^* = \bigcup_{t=0}^{p^k} C_t$ and $-1 = \nu^{(p^{2k}-1)/2} \in C_0$.

$$\begin{aligned} p^{2k}(i, j) &= \sum_{z \in \mathrm{GF}(p^{2k})} \sum_{x \in C_i} \sum_{y \in C_j} \omega^{\mathrm{Tr}_{2k}(z(x-y-1))} \\ &= (p^k - 1)^2 + \sum_{t=0}^{p^k} \sum_{z \in C_t} \omega^{-\mathrm{Tr}_{2k}(z)} \sum_{x \in C_i} \omega^{\mathrm{Tr}_{2k}(zx)} \sum_{y \in C_j} \omega^{-\mathrm{Tr}_{2k}(zy)} \\ &= (p^k - 1)^2 + \sum_{t=0}^{p^k} P_t P_{t+i} P_{t+j} \ , \end{aligned}$$

where indices of P_t are calculated modulo $p^k + 1$ and

$$\begin{aligned} P_t \ &= \sum_{x \in C_t} \omega^{\mathrm{Tr}_{2k}(x)} = \frac{1}{p^k + 1} \sum_{z \in \mathrm{GF}(p^{2k})^*} \omega^{\mathrm{Tr}_{2k}\left(z^{p^k+1} \nu^t\right)} \\ &\overset{(*)}{=} \begin{cases} p^k - 1, \text{ if} \quad t = (p^k + 1)/2 \\ -1, \quad \text{otherwise} \end{cases} \end{aligned}$$

for $t = 0, \ldots, p^k$ and $(*)$ follows from [8, Lemma 2 (iii)]. Therefore, if $i \neq j$ and $ij \neq 0$ then

$$(i, j) = p^{-2k} \left((p^k - 1)^2 + 3(p^k - 1) - (p^k - 2)\right) = 1 \ .$$

Similarly, it is easy to see that $(0, 0) = p^k - 2$ and in the rest of the cases, $(i, j) = 0$. □

3 Estimate of the Jacobsthal Sums of Order $p^k + 1$

Following [11, Definition 5.49], for any $a \in \mathrm{GF}(q)^*$, define a *Jacobsthal sum* of order n as

$$H_n(a) = \sum_{x \in \mathrm{GF}(q)} \eta(x^{n+1} + ax) \ ,$$

where $\eta(\cdot)$ is the quadratic character of $\mathrm{GF}(q)$ extended by setting $\eta(0) = 0$. Define also a companion sum

$$I_n(a) = \sum_{x \in \mathrm{GF}(q)^*} \eta(x^n + a) \ .$$

It is well known (see, e.g., [11, Theorem 5.50]) that $I_{2n}(a) = I_n(a) + H_n(a)$.

In our case, $q = p^{2k}$ and we consider $n = p^k + 1$. If $a \in \mathrm{GF}(p^k)$ then, obviously, $I_{p^k+1}(a) = I_{2(p^k+1)}(a) = p^{2k} - 1$ and $H_{p^k+1}(a) = 0$. Now take any $a \in \mathrm{GF}(p^{2k}) \setminus \mathrm{GF}(p^k)$ and assume $a^{-1} \in C_i$. Then $i \neq 0$ since $C_0 = \mathrm{GF}(p^k)^*$, and we can compute

$$\begin{aligned} I_{p^k+1}(a) &= \eta(a) \sum_{x \in \mathrm{GF}(p^{2k})^*} \eta\big(x^{p^k+1}/a + 1\big) \\ &= (-1)^i (p^k + 1) \left(\sum_{j=0}^{(p^k-1)/2} (i, 2j) - \sum_{j=0}^{(p^k-1)/2} (i, 2j+1) \right) \\ &\overset{(*)}{=} (p^k + 1) \begin{cases} \frac{p^k+1}{2} - 2 - \frac{p^k+1}{2} = -2, & \text{if } i \text{ is even} \\ -\frac{p^k+1}{2} + 1 + \frac{p^k+1}{2} - 1 = 0, & \text{if } i \text{ is odd} \end{cases} \\ &= -(p^k + 1)(\eta(a) + 1) \ , \end{aligned} \tag{1}$$

where $(*)$ follows from Lemma 1. Note that $\eta(a) = (-1)^{p^k+1-i} = (-1)^i$ since $a \in C_{p^k+1-i}$. Calculating $H_{p^k+1}(a)$ (that is equivalent to calculating $I_{2(p^k+1)}(a)$) is not that easy. In the following theorem, we provide an estimate. Note that this estimate is much better than the one in [11, p. 233] which becomes trivial if $n = p^k + 1$. Computations show that the bound found in Theorem 2 is achievable.

Theorem 2. *For any $a \in \mathrm{GF}(p^{2k}) \setminus \mathrm{GF}(p^k)$,*

$$|H_{p^k+1}(a)| \leq 2p^{k/2}(p^k + 1) \ .$$

Proof. Since $I_{2(p^k+1)}(a) = I_{p^k+1}(a) + H_{p^k+1}(a)$ and the exact value of $I_{p^k+1}(a)$ was found in (1), we need to estimate $I_{2(p^k+1)}(a)$. Raising elements of $\mathrm{GF}(p^{2k})^*$ to the power of $p^k + 1$ defines a $(p^k + 1)$-to-1 mapping onto $\mathrm{GF}(p^k)^*$. Thus, denoting $y = x^{p^k+1}$, we obtain from the definition

$$\frac{I_{2(p^k+1)}(a)}{p^k + 1} + \eta(a) = \sum_{y \in \mathrm{GF}(p^k)} \eta(y^2 + a) = N(a) - p^k \ ,$$

where $N(a)$ is the number of pairs $(y,t) \in \mathrm{GF}(p^k) \times \mathrm{GF}(p^{2k})^*$ that satisfy $y^2+a=t^2$.

If μ is a primitive element of $\mathrm{GF}(p^k)$ then $\mu^{1/2} \in \mathrm{GF}(p^{2k}) \setminus \mathrm{GF}(p^k)$ and any element $x \in \mathrm{GF}(p^{2k})$ has a unique representation as $x = x_0 + 2\mu^{1/2}x_1$ with $x_0, x_1 \in \mathrm{GF}(p^k)$. This way, assume $a = a_0 + 2\mu^{1/2}a_1$ and $t = t_0 + 2\mu^{1/2}t_1$. Thus, $y^2+a=t^2$ is equivalent to $y^2+a_0 = t_0^2 + 4\mu t_1^2$ with $a_1 = 2t_0t_1$. Note that $t_1 \neq 0$ since in the opposite case, $t \in \mathrm{GF}(p^k)$ that leads to $a \in \mathrm{GF}(p^k)$. Combining the latter equations we obtain $y^2t_0^2 + a_0t_0^2 = t_0^4 + \mu a_1^2$. Therefore, $N(a)$ is equal to the number of pairs $(y,z) \in \mathrm{GF}(p^k) \times \mathrm{GF}(p^k)^*$ that satisfy

$$y^2z^2 + Az^2 = z^4 + C \ ,$$

where $C = \mu a_1^2 \neq 0$ and $A = a_0$, both in $\mathrm{GF}(p^k)$.

Now we can calculate

$$\begin{aligned}
2p^k\left(N(a)-p^k+1\right) &= 2 \sum_{y,z,l \in \mathrm{GF}(p^k);\, zl \neq 0} \omega^{\mathrm{Tr}_k\left(l(z^4-Az^2+C)-ly^2z^2\right)} \\
&= \sum_{zl\neq 0} \omega^{\mathrm{Tr}_k\left(l^2(z^4-Az^2+C)\right)} \sum_y \omega^{-\mathrm{Tr}_k\left(l^2z^2y^2\right)} \\
&\quad + \sum_{zl\neq 0} \omega^{\mathrm{Tr}_k\left(\mu l^2(z^4-Az^2+C)\right)} \sum_y \omega^{-\mathrm{Tr}_k\left(\mu l^2z^2y^2\right)} \\
&= \sum_y \omega^{-\mathrm{Tr}_k\left(y^2\right)} \left(\sum_{z\neq 0,\, l} \omega^{\mathrm{Tr}_k\left(l^2(z^4-Az^2+C)\right)} - \sum_{z\neq 0,\, l} \omega^{\mathrm{Tr}_k\left(\mu l^2(z^4-Az^2+C)\right)} \right) \\
&= 2\sum_y \omega^{-\mathrm{Tr}_k\left(y^2\right)} \sum_{z^5-Az^3+Cz\neq 0,\, l} \omega^{\mathrm{Tr}_k\left(l^2(z^4-Az^2+C)\right)} \\
&= 2p^k s\zeta(-1) \sum_{z\neq 0} \zeta(z^4-Az^2+C) \\
&= 2p^k \sum_{z\neq 0} (1+\zeta(z))\zeta(z^2-Az+C) \\
&= 2p^k \sum_z \zeta(z^2-Az+C) - \zeta(C) + \sum_z \zeta(z^3-Az^2+Cz) \\
&\overset{(*)}{=} 2p^k \sum_z \zeta(z^3-Az^2+Cz) \ ,
\end{aligned}$$

where $\zeta(\cdot)$ is the quadratic character of $\mathrm{GF}(p^k)$ extended by setting $\zeta(0)=0$; $s=(-1)^k$ if $p \equiv 3 \pmod 4$ and $s=1$ otherwise; and $(*)$ follows from [11, Theorem 5.48] since z^2-Az+C can not have both roots in $\mathrm{GF}(p^k)$ equal (C is a nonsquare in $\mathrm{GF}(p^k)$). Also note that $s\zeta(-1) \equiv 1$. Thus,

$$\begin{aligned}
\frac{I_{2(p^k+1)}(a)}{p^k+1} &= \sum_{z\in\mathrm{GF}(p^k)} \zeta(z^3-a_0z^2+\mu a_1^2 z) - \eta(a) - 1 = N - p^k - \eta(a) - 1 \\
\frac{H_{p^k+1}(a)}{p^k+1} &= N - p^k \ ,
\end{aligned}$$

where N denotes the number of points on the elliptic curve $f^2 = z^3 - Az^2 + Cz$ over $\mathrm{GF}(p^k)$ *excluding* the point at infinity. It remains to use Hasse theorem [12, p. 138] giving $|N - p^k| \leq 2p^{k/2}$ to obtain the claimed result (also, [11, Theorem 5.41] can be used). □

4 Calculating the Exponential Sum of $f(x)$

In this section, we consider the function $f(x)$ with arbitrary coefficients $a, b \in \mathrm{GF}(p^n)$. If n is even, let U denote a cyclic subgroup of order $p^{n/2}+1$ of the multiplicative group of $\mathrm{GF}(p^n)$ (generated by $\xi^{p^{n/2}-1}$, where ξ is a primitive element of $\mathrm{GF}(p^n)$).

Theorem 3. *Let $n = 4k$. For any $a, b \in \mathrm{GF}(p^n)$, define the following p-ary function mapping $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$*

$$f(x) = \mathrm{Tr}_n\left(ax^{p^{3k}+p^{2k}-p^k+1} + bx^2\right) \ .$$

Then the Walsh transform coefficient of $f(x)$ evaluated at point zero is equal to

$$S_f(0) = p^{2k}(2N(a,b) - 1) \ ,$$

where $2N(a,b)$ is the number of zeros in U of the polynomial

$$L(X) = b^{p^{2k}}X + aX^{p^k} + bX^{p^{2k}} + a^{p^{2k}}X^{p^{3k}} \ . \tag{2}$$

Proof. Let ξ be a primitive element of $\mathrm{GF}(p^n)$ and also denote $d = p^{3k} + p^{2k} - p^k + 1$. If we let $x = \xi^j y^{p^{2k}+1}$ for $j = 0, \ldots, p^{2k}$ and y running through $\mathrm{GF}(p^n)^*$ then x will run through $\mathrm{GF}(p^n)^*$ in total $p^{2k}+1$ times. Also note that $d - 2 = (p^{2k}-1)(p^k+1)$ and thus, $d(p^{2k}+1) \equiv 2(p^{2k}+1) \pmod{p^n - 1}$. Therefore, the Walsh transform coefficient of $f(x)$ evaluated at point zero is equal to

$$\begin{aligned}
S_f(0) - 1 &= \sum_{x \in \mathrm{GF}(p^n)^*} \omega^{\mathrm{Tr}_n\left(ax^{p^{3k}+p^{2k}-p^k+1}+bx^2\right)} \\
&= \frac{1}{p^{2k}+1} \sum_{j=0}^{p^{2k}} \sum_{y \in \mathrm{GF}(p^n)^*} \omega^{\mathrm{Tr}_n\left(a\xi^{dj}y^{2(p^{2k}+1)}+b\xi^{2j}y^{2(p^{2k}+1)}\right)} \\
&= \sum_{j=0}^{p^{2k}} \sum_{z \in \mathrm{GF}(p^{2k})^*} \omega^{\mathrm{Tr}_n\left(\left(a\xi^{dj}+b\xi^{2j}\right)z^2\right)} \\
&= \sum_{j=0}^{p^{2k}} \sum_{z \in \mathrm{GF}(p^{2k})^*} \omega^{\mathrm{Tr}_{2k}\left(\xi^{(p^{2k}+1)j}L(\xi^{(p^{2k}-1)j})z^2\right)} \\
&\overset{(*)}{=} \sum_{j=0}^{p^{2k}} I\left(L\left(\xi^{(p^{2k}-1)j}\right) \neq 0\right)\left(-sp^k\eta\left(\xi^{(p^{2k}+1)j}L\left(\xi^{(p^{2k}-1)j}\right)\right) - 1\right) \\
&\quad + 2N(a,b)(p^{2k}-1) \ ,
\end{aligned}$$

where $z = y^{p^{2k}+1} \in \mathrm{GF}(p^{2k})^*$ is a $(p^{2k}+1)$-to-1 mapping of $\mathrm{GF}(p^n)^*$, $(*)$ is obtained by [8, Corollary 3], $s = (-1)^k$ if $p \equiv 3 \pmod 4$ and $s = 1$ otherwise, $I(\cdot)$ is the indicator function, $\eta(\cdot)$ is the quadratic character of $\mathrm{GF}(p^{2k})$ and since

$$\begin{aligned}
&\mathrm{Tr}_{2k}^n\left(a\xi^{dj} + b\xi^{2j}\right) = a\xi^{dj} + b\xi^{2j} + a^{p^{2k}}\xi^{djp^{2k}} + b^{p^{2k}}\xi^{2jp^{2k}} \\
&= \xi^{(p^{2k}+1)j}\left(a\xi^{p^k(p^{2k}-1)j} + b\xi^{-(p^{2k}-1)j} + a^{p^{2k}}\xi^{-p^k(p^{2k}-1)j} + b^{p^{2k}}\xi^{(p^{2k}-1)j}\right) \\
&= \xi^{(p^{2k}+1)j}L\left(\xi^{(p^{2k}-1)j}\right).
\end{aligned}$$

also noting that $\xi^{-(p^{2k}-1)j} = \xi^{p^{2k}(p^{2k}-1)j}$.

Further, note that for any $j = 0, \ldots, \frac{p^{2k}-1}{2}$ with $L\left(\xi^{(p^{2k}-1)j}\right) \neq 0$ we have

$$\eta\left(\xi^{(p^{2k}+1)(j+(p^{2k}+1)/2)}L\left(\xi^{(p^{2k}-1)(j+(p^{2k}+1)/2)}\right)\right) = -\eta\left(\xi^{(p^{2k}+1)j}L\left(\xi^{(p^{2k}-1)j}\right)\right)$$

since $L(-x) = -L(x)$ for any $x \in \mathrm{GF}(p^n)$ and $\eta(-1) = \eta\left(\left(\xi^{p^{2k}+1}\right)^{(p^{2k}-1)/2}\right) = 1$. Therefore,

$$S_f(0) = -(p^{2k} + 1 - 2N(a,b)) + 2N(a,b)(p^{2k}-1) + 1 = p^{2k}(2N(a,b) - 1) \ .$$

Obviously, the number of zeros in U of $L(X)$ is even since $-U = U$ and $L(-x) = -L(x)$ for any $x \in \mathrm{GF}(p^n)$. □

In the following corollary, we prove that it is sufficient to consider just two inequivalent cases, when b is a square and nonsquare in $\mathrm{GF}(p^n)^*$, for instance, taking $b = 1$ and $b = \xi$, where ξ is a primitive element of $\mathrm{GF}(p^n)$.

Corollary 1. *Under the conditions and using the notations of Theorem 1, for any* $h \in \mathrm{GF}(p^n)^*$,

$$N(a,b) = N(ah^d, bh^2) \ .$$

Proof. Recalling definition (2), $2N(ah^d, bh^2)$ is equal to the number of zeros in U of the polynomial

$$\begin{aligned}
(bh^2)^{p^{2k}}X + ah^dX^{p^k} &+ bh^2X^{p^{2k}} + (ah^d)^{p^{2k}}X^{p^{3k}} \\
&= h^{p^{2k}+1}\Big(b^{p^{2k}}h^{p^{2k}-1}X + ah^{p^k(p^{2k}-1)}X^{p^k} \\
&\quad + bh^{-(p^{2k}-1)}X^{p^{2k}} + a^{p^{2k}}h^{-p^k(p^{2k}-1)}X^{p^{3k}}\Big) \\
&= h^{p^{2k}+1}\left(b^{p^{2k}}Y + aY^{p^k} + bY^{p^{2k}} + a^{p^{2k}}Y^{p^{3k}}\right) \ ,
\end{aligned}$$

where $Y = h^{p^{2k}-1}X$ and since $h^{p^{2k}-1} \in U$. By definition, the latter polynomial has $2N(a,b)$ zeros in U. □

In what follows, we consider separately the cases when either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$ with $b \neq 0$; and when $a^{p^k(p^k+1)} = b^{p^k+1}$ with $a^2 \neq b^d$, where $d = p^{3k} + p^{2k} - p^k + 1$. This covers all the value space for the pairs $(a,b) \neq (0,0)$.

4.1 Case $a^{p^k(p^k+1)} \neq b^{p^k+1}$

In this subsection, we show that the exponential sum of $f(x)$ takes on just three values $-p^{2k}$, p^{2k} and $3p^{2k}$ when either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$ with $b \neq 0$.

Proposition 1. *Let $n = 4k$ and take any $a, b \in \mathrm{GF}(p^n)$ such that either $a^2 = b^d$ with $b \neq 0$ or $a^{p^k(p^k+1)} \neq b^{p^k+1}$. Then polynomial $L(X)$ defined in (2) has none, two or four zeros in U, i.e., $N(a,b) \in \{0,1,2\}$. Moreover, if $a^{p^k(p^k+1)} \neq b^{p^k+1}$ then zeros of $L(X)$ in $\mathrm{GF}(p^n)$ are the same as of*

$$F(X) = \left(a^{p^k(p^k+1)} - b^{p^k+1}\right)X^{p^{2k}} + \left(a^{p^{2k}}b^{p^{3k}} - ab^{p^k}\right)X^{p^k} + \left(a^{p^k(p^k+1)} - b^{p^k+1}\right)^{p^k} X \ .$$

Proof. First, assume $a^2 = b^d \neq 0$ with $a^{p^k(p^k+1)} = b^{p^k+1}$. Then

$$a^{p^k(p^k+1)} = b^{dp^k(p^k+1)/2} = b^{p^k\left(p^n-1+2(p^{3k}+1)\right)/2} = b^{(p^n-1)/2}b^{p^k+1} = b^{p^k+1} \quad (3)$$

if and only if b is a square in $\mathrm{GF}(p^n)^*$. By Corollary 1, taking $h = b^{-1/2}$ we obtain that $N(a,b) = N(ab^{-d/2}, 1) = N(\pm 1, 1)$. By definition, $2N(\pm 1, 1)$ is equal to the number of zeros in U of $x \pm x^{p^k} + x^{-1} \pm x^{-p^k}$. For any $v \in U$ we obtain

$$v \pm v^{p^k} + v^{-1} \pm v^{-p^k} = v^{-(p^k+1)}\left(v^{p^k+1} \pm 1\right)\left(v \pm v^{p^k}\right) = 0$$

only if $v^{2(p^k+1)} = 1$ or $v^{2(p^k-1)} = 1$ which leads to $v^2 = 1$ since $\gcd(2(p^k+1), p^{2k}+1) = \gcd(2(p^k-1), p^{2k}+1) = 2$. Thus, $v = \pm 1$ that gives no zeros when $a = b^{d/2}$ and two when $a = -b^{d/2}$.

From now on assume $a^{p^k(p^k+1)} \neq b^{p^k+1}$. Note that zeros of

$$a^{p^{2k}}L(X)^{p^k} - b^{p^k}L(X) = F(X)$$

are exactly the union of solution sets for $L(X) = 0$ and $a^{p^{2k}}L(X)^{p^k-1} = b^{p^k}$. Since $L(x) \in \mathrm{GF}(p^{2k})$ for any $x \in \mathrm{GF}(p^n)$ and assuming $L(x) \neq 0$, the latter equation can have solution only if $a^{p^{2k}(p^k+1)} = b^{p^k(p^k+1)}$ that is equivalent to $a^{p^k(p^k+1)} = b^{p^k+1}$. Thus, $L(X)$ and $F(X)$ have the same zeros. Also note that $F(x)$ degenerates if and only if $a^{p^k(p^k+1)} = b^{p^k+1}$ since in this case,

$$\begin{aligned} a^{p^{2k}}b^{p^{3k}} - ab^{p^k} &= a^{-p^k}\left(a^{p^k(p^k+1)}b^{p^{3k}} - (a^{p^k(p^k+1)})^{p^{3k}}b^{p^k}\right) \\ &= a^{-p^k}\left(b^{p^{3k}+p^k+1} - b^{p^{3k}+p^k+1}\right) = 0 \ , \end{aligned} \quad (4)$$

i.e., $ab^{p^k} \in \mathrm{GF}(p^{2k})$.

Raising the elements of U to the power of $p^k - 1$ defines a 2-to-1 mapping onto U_+ the set of squares of U since $\gcd(p^k - 1, p^{2k} + 1) = 2$. Thus, making a substitution $Y = X^{p^k-1}$ and denoting $A = a^{p^k(p^k+1)} - b^{p^k+1}$ we obtain the polynomial

$$P(Y) = AY^{p^k+1} + \left(a^{p^{2k}}b^{p^{3k}} - ab^{p^k}\right)Y + A^{p^k}$$

that has $N(a,b)$ zeros in U_+. Further, assuming $Y^{p^{2k}} = Y^{-1}$, we obtain

$$AY^2P(Y)^{p^k} - \left(a^{p^{3k}}b - a^{p^k}b^{p^{2k}}\right)YP(Y) - A^{p^k}P(Y)$$
$$= A^{p^k}\left(A^{p^{3k}}Y^2 - \left(a^{p^{2k}}b^{p^{3k}} - ab^{p^k} + a^{p^{3k}}b - a^{p^k}b^{p^{2k}}\right)Y - A^{p^k}\right) .$$

Since $A \neq 0$, the latter polynomial is non-degenerate and has at most two zeros in $\mathrm{GF}(p^n)$ which also means that $N(a,b) \leq 2$. □

4.2 Case $a^{p^k(p^k+1)} = b^{p^k+1}$ and Jacobsthal Sums

In this subsection, we consider the case when $a^{p^k(p^k+1)} = b^{p^k+1}$ with $a^2 \neq b^d$ and express the exponential sum of $f(x)$ using Jacobsthal sums of order p^k+1.

Proposition 2. *Let $n = 4k$ and take any $a, b \in \mathrm{GF}(p^n)$ such that $a^{p^k(p^k+1)} = b^{p^k+1}$ and $a^2 \neq b^d$. If $2N(a,b)$ is the number of zeros in U of the polynomial $L(x)$ defined in (2) then*

$$N(a,b) = \#\left\{c \in \mathrm{GF}(p^k) \mid (cg)^2 - b^{p^{2k}+1} \text{ is a nonsquare in } \mathrm{GF}(p^{2k})\right\} , \quad (5)$$

where g is any element in $\mathrm{GF}(p^{2k})^*$ with $g^{p^k-1} = -b^{p^{3k}}/a$.

Proof. Note that in our case, $a, b \neq 0$ and $g \in \mathrm{GF}(p^{2k})^*$ since $\left(b^{p^{3k}}/a\right)^{p^k+1} = 1$. Take any $u \in U$ with $L(u) = 0$. Multiplying both sides of $L(u) = 0$ by $b^{p^{3k}}$ and using (4), we obtain

$$a\left(b^{p^{2k}}u + bu^{-1}\right)^{p^k} + b^{p^{3k}}\left(b^{p^{2k}}u + bu^{-1}\right) = 0 . \quad (6)$$

Denote $b^{p^{2k}}u + bu^{-1} = g \in \mathrm{GF}(p^{2k})$. Find solutions in U of the quadratic equation $b^{p^{2k}}x + bx^{-1} = g$ which discriminant is equal to $D = g^2 - 4b^{p^{2k}+1} \in \mathrm{GF}(p^{2k})$.

First, assume D is a square in $\mathrm{GF}(p^{2k})$. Then $u = (g \pm \sqrt{D})/2b^{p^{2k}}$ and $b^{p^{2k}}u \in \mathrm{GF}(p^{2k})^*$ resulting in $g = 2b^{p^{2k}}u \neq 0$ and $D = 0$. In this case, (6) is reduced to $au^{p^k-1} = -b^{p^{2k}}$. We also obtain that

$$\left(b^{p^{2k}}u\right)^{p^{2k}+1} = b^{p^{2k}+1} = \left(b^{p^{2k}}u\right)^2$$

that is equivalent to $b = u^2b^{p^{2k}}$ Then $u = \pm b^{-(p^{2k}-1)/2}$ and

$$au^{p^k-1}b^{-p^{2k}} = ab^{-d/2} = -1$$

that leads to $a = -b^{d/2}$. Thus, no solutions in U exist if $a^2 \neq b^d$.

If D is a nonsquare in $\mathrm{GF}(p^{2k})$ then there exists some $d \in \mathrm{GF}(p^n) \setminus \mathrm{GF}(p^{2k})$ such that $g^2 - 4b^{p^{2k}+1} = d^2$. Raising both sides of the latter identity to the power of p^{2k}, we obtain $g^2 - 4b^{p^{2k}+1} = d^{2p^{2k}} = d^2$ that leads to $d^{p^{2k}} = -d$ since $d \notin \mathrm{GF}(p^{2k})$. Solutions of $b^{p^{2k}}x + bx^{-1} = g$ are $x_{1,2} = (g \pm d)/2b^{p^{2k}}$ and

$$x_{1,2}^{p^{2k}+1} = \frac{g^{p^{2k}+1} \pm g^{p^{2k}}d \pm gd^{p^{2k}} + d^{p^{2k}+1}}{4b^{p^{2k}+1}} = \frac{g^2 \pm gd \mp gd - d^2}{4b^{p^{2k}+1}} = 1 .$$

Thus, $x_{1,2} \in U$.

Summarizing the arguments presented above, we conclude that if $a^{p^k(p^k+1)} = b^{p^k+1}$ and $a^2 \neq b^d$ then for any $g \in \mathrm{GF}(p^{2k})$, the equation $b^{p^{2k}}x + bx^{-1} = g$ has no solutions in U if $g^2 - 4b^{p^{2k}+1}$ is a square in $\mathrm{GF}(p^{2k})$ and has two solutions in U otherwise.

If $b^{p^{2k}}u + bu^{-1} \neq 0$ then (6) can be written as

$$\left(b^{p^{2k}}u + bu^{-1}\right)^{p^k-1} = -\frac{b^{p^{3k}}}{a} \quad .$$

Raising elements of $\mathrm{GF}(p^{2k})^*$ to the power of $p^k - 1$ defines a $(p^k - 1)$-to-1 mapping onto the cyclic subgroup of $\mathrm{GF}(p^{2k})^*$ of order $p^k + 1$ and all elements in the set $\{2cg \mid c \in \mathrm{GF}(p^k)^*\}$ with $g^{p^k-1} = -b^{p^{3k}}/a$ map to the same element $-b^{p^{3k}}/a$. Include $c = 0$ to take care of the case when $b^{p^{2k}}u + bu^{-1} = 0$. The discriminant of the quadratic equation $b^{p^{2k}}x + bx^{-1} = 2cg$, equal to $(2cg)^2 - 4b^{p^{2k}+1}$, is a square if and only if $D = (cg)^2 - b^{p^{2k}+1}$ is a square. Only those $c \in \mathrm{GF}(p^k)$ with D being a nonsquare contribute two solutions to $2N(a,b)$. □

Like in Proposition 2, assume $a, b \in \mathrm{GF}(p^n)^*$ with $a^2 \neq b^d$ and $g \in \mathrm{GF}(p^{2k})^*$ with $g^{p^k-1} = -b^{p^{3k}}/a$. In this case, $b^{p^{2k}+1}/g^2 \notin \mathrm{GF}(p^k)$ since

$$\left(\frac{b^{p^{2k}+1}}{g^2}\right)^{p^k-1} = \frac{a^2 b^{(p^{2k}+1)(p^k-1)}}{b^{2p^{3k}}} = \frac{a^2}{b^d} \neq 1 \tag{7}$$

which also means that $(cg)^2 - b^{p^{2k}+1} \neq 0$ for any $c \in \mathrm{GF}(p^k)$. Therefore, by Proposition 2,

$$\begin{aligned} p^k - 2N(a,b) &= \sum_{c \in \mathrm{GF}(p^k)} \eta\big((cg)^2 - b^{p^{2k}+1}\big) \\ &= \eta\big(-b^{p^{2k}+1}\big) + \frac{1}{p^k+1} \sum_{x \in \mathrm{GF}(p^{2k})^*} \eta\big(x^{2(p^k+1)} - b^{p^{2k}+1}/g^2\big) \\ &= \eta\big(-b^{p^{2k}+1}/g^2\big) + \frac{I_{2(p^k+1)}\big(-b^{p^{2k}+1}/g^2\big)}{p^k+1} \\ &\overset{(1)}{=} \frac{H_{p^k+1}\big(-b^{p^{2k}+1}/g^2\big)}{p^k+1} - 1 \quad . \end{aligned}$$

We conclude that

$$2N(a,b) = p^k - \frac{H_{p^k+1}\big(-b^{p^{2k}+1}/g^2\big)}{p^k+1} + 1 \tag{8}$$

and, by Theorem 3,

$$S_f(0) = p^{2k}\left(p^k - \frac{H_{p^k+1}\big(-b^{p^{2k}+1}/g^2\big)}{p^k+1}\right) \quad .$$

Thus, finding the value distribution of $S_f(0)$ when $a^{p^k(p^k+1)} = b^{p^k+1}$ with $a^2 \neq b^d$, is related to finding the values of the Jacobsthal sum of order p^k+1. In the following corollary, we list some basic properties of $N(a,b)$.

Corollary 2. *Under the conditions of Proposition 2,*

(i) $N(a,b) = \begin{cases} N(a^{-1},b^{-1}), & \text{if } b^{(p^n-1)/2} = 1 \\ p^k+1-N(a^{-1},b^{-1}), & \text{otherwise} \end{cases}$;

(ii) $N(a,b)+N(-a,b) = N(a,b)+N(a,-b) = p^k+1$;

(iii) $N(-a,b) = \begin{cases} p^k+1-N(a^{-1},b^{-1}), & \text{if } b^{(p^n-1)/2} = 1 \\ N(a^{-1},b^{-1}), & \text{otherwise} \end{cases}$;

(iv) if $b^{(p^n-1)/2} = 1$ *(resp.* $b^{(p^n-1)/2} = -1$*) then* $N(a,b)$ *is an even (resp. odd) number;*

(v) $\left|N(a,b) - \frac{p^k+1}{2}\right| \leq p^{k/2}$*, in particular,* $N(a,b)$ *is positive and, if* $k > 2$ *then* $N(a,b) > 8$;

(vi) if $p \equiv -1 \pmod 4$*,* k *is odd and* $b^{(p^n-1)/2} = 1$ *then* $N(a,b) = N(-a,b) = (p^k+1)/2$ *for* $a = \nu^{(p^{2k}-1)/4} b^{d/2}$*, where* ν *is a primitive element of* $\mathrm{GF}(p^{2k})$;

(vii) for any $b \in \mathrm{GF}(p^n)^*$,

$$\sum_{a\in\mathrm{GF}(p^n):\ a^{p^k(p^k+1)}=b^{p^k+1},\ a^2\neq b^d} N(a,b) = (p^k+1)\left(p^k - b^{(p^n-1)/2}\right)/2 \ . \quad (9)$$

Proof. First, note that $b^{p^{2k}+1}$ is a square in $\mathrm{GF}(p^{2k})$ if and only if $b^{(p^n-1)/2} = 1$, i.e., b is a square in $\mathrm{GF}(p^n)$. Assume $c \neq 0$ in (5). Then if b is a square (resp. nonsquare) in $\mathrm{GF}(p^n)$ then $(cg)^2 - b^{p^{2k}+1}$ is a nonsquare in $\mathrm{GF}(p^{2k})$ if and only if $(cg)^{-2} - b^{-(p^{2k}+1)}$ is a nonsquare (resp. square), since $-1 = \left(\nu^{(p^{2k}-1)/4}\right)^2$. If b is a square in $\mathrm{GF}(p^n)$ then, by (5),

$$\begin{aligned} N(a,b) &= \#\left\{c \in \mathrm{GF}(p^k)^* \mid (cg)^2 - b^{p^{2k}+1} \text{ is a nonsquare in } \mathrm{GF}(p^{2k})\right\} \\ &= \#\left\{c \in \mathrm{GF}(p^k)^* \mid (cg^{-1})^2 - b^{-(p^{2k}+1)} \text{ is a nonsquare in } \mathrm{GF}(p^{2k})\right\} \\ &= N(a^{-1},b^{-1}) \end{aligned}$$

since $g^{-(p^k-1)} = -a/b^{p^{3k}}$ if $g^{p^k-1} = -b^{p^{3k}}/a$. Similarly, If b is a nonsquare in $\mathrm{GF}(p^n)$ then

$$\begin{aligned} N(a,b) &= 1 + \#\left\{c \in \mathrm{GF}(p^k)^* \mid (cg)^2 - b^{p^{2k}+1} \text{ is a nonsquare in } \mathrm{GF}(p^{2k})\right\} \\ &= 1 + \#\left\{c \in \mathrm{GF}(p^k)^* \mid (cg^{-1})^2 - b^{-(p^{2k}+1)} \text{ is a square in } \mathrm{GF}(p^{2k})\right\} \\ &= 1 + p^k - 1 - \left(N(a^{-1},b^{-1}) - 1\right) \ . \end{aligned}$$

This proves (i).

For a pair (a,b), the corresponding $g \in \mathrm{GF}(p^{2k})^*$ satisfies $g^{p^k-1} = -b^{p^{3k}}/a$. Then $\left(\nu^{(p^k+1)/2}g\right)^{p^k-1} = b^{p^{3k}}/a$ which means that $\nu^{(p^k+1)/2}g$ corresponds both to $(-a,b)$ and $(a,-b)$. Also, $\left(c\nu^{(p^k+1)/2}g\right)^2 = \nu^{p^k+1}c^2g^2$ and ν^{p^k+1} is a generator of $\mathrm{GF}(p^k)^*$. If $b^{p^{2k}+1}$ is a square in $\mathrm{GF}(p^{2k})$ then for any $c \in \mathrm{GF}(p^k)^*$, we have $cg^2/b^{p^{2k}+1} \in C_{2i}$ with $i \neq 0$ that follows from (7). In this case, by (5),

$$\begin{aligned} N(a,b)+N(-a,b) &= N(a,b)+N(a,-b) \\ &= 2\#\left\{c \in \mathrm{GF}(p^k)^* \mid cg^2 - b^{p^{2k}+1} \text{ is a nonsq. in } \mathrm{GF}(p^{2k})\right\} \\ &= 2\#\{x \in C_{2i} \mid x-1 \text{ is a nonsquare in } \mathrm{GF}(p^{2k})\} \\ &= 2\sum_{j=0}^{(p^k-1)/2}(2i,2j+1) \overset{(*)}{=} p^k+1 \end{aligned}$$

since the set of nonsquares in $\mathrm{GF}(p^{2k})$ is equal to $\bigcup_{j=0}^{(p^k-1)/2} C_{2j+1}$ and where $(*)$ is obtained using Lemma 1. Similarly, if $b^{p^{2k}+1}$ is a nonsquare in $\mathrm{GF}(p^{2k})$ then for any $c \in \mathrm{GF}(p^k)^*$, we have $cg^2/b^{p^{2k}+1} \in C_{2i+1}$ and

$$\begin{aligned} N(a,b)+N(\pm a,\mp b) &= 2+2\#\{x \in C_{2i+1} \mid x-1 \text{ is a square in } \mathrm{GF}(p^{2k})\} \\ &= 2+2\sum_{j=0}^{(p^k-1)/2}(2i+1,2j) = p^k+1 \end{aligned}$$

since the set of squares in $\mathrm{GF}(p^{2k})$ is equal to $\bigcup_{j=0}^{(p^k-1)/2} C_{2j}$. The additive term 2 comes from $c=0$. This proves (ii), and (iii) follows directly by combining (i) and (ii).

If $b^{p^{2k}+1}$ is a square in $\mathrm{GF}(p^{2k})$ then $c \neq 0$ and $N(a,b)$ is even since c^2 is 2-to-1 on $\mathrm{GF}(p^k)^*$. If $b^{p^{2k}+1}$ is a nonsquare then $c=0$ contributes 1 to $N(a,b)$ and makes it odd.

Combining (8) with Theorem 2 we immediately obtain the estimate in (v). Also note that $(p^k+1)/2 - p^{k/2}$ grows both with p and k. The lowest value is achieved when $p=3$ and $k=1$ giving $2-3^{1/2} > 0$ (thus, $N(a,b) > 0$) and if $k > 2$ then $N(a,b) \geq 14 - 27^{1/2} > 8$.

If b is square in $\mathrm{GF}(p^n)^*$ then, by Corollary 1,

$$N(\pm\nu^{(p^{2k}-1)/4}b^{d/2}, b) = N(\pm\nu^{(p^{2k}-1)/4}, 1) \ .$$

Then (vi) follows from (ii) and (iii) since $a^{-1} = -a$ if and only if $a^2 = -1 = \nu^{(p^{2k}-1)/2}$ (we also have to remember the requirement $a^{p^k(p^k+1)} = b^{p^k+1}$ and $a^2 \neq b^d$ that in our case becomes $a^{p^k+1} = 1$ and $a \neq \pm 1$).

Take any $b \in \mathrm{GF}(p^n)^*$ and fix (conditions of Proposition 2 provide that $b \neq 0$). Note that $x^{p^k(p^k+1)} = b^{p^k+1}$ has p^k+1 solutions in $\mathrm{GF}(p^n)$. If b is a square in $\mathrm{GF}(p^n)$ then both $a = \pm b^{d/2}$ satisfy $a^{p^k(p^k+1)} = b^{p^k+1}$ (see (3)). Thus, summation conditions in (9) are satisfied by p^k-1 values of $a \in \mathrm{GF}(p^n)$. On the other

hand, if b is a nonsquare in $\mathrm{GF}(p^n)$ then $a^2 \neq b^{d/2}$ whenever $a^{p^k(p^k+1)} = b^{p^k+1}$. Therefore, (9) immediately follows from (ii). □

Take any $b \in \mathrm{GF}(p^n)^*$ and fix. Having in mind Theorem 3 and Proposition 1, suppose $S_f(0)$ takes on the values $-p^{2k}$, p^{2k} and $3p^{2k}$ respectively r, s and t times when $a \in \mathrm{GF}(p^n)$ and either $a^{p^k(p^k+1)} \neq b^{p^k+1}$ or $a^2 = b^d$. Actually, by Corollary 2 (v), for all the remaining values of a we have that $S_f(0) \neq -p^{2k}$ and, if $k > 2$, then $S_f(0) > 15p^{2k}$.

First, assume b is a square in $\mathrm{GF}(p^n)^*$. Then $r + s + t = p^n - p^k + 1$ (see the proof of Corollary 2 (vii)). Further, by Theorem 3,

$$\begin{aligned}\sum_{a\in\mathrm{GF}(p^n)} S_f(0) &= -rp^{2k} + sp^{2k} + 3tp^{2k} + p^{2k} \sum_{a^{p^k(p^k+1)}=b^{p^k+1},\ a^2\neq b^d} (2N(a,b)-1)\\ &\overset{(9)}{=} p^{2k}(-r+s+3t) + p^{2k}(p^{2k}-1-p^k+1)\\ &= p^{2k}(-r+s+3t-p^k) + p^n \ .\end{aligned}$$

Similarly, if b is a nonsquare in $\mathrm{GF}(p^n)^*$ then $r + s + t = p^n - p^k - 1$ and

$$\begin{aligned}\sum_{a\in\mathrm{GF}(p^n)} S_f(0) &\overset{(9)}{=} p^{2k}(-r+s+3t) + p^{2k}((p^k+1)^2 - p^k - 1)\\ &= p^{2k}(-r+s+3t+p^k) + p^n \ .\end{aligned}$$

On the other hand, for any $b \in \mathrm{GF}(p^n)$,

$$\begin{aligned}\sum_{a\in\mathrm{GF}(p^n)} S_f(0) &= \sum_{a\in\mathrm{GF}(p^n)} \sum_{x\in\mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^{3k}+p^{2k}-p^k+1}+bx^2\right)}\\ &= \sum_{x\in\mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(bx^2\right)} \sum_{a\in\mathrm{GF}(p^n)} \omega^{\mathrm{Tr}_n\left(ax^{p^{3k}+p^{2k}-p^k+1}\right)} = p^n \ .\end{aligned}$$

Thus, if $b \neq 0$ then $r + s + t = p^n - p^k + b^{(p^n-1)/2}$ and $-r + s + 3t = b^{(p^n-1)/2}p^k$.

Note that finding the sum of squares of $S_f(0)$ is easy in our case. Therefore, knowing the values and the distribution of the Jacobsthal sum of order $p^k + 1$ would give us the third equation allowing to find r, s and t. However, in this way we are facing some long-lasting open problems. On the other hand, it may be possible to extract some extra relations for the unknowns, thus, bypassing the problem of finding the value distribution of Jacobsthal sums. This is the first direct connection between sequences and Jacobsthal sums we are aware of. We find it interesting and believe that this gives an important link between sequences/codes and classical character sums.

References

1. Niho, Y.: Multi-Valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences. PhD thesis, University of Southern California, Los Angeles (1972)

2. Helleseth, T.: A note on the cross-correlation function between two binary maximal length linear sequences. Discrete Math. 23(3), 301–307 (1978)
3. Helleseth, T., Kholosha, A.: New binomial bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory (to appear 2010), http://arxiv.org/abs/0907.3348
4. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combin. Theory Ser. A 40(1), 90–107 (1985)
5. Hou, X.D.: p-Ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields Appl. 10(4), 566–582 (2004)
6. Pott, A., Tan, Y., Feng, T., Ling, S.: Association schemes arising from bent functions. In: Kholosha, A., Rosnes, E., Parker, M. (eds.) WCC 2009 Preproceedings - The International Workshop on Coding and Cryptography, Bergen, pp. 48–61 (2009)
7. Tan, Y., Pott, A., Feng, T.: Strongly regular graphs associated with ternary bent functions. J. Combin. Theory Ser. A 117(6), 668–682 (2010)
8. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory 52(5), 2018–2032 (2006)
9. Baumert, L., Mills, W., Ward, R.L.: Uniform cyclotomy. J. Number Theory 14(1), 67–82 (1982)
10. Hauge, E.R., Helleseth, T.: DeBruijn sequences, irreducible codes and cyclotomy. Discrete Math. 159(1-3), 143–154 (1996)
11. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge (1997)
12. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd edn. Graduate Texts in Mathematics, vol. 106. Springer, Berlin (2009)

Infinite Sequences with Finite Cross-Correlation

Solomon W. Golomb

University of Southern California
Los Angeles, CA 90089-2565, USA

Abstract. Let $A = \{a_k\}_{k=1}^{\infty}$ be an infinite increasing sequence of positive integers. We define the infinite binary sequence $\overline{A} = \{\alpha_j\}_{j=1}^{\infty}$ to have $\alpha_j = 1$ if $j \in A$, $\alpha_j = 0$ if $j \notin A$ (including when $j \leq 0$). If $B = \{b_k\}_{k=1}^{\infty}$ is also an infinite increasing sequence of positive integers with $\overline{B} = \{\beta_j\}_{j=1}^{\infty}$, by the "cross-correlation of A and B" we will mean the un-normalized, infinite-domain cross-correlation of $\overline{A}$ and $\overline{B}$, i.e.

$$C_{AB}(\tau) = \sum_{i=1}^{\infty} \alpha_i \beta_{i+\tau}$$

for all $\tau \in Z$. Our interest will be in identifying pairs of sequences A and B for which $C_{AB}(\tau)$ is finite for all $\tau \in Z$, and especially when $C_{AB}(\tau) < K$ for some uniform bound K, for all $\tau \in Z$. We will exhibit pairs of sequences A and B where $C_{AB}(\tau) \leq 1$ for all $\tau \in Z$. If $B = P = \{p_1, p_2, p_3, \ldots\} = \{2, 3, 5, 7, \ldots\}$ is the sequence of the prime numbers, we will exhibit sequences A such that $C_{AP}(\tau)$ is finite for all $\tau \in Z$, and question whether a sequence A exists such that $C_{AP}(\tau) < K$ for some uniform bound K and all $\tau \in Z$.

1 Introduction

It is well-known that the set S of infinite sequences $\{a_1 < a_2 < a_3 \ldots\}$ of positive integers is uncountably infinite. (Thus, Neil J.A. Sloane's "Online Encyclopedia of Integer Sequences" will never be complete.) In this paper, we explore ways in which two or more such sequences can have few elements, or patterns of elements, in common.

First, we show that the set S can have an uncountably infinite subset T such that, for any two sequences T_1 and T_2 in T, their intersection $T_1 \cap T_2$ contains only finitely many integers. Specifically, for each real number $x \in [\frac{1}{2}, 1)$, take the binary expansion of x as $x = 0.1c_2c_3c_4c_5 \ldots$, where each c_i is either 0 or 1. Then, associate with x the sequence $1, 1c_2, 1c_2c_3, 1c_2c_3c_4, \ldots$, where the n$th$ term is an n-bit binary number. (For example, with $x = \frac{3}{4} = 0.110000 \ldots$, we would associate the sequence of binary numbers {1, 11, 110, 1100, 11000,...} which in decimal notation becomes {1, 3, 6, 12, 24, 48,...}.) For $x \in [\frac{1}{2}, 1)$ and $y \in [\frac{1}{2}, 1)$ with $x \neq y$, where the binary expansion of y is $y = 0.1d_2d_3d_4d_5 \ldots$, and where the sequence of integers associated with y, in binary notation, is $\{1, 1d_2, 1d_2d_3, 1d_2d_3d_4, \ldots\}$, consider the smallest i such that $c_i \neq d_i$. Then the sequences for x and y will differ in their i^{th} terms, and in all terms thereafter,

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 430–441, 2010.

thus agreeing in only their first $i-1$ terms, a *finite* number of agreements. It is of course well-known that there are uncountably many real numbers in the interval $[\frac{1}{2}, 1)$. (The *countable* set of rational numbers with terminating binary expansions, such as $\frac{3}{4} = 0.110000\ldots = 0.1011111\ldots$, actually contribute *two* distinct sequences in T.) Thus T contains an uncountably large subset of S such that any two sequences in T can have only finitely many integers in common.

2 Cross-Correlation of Sequences

To each infinite integer sequence $A = \{a_1, a_2, a_3, \ldots\}$ with $a_1 < a_2 < a_3 < \ldots$, we associate a companion infinite binary sequence $\overline{A} = \{\alpha_1\alpha_2\alpha_3\alpha_4\ldots\}$, where $\alpha_1 = 1$ if $i \in A, \alpha_i = 0$ if $i \notin A$. (For example, if $A = \{2, 4, 6, 8, \ldots\}$ is the sequence of positive even integers, then $\overline{A} = \{01010101\ldots\}$.) With a second infinite sequence $B = \{b_1, b_2, b_3, \ldots\}$ with $b_1 < b_2 < b_3 < \ldots$, and $\overline{B} = \{\beta_1\beta_2\beta_3\beta_4, \ldots\}$, we define the (infinite, unnormalized) cross-correlation of A and B to be

$$C_{AB}(\tau) = \sum_{j=1}^{\infty} \alpha_j \beta_{j+\tau},$$

for all $\tau \in Z$ (i.e. all integers $\tau, -\infty < \tau < +\infty$). We are particularly interested in sequence pairs with the following three levels of restrictions.
R-1. $C_{AB}(\tau) \leq 1$ for all $\tau \in Z$. (This is the most restrictive condition that can be imposed, since $\overline{A}$ and $\overline{B}$ each contain infinitely many 1's, and as the two sequences slide past one another, each 1 in $\overline{A}$ will collide with a 1 in $\overline{B}$ infinitely many times.)
R-2. $C_{AB}(\tau) < K$ for all $\tau \in Z$, where K is a finite (though perhaps very large) bound, independent of τ.
R-3. $C_{AB}(\tau) < \infty$ for all $\tau \in Z$. (This is the weakest condition we shall consider.)

3 Sequences That Collide Minimally

Theorem 1. *The condition $C_{AB}(\tau) < 1$ for all $\tau \in Z$ (restriction R-1) is equivalent to the following condition: The "difference sets" ΔA and ΔB are disjoint. (With $A = \{a_1, a_2, a_3, \ldots\}$ where $a_1 < a_2 < a_3 < \ldots$, and $B = \{b_1, b_2, b_3, \ldots\}$ where $b_1 < b_2 < b_3 < \ldots$, we define $\Delta A = \{$all $a_j - a_i$ with $0 < i < j\}$ and $\Delta B = \{$all $b_j - b_i$ with $0 < i < j$.)*

Proof. If and only if there are positive integers i, j, k, l with $i < j$ and $k < l$ such that $a_j - a_i = b_l - b_k$, there is $\tau \in Z$ with $b_l - a_j = b_k - a_i = \tau$. Then $C_{AB}(\tau) \geq 2$, since shifting $\overline{A}$ relative to $\overline{B}$ by τ produces at least these two hits. Conversely, if there is any $\tau \in Z$ with $C_{AB}(\tau) \geq 2$, there must be terms $a_i < a_j$ in A and $b_k < b_l$ in B with $a_j - a_i = b_l - b_k$, from which $b_l - a_j = b_k - a_i = \tau$. □

Example 1. Define the Fibonacci sequence $\{f_n\}_{n=1}^{\infty}$ by $f_1 = f_2 = 1$, $f_{n+1} = f_n + f_{n-1}$ for all $n > 1$. Let $A = \{f_{2n-1}\}_{n=1}^{\infty} = \{1, 2, 5, 13, 34, 89, 233, \ldots\}$ and

$B = \{f_{2n}\}_{n=1}^{\infty} = \{1, 3, 8, 21, 55, 144, 377, \ldots\}$. Then $\Delta A = \{1, 3, 4, 8, 11, 12, 21, 29, 32, 33, 55, 76, 84, 87, 88, 144, \ldots\}$ and $\Delta B = \{2, 5, 7, 13, 18, 20, 34, 47, 52, 54, 89, 123, 136, \ldots\}$. For this choice of sequences A and B, since $(\Delta A) \cap (\Delta B) = \emptyset$, we have $C_{AB}(\tau) \leq 1$ for all $\tau \in Z$.

Remark 1

1. In this example, A and B are among the first differences of each other.
2. By the Fibonacci property, these two sequences A and B have the same asymptotic growth rate, $(3 + \sqrt{5})/2 = 2.618\ldots$, and are accordingly "equi-dense."
3. In general, in order for $(\Delta A) \cap (\Delta B) = \emptyset$, we would expect that as one sequence becomes more dense, the other must become less dense.
4. It is possible to find "equi-dense" sequences A and B, each more dense than $\{f_{2n-1}\}$ and $\{f_{2n}\}$, but still with $(\Delta A) \cap (\Delta B) = \emptyset$. This is discussed in Sections 7 and 8.

4 Repeated Difference Patterns

Just as the existence of an integer $\delta > 0$ such that $a_i + \delta = a_j, b_k + \delta = b_l$ leads to a value of τ (namely, $\tau = b_k - a_i$) for which $C_{AB}(\tau) \geq 2$, a pattern in which $a_i + \delta_1 = a_j, a_i + \delta_2 = a_k, 0 < \delta_1 < \delta_2$, mirrored by $b_l + \delta_1 = b_m, b_l + \delta_2 = b_n$, leads to a value of τ (namely, $\tau = b_l - a_i$) for which $C(\tau) \geq 3$. More generally,

Theorem 2. *$C_{AB}(\tau) \geq k$ if and only if there is a "k-tuple pattern" with $0 < \delta_1 < \delta_2 < \ldots < \delta_{k-1}$ such that there is $a_i \in A$ and $b_j \in B$ such that all k of $a_i, a_i+\delta_1, a_i+\delta_2, \ldots, a_i+\delta_{k-1}$ are in A, and all k of $b_j, b_j+\delta_1, b_j+\delta_2, \ldots, b_j+\delta_{k-1}$ are in B.*

Proof. If and only if this common "k-tuples pattern" can be found in both sequence A and sequence B, there will be a set of k 1's somewhere in $\overline{A}$ and a set of k 1's somewhere in $\overline{B}$ having the same spacing, corresponding to the distances $\delta_1, \delta_2, \ldots, \delta_{k-1}$, beyond the first 1 in the pattern, and there will be a shift by some τ that brings these two 1's-patterns into coincidence; so for this value of $\tau, C(\tau) \geq k$. (Note that the binary digits that occur in $\overline{A}$ and in $\overline{B}$ *between* the 1's of the corresponding k-tuples have no impact on the proof just given.) □

We will explore the relevance of this theorem to the validity of the "prime k-tuples conjecture" in the next sections.

5 Cross-Correlations with the Sequence of the Prime Numbers

Let $P = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$ be the infinite increasing sequence of the prime numbers, with $\overline{P} = \{011010100010100010\ldots\}$. In [1], I posed a two-part problem. In Part a., I asked for an infinite increasing sequence $A = \{a_1, a_2, a_3, \ldots\}$ of positive integers for which $C_{AP}(\tau) < \infty$ for all $\tau \in Z$. An example will be

described below. In Part b., I asked if there is such a sequence A for which $C_{AP}(\tau) < K$ for a fixed bound K for all $\tau \in Z$. Whether such a sequence exists is not known, and its existence would contradict a widely believed conjecture about the prime numbers.

Theorem 3. *The sequence* $A = \{a_n\}_{n=1}^{\infty}$ *where* $a_n = ((2n)!\,)^3$ *has finite cross-correlation,* $C_{AP}(\tau) < \infty$ *for all* $\tau \in Z$*, with the sequence* P *of the prime numbers.*

Proof. We will show that $C_{AP}(\tau) \leq |\tau|$ for all $\tau \in Z$.

i) $C_{AP}(0) = 0$, since $((2n)!\,)^3$ is composite for all $n \geq 1$.
ii) Since $x^3 + 1 = (x+1)(x^2 - x + 1)$ and $x^3 - 1 = (x-1)(x^2 + x + 1)$, $a_n + 1 = ((2n)!\,)^3 + 1$ is composite for all $n \geq 1$, and $a_n - 1 = ((2n)!\,)^3 - 1$ is composite except at $n = 1$, where $(2!\,)^3 - 1 = 7$. Thus $C_{AP}(\pm 1) \leq 1$.
iii) Since $((2n)!\,)^3 + \tau$ is divisible by $|\tau|$ for all $n \geq |\tau|$, we see that $a_n \pm \tau$ can be prime only for (some) values of $n < |\tau|$. Hence, for all $|\tau| > 1, C_{AP}(\tau) \leq |\tau|$. □

The *prime k-tuples conjecture* is the assertion that there are infinitely many integer values of x such that all k of the numbers $\{x, x+a_1, x+a_2, \ldots, x+a_{k-1}\}$ are prime, provided only that the k numbers $\{0, a_1, a_2, \ldots, a_{k-1}\}$ do not fill a complete residue system modulo any prime p. (That is, the least non-negative remainders, upon division by p, of the numbers $0, a_1, a_2, \ldots, a_{k-1}$ do not include all the values $0, 1, 2, \ldots, p-1$.) The simplest special case occurs with $k = 2$ and $a_1 = 2$, the "twin prime conjecture" that for infinitely many integer values of x, both x and $x + 2$ are prime. No one seriously doubts that this special case is true.

From our perspective, the prime k-tuples conjecture is the assertion that every "permissible" pattern of 1's occurs infinitely often in the binary sequence $\overline{P}$.

In L.E. Dickson's three-volume *History of the Theory of Numbers*, the first published reference he found to the "twin prime conjecture" was the more general conjecture, from the nineteenth century, of de Polignac: "Every even number is a difference of two primes, and in fact, in infinitely many ways." This is precisely the case $k = 2$ of the prime k-tuples conjecture.

If the de Polignac conjecture is true (and there seems to be little reason to doubt it), then

Theorem 4. *No matter what infinite increasing positive integer sequence* A *is chosen,* $C_{AB}(\tau) \leq 1$ *for all* $\tau \in Z$ *will not be possible, if de Polignac's Conjecture is true.*

Proof. Suppose there were such a sequence A. Let B be the subsequence of A containing all terms of A which are *even* numbers, and let C be the subsequence of A containing all the terms of A which are *odd* numbers (Thus $B \cup C = A$, and $B \cap C = \emptyset$. Because A is an infinite sequence, at least one of B and C must be an infinite sequence of integers. Both ΔB and ΔC consist entirely of

even integers, and at least one of these two sets is infinite. Hence ΔA contains infinitely many even integers. (Here ΔA, ΔB, and ΔC are defined as in Section 3. above.) If de Polignac's Conjecture is true, ΔP contains *every* even integer (in fact, infinitely often), so that (ΔA) ∩ (ΔP) contains infinitely many integers, whence $C_{AP}(\tau) > 1$ for infinitely many values of $\tau \in Z$. □

6 "Golomb's Conjecture"

The existence of an infinite sequence A of positive integers such that $C_{AP}(\tau) < K$ for all $\tau \in Z$, where K is a finite (though possibly very large) bound independent of τ, is referred to in [3] as "Golomb's Conjecture." This conjecture is inconsistent with the "prime k-tuples conjectures." A proof of this inconsistency is also given in [3] (where a conjecture of Hardy-Littlewood is also shown to be inconsistent with the prime k-tuples conjecture).

The cross-correlation viewpoint presented in this paper facilitates visualizing the inconsistency of these two conjectures ("Golomb's" and "prime k-tuples"). Whatever sequence A is considered, the corresponding binary sequence $\overline{A}$ has infinitely many (though possibly sparsely situated) 1's, and when this pattern is translated across the fairly dense pattern of 1's in $\overline{P}$, the "prime k-tuples conjecture" implies that the number of 1-on-1 "hits" will exceed any pre-assigned bound K, for some shift τ.

The plausibility of Golomb's Conjecture arises from considering a sequence $A = \{a_n\}$, all $n \geq 1$, with an extraordinarily fast growth rate. For example, if $a_n = \left(\left(10^{10^{10^{10^{10^n}}}}\right)!\right)^3$, so that $C_{AP}(\tau)$ is finite for all $\tau \in Z$ as in Theorem 3, the *expected number* of primes in A, namely $\sum_{n=1}^{\infty} \frac{1}{\ln a_n}$, is a tiny positive real number, and this will be true for each translate sequence $A_\tau = \{a_n + \tau\}$, for all $\tau \in Z$. If we then take a huge value of K, e.g. $K_0 = 10^{10^{10^{10^{100}}}}$, for Golomb's Conjecture to be false there must be *infinitely many* values of τ with $C_{AP}(\tau) > K_0$. (If there were only finitely many such values, since $C_{AP}(\tau)$ is always finite, there would be a largest value $C_{AP}(\tau)_{MAX} = L$, and taking any $K > L$, for this K we would have $C_{AP}(\tau) < K$ for all $\tau \in Z$.)

Since far faster growth rates than the $A = \{a_n\}$ suggested here, and far larger values than the K_0 suggested here, can be chosen, it takes considerable faith to remain convinced of the truth of the prime k-tuples conjecture.

7 Infinite Spanning Birulers

A *spanning ruler with n marks* has been defined [2] as an increasing set of n non-negative integers $\{d_1, d_2, \ldots, d_n\}, d_i < d_{i+1},$, such that the $\binom{n}{2}$ differences $d_j - d_i$, with $i < j$, are all distinct. (We depart from the original convention, where $d_1 = 0$, to take $d_1 = 1$ to conform to our current context. Clearly, adding any

constant c to all the marks on a ruler has no effect on the "measured distances", i.e. the set of all differences between pairs of marks.)

The shortest spanning ruler with n marks has the *smallest measured length,* $L(n) = d_n - d_1$, subject to the "all differences distinct" requirement, and is referred to in the literature as the *Golomb ruler* with n marks. (Some authors use the term *Golomb ruler* to refer to *any* spanning ruler, which muddles a useful distinction.) There has been a decades-long search for Golomb rulers with n marks, and their lengths, $L(n)$. At this writing, $L(n)$ is known precisely for $n \leq 27$, and conjectured values of $L(n)$ extend beyond $n = 200$. It is also conjectured that $L(n) \sim cn^2$ as $n \to \infty$ for some positive constant **c**. Trivially $L(n) \geq \binom{n}{2}$ for all $n \geq 2$, since this is the number of measured distances between n marks, which must all be distinct positive integers.

In [2] we also considered *sets* of k spanning rulers with the property that all the measured distances of all k rulers combined are distinct. For present purposes, we consider the case $k = 2$: sets of only *two* rulers with the property that all measured distances of the two rulers combined are distinct, and such pairs of rulers will be called *spanning birulers.*

The two Fibonacci subsequences $\{f_{2n-1}\}$ and $\{f_{2n}\}$ (for all $n \geq 1$) considered in Section 3 *supra* are an example of *infinite spanning birulers*, where each of the two sequences has exponential growth.

We will now construct a pair of sequences $A = \{a_1, a_2, a_3, \ldots\}$ and $B = \{b_1, b_2, b_3, \ldots\}$, with $a_1 = b_1 = 1$, as an infinite spanning biruler, using the "greedy algorithm" to adjoin terms alternately to sequence A and to sequence B. The two sequences constructed in this manner begin as follows:

$$\begin{aligned} A &= \{1, 2, 5, 11, 22, 41, 65, 83, 121, 152, \ldots\} \\ B &= \{1, 3, 8, 16, 30, 53, 78, 104, 137, 190, \ldots\} \end{aligned}$$

The non-overlapping and repeat-free *difference triangles* for these two sequences are:

A: 1, 2, 5, 11, 22, 41, 65, 83, 121, 152, ...

1 3 6 11 19 24 18 38 31

4 9 17 30 43 42 56 69

10 20 36 54 61 80 87

21 39 60 72 99 111

40 63 78 110 130

64 81 116 141

82 119 147

120 150

151

Thus, $\Delta A = \{1, 3, 4, 6, 9, 10, 11, 17, 18, 19, 20, 21, 24, 31, 36, 38, 39, 40, 42, 43, 54, 56, 60, 61, 63, 64, 66, 69, 72, 78, 80, 81, 82, 87, 99, 110, 111, 116, 119, 120, 130, 141, 147, 150, 151, \ldots$

B: 1, 3, 8, 16, 30, 53, 78, 104, 137, 190, ...

2 5 8 14 23 25 26 33 53

7 13 22 37 48 51 59 86

15 27 45 62 74 84 112

29 50 70 88 107 137

52 75 96 121 160

77 101 129 174

103 134 182

136 187

189

Thus, $\Delta B = \{2, 5, 7, 8, 13, 14, 15, 22, 23, 25, 26, 27, 29, 33, 37, 45, 48, 50, 51, 52, 53, 59, 62, 70, 74, 75, 77, 84, 86, 88, 96, 101, 103, 107, 112, 121, 129, 134, 136, 137, 160, 174, 182, 187, 189, \ldots\}$

The numbers not yet used as differences in either ΔA or ΔB, thus far, are: 12, 16, 28, 30, 32, 34, 35, 41, 44, 46, 47, 49, 55, 57, 58, 65, 67, 68, 71, 73, 76, 79, 83, 85, 89, 90, 91, 92, 93, 94, 95, 97, 98, 100, 102, 104, 105, 106, 108, 109, 113, 114, 117, 118, 122, 123, 124, 125, 126, 127, 128, 131, 132, 133, 135, 138, 139, 140, 142, 143, 144, 145, 146, 148, 149, and all numbers from 152 onward *except* $160, 174, 182, 187$, and 189. Many of these as yet unused differences will occur later on in either ΔA or ΔB as the sequences A and B are extended further. For example, when the next eligible term, 210, is adjoined to sequence A, the new differences generated in ΔA are $58, 89, 127, 145, 169, 188, 199, 205, 208$, and 209, thereby removing these numbers from the above list of "not yet-used differences".

Theorem 5. *If two sequences $A = \{a_i\}$ and $B = \{b_i\}$, all $i \geq 1$, are constructed taking $a_i = b_i = 1$, and then adjoining new terms alternately to A and B (i.e. in the sequence $a_2, b_2, a_3, b_3, a_4, b_4, \ldots$) with the constraint that all differences $\Delta A = \{a_j - a_i\}$ from A, and $\Delta B = \{b_j - b_i\}$ from B, be disjoint (i.e. $(\Delta A) \cap (\Delta B) = \emptyset$), with or without additional restrictions on whether or not terms within ΔA, and/or within ΔB, be distinct, the construction process may be continued indefinitely.*

Proof. At any finite stage in the construction, a largest integer t will have been adjoined to either A or B. Then any integer $u \geq 2t$ can be adjoined next, since all numbers $u - a_i$ and $u - b_i$ will be bigger than anything already in $(\Delta A) \cup (\Delta B)$. (Note that u will be adjoined to *either A or B*, but not to both, so it will not put $u - 1$ in both ΔA and ΔB.) □

Remark 2

1. If we simply take $u = 2t$ every time, we get $A = \{1, 2, 8, 32, 128, \ldots\}$ with $a_n = 2 \cdot 4^{n-2}$ for all $n > 1$, and $B = \{1, 4, 16, 64, 256, \ldots\}$ with $b_n = 4^{n-1}$ for all $n \geq 1$. Here, $(\Delta A) \cup (\Delta B)$ consists entirely of distinct integers, and both A and B grow like powers of 4.

2. The Fibonacci example in Section 3 already provided a pair of sequences with a smaller exponential growth rate, the powers of $\frac{(3+\sqrt{5})}{2} = 2.618\ldots$. Slower growth rates seem possible, especially if we do not require that only distinct values occur within ΔA and within ΔB.
3. It seems reasonable to conjecture that the sequences A and B as constructed above by the greedy algorithm have polynomial growth rate. However, we can show that *at least* quadratic growth rate must occur for at least one of any pair of sequences that form an infinite spanning biruler, as follows.

Theorem 6. *The lengths $L_A(n)$ and $L_B(n)$ of any pair of spanning birulers, $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ must satisfy max $(L_A(n), L_B(n)) \geq n(n-1)$.*

Proof. A ruler with n marks has $\binom{n}{2} = \frac{n(n-1)}{2}$ measured distances, so two such rulers have $n(n-1)$ measured distances. If all of these measured distances are distinct, at least one of the rulers must measure a length $L \geq n(n-1)$. □

Stronger lower bounds can be obtained using the techniques employed to obtain lower bounds on the lengths of Golomb rulers.

8 Sequences with Repeated Differences

For two infinite integer sequences A and B to have $C_{AB}(\tau) \leq 1$ for all $\tau \in (-\infty, \infty)$, it is sufficient but not necessary that A and B constitute a pair of infinite spanning birulers. The necessary and sufficient condition, namely $(\Delta A) \cap (\Delta B) = \emptyset$, requires only that none of the differences of terms in sequence A coincide with any of the differences of terms in sequence B. This allows repeated differences separately within ΔA and within ΔB.

Using the greedy algorithm again, but with this weaker constraint, we get new sequences A and B that do not grow quite as fast as those in the previous section. Here,

$$A = \{1, 2, 5, 11, 20, 35, 46, 68, 86, 92, \ldots\}$$
$$B = \{1, 3, 8, 15, 28, 40, 57, 77, 104, 116, \ldots\}$$

The difference triangles for these sequences are:

A: 1, 2, 5, 11, 20, 35, 46, 68, 86, 92, ...

1 3 6 9 15 11 22 18 6

4 9 15 24 26 33 40 24

10 18 30 35 48 51 46

19 33 41 57 66 57

34 44 63 75 72

45 66 81 81

67 84 87

85 90

91

with $\Delta A = \{$ 1, 3, 4, 6, 9, 10, 11, 15, 18, 19, 22, 24, 26, 30, 33, 34, 40, 41, 44, 45, 46, 48, 57, 63, 66, 67, 72, 75, 81, 84, 85, 87, 90, 91, $\ldots\}$

and

B: 1, 3, 8, 15, 28, 40, 57, 77, 104, 116, ...

2 5 7 13 12 17 20 27 12
7 12 20 25 29 37 47 39
14 25 32 42 49 64 59
27 37 49 62 76 76
39 54 69 89 88
56 74 96 101
76 101 108
103 113
115

with $\Delta B = \{$ 2, 5, 7, 12, 13, 14, 17, 20, 25, 27, 29, 32, 37, 39, 42, 47, 49, 54, 56, 59, 62, 64, 69, 74, 76, 88, 89, 96, 101, 103, 108, 113, 115, ...$\}$.

Note that although A and B are each necessarily increasing sequences, and were constructed by alternately adjoining new terms to A and B by the greedy algorithm (i.e. taking the smallest next term consistent with $(\Delta A) \cap (\Delta B) = \emptyset$), the *tenth* term of sequence A (namely $a_{10} = 92$) is smaller than the *ninth* term of sequence B (namely $b_9 = 104$).

As another example, we will form sequences $C = \{c_i\}$ and $D = \{d_i\}$ with $(\Delta C) \cap (\Delta D) = \emptyset$, where we take $C = \{$ 1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331, 1728, ...$\}$ to be the sequence of perfect cubes, and we form D by the greedy algorithm.

The difference triangle for C is:

C: 1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331, 1728, 2197, ...

7 19 37 61 91 127 169 217 271 331 397 469
26 56 98 152 218 296 386 488 602 728 866
63 117 189 279 387 513 657 819 999 1197
124 208 316 448 604 784 988 1216 1468
215 335 485 665 875 1115 1385 1685
342 504 702 936 1206 1512 1854
511 721 973 1267 1603 1981
728 992 1304 1664 2072
999 1323 1701 2133
1330 1720 2170
1727 2189
2196

There are 110 distinct members of ΔC below 2500. (The above table does not contain them all.) These are: $\Delta C = \{$7, 19, 26, 37, 56, 61, 63, 91, 98, 117, 124, 127, 152, 169, 189, 208, 215, 217, 218, 271, 279, 296, 316, 331, 335, 342, 386, 387, 397, 448, 469, 485, 488, 504, 511, 513, 547, 602, 604, 631, 657, 665, 702, 721, 728, 784, 817, 819, 866, 875, 919, 936, 973, 988, 992, 999, 1016, 1027, 1115, 1141, 1178, 1197, 1206, 1216, 1261, 1267, 1304, 1323, 1330, 1352, 1385, 1387, 1413, 1468, 1512, 1519, 1538, 1603, 1647, 1657, 1664, 1685, 1701, 1720, 1727,

1736, 1744, 1801, 1854, 1899, 1946, 1951, 1981, 2015, 2044, 2072, 2107, 2168, 2169, 2170, 2189, 2196, 2232, 2269, 2368, 2375, 2401, 2402, 2437, 2457}.

Note that as a multiset, ΔC contains infinitely many duplicates. Three of these occur below 2500: $721 = 16^3 - 15^3 = 9^3 - 2^3, 728 = 12^3 - 10^3 = 9^3 - 1^3, 999 = 10^3 - 1^3 = 12^3 - 9^3$. (Remember Ramanujan's famous observation to Hardy that $1729 = 12^3 + 1^3 = 10^3 + 9^3$, which accounts for two of the three examples just given.) Up to 2500, ΔC has several pairs of consecutive integers, and one triple: $(2168, 2169, 2170)$.

Note that ΔC can contain no cubes (by Fermat's Last Theorem, for the exponent 3). We use the greedy algorithm to construct the infinite sequence $D = \{d_1, d_2, d_3, \ldots\}$ of positive integers such that $(\Delta C) \cap (\Delta D) = \emptyset$.

$D = \{$ 1, 2, 3, 4, 5, 6, 7, 15, 16, 17, 18, 19, 46, 47, 48, 49, 50, 51, 89, 90, 91, 160, 161, 162, $\ldots\}$

Here is the difference triangle to generate ΔD.

D: 1, 2, 3, 4, 5, 6, 7, 15, 16, 17, 18, 19, 46, 47, 48, 49, 50, 51, 89, 90, 91, 160, 161, 162, ...

1 1 1 1 1 1 8 1 1 1 1 27 1 1 1 1 1 38 1 1 69 1 1
2 2 2 2 2 9 9 2 2 2 28 28 2 2 2 2 39 39 2 70 70 2
3 3 3 3 10 10 10 3 3 29 29 29 3 3 3 40 40 40 71 71 71
4 4 4 11 11 11 11 4 30 30 30 30 4 4 41 41 41 109 72 72
5 5 12 12 12 12 12 31 31 31 31 31 5 42 42 42 110 110 73
6 13 13 13 13 13 39 32 32 32 32 32 43 43 43 111 111 111
14 14 14 14 14 40 40 33 33 33 33 76 44 44 112 112 112
15 15 15 15 41 41 41 34 34 34 71 71 45 113 113 113
16 16 16 42 42 42 42 35 35 72 72 72 114 114 114
17 17 43 43 43 43 43 36 73 73 73 141 115 115
18 44 44 44 44 44 44 74 74 74 142 142 116
45 45 45 45 45 45 82 75 75 143 143 143
46 46 46 46 46 83 83 76 144 144 144
47 47 47 47 84 84 84 145 145 145
48 48 48 85 85 85 153 146 146
49 49 86 86 86 154 154 147
50 87 87 87 155 155 155
88 88 88 156 156 156
89 89 157 157 157
90 158 158 158
159 159 159
160 160
161

Thus far, below 162, ΔD omits only $\{7, 19-26, 37, 51-68, 77-82, 91-108, 117-140, 148-152\}$, thus avoiding {7, 19, 26, 37, 56, 61, 63, 91, 98, 117, 124, 127, 152} which are the numbers in ΔC below 162.

Since the sequence C contains arbitarily large terms, the proof given earlier, in Theorem 5, that the greedy algorithm does not terminate when adjoining new terms to two sequences by alternating between them, does not apply to the construction here of the sequence D. It seems likely that D will be an infinite sequence, and of greater density than the sequence C, but no proof is currently available.

It would be a research goal to find an *explicit* sequence D', with polynomial growth (preferable no faster than cubic growth) with $(\Delta C) \cap (\Delta D') = \emptyset$. A failed attempt would be to try $D' = \{n^3 + n\}$, but this $\Delta D'$ does have a very sparse intersection with ΔC. (E.g., $604 = (11^3 + 11) - (9^3 + 9) = 9^3 - 5^3$.)

If $A = \{\binom{n}{2}\}$ for all $n \geq 2, \Delta A$ contains every positive integer greater than 1, so there can be no infinite sequence B of positive integers with $(\Delta A) \cap (\Delta B) = \emptyset$.

If $A = \{n^2\}$ for all $n \geq 1$, the only positive integers not found in ΔA are $1, 4$, and $4k + 2$ for all $k \geq 0$. The set $B = \{2, 4, 6, 8\}$, with only four elements, is the largest set of positive integers with $(\Delta A) \cap (\Delta B) = \emptyset$ for this choice of sequence A.

It is an open question whether two sequences A and B, each with quadratic rates of growth, can be shown to exist, or proved not to exist, with $(\Delta A) \cap (\Delta B) = \emptyset$.

9 Conclusions

With every infinite sequence $A = \{a_n\}_{n=1}^{\infty}$ of positive integers, we associate an infinite binary sequence $\overline{A} = \{\alpha_k\}_{k=1}^{\infty}$ where $\alpha_k = 1$ if $k = a_n$ for any n, $\alpha_k = 0$ otherwise. If $B = \{b_n\}_{n=1}^{\infty}$ is a second infinite sequence of positive integers, and $\overline{B} = \{\beta_k\}_{k=1}^{\infty}$ where $\beta_k = 1$ if $k = b_n$ for any n, $\beta_k = 0$ otherwise, then we define the (unnormalized, infinite) crosscorrelation $C_{AB}(\tau) = \sum_{k=1}^{\infty} \alpha_k \beta_{k+\tau}$ for all $\tau, -\infty < \tau < +\infty$. We are interested in pairs of sequences, A and B, where $C_{AB}(\tau)$ is finite for all integers τ.

Two infinite sequences A and B of positive integers cannot have $C_{AB}(\tau) = 0$ for all τ. In fact, there must be infinitely many values of τ for which $C_{AB}(\tau) \geq 1$.

The most restrictive case we considered was where $C_{AB}(\tau) \leq 1$ for all $\tau \in Z$. Example of such pairs of sequences were given. With $P = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$, the sequence of the primes, we exhibited a sequence A such that $C_{AP}(\tau) \leq |\tau|$ for all $\tau \in Z$. We showed that de Polignac's Conjecture (the case $k = 2$ of the "prime k-tuples conjecture") implies $C_{AP}(\tau) > 1$ for infinitely many integers τ. We also observed that "Golomb's Conjecture", the existence of a sequence A for which $C_{AP}(\tau) < K$ for all $\tau \in Z$, where K is a finite bound independent of τ, is inconsistent with the "prime k-tuples conjecture."

Numerous examples where $(\Delta \mathrm{A}) \cap (\Delta \mathrm{B}) = \emptyset$ are possible, giving $C_{AB}(\tau) \leq 1$ for all $\tau \in Z$. One situation takes A and B to be a pair of *spanning birulers,* where all differences are distinct within ΔA and ΔB, and non-overlapping between ΔA and ΔB. A weaker restriction allows repeated differences within ΔA and ΔB separately, but still requires ΔA and ΔB to be non-overlapping. Various examples can be constructed using the greedy algorithm.

Acknowledgements

1. The Fibonacci example in Section 3 was one of several examples that emerged from a discussion with N.J.A. Sloane and J.H. Conway in March, 2010.
2. My formulation of "Golomb's Conjecture" in terms of cross-correlation was an outgrowth of a discussion with Peter Sarnak in January, 2010.
3. Noah Olsman, an undergraduate student at USC, performed useful computer calculations during Spring, 2010.

References

1. Problem 10208. Amer. Math. Monthly (1992)
2. Golomb, S.W., Taylor, H.: Cyclic projective planes, perfect circular rulers, and good spanning rulers. In: Sequences and their Applications, Bergen, pp. 166–181 (2001); Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London (2002)
3. Ribenboim, P.: The little book of bigger primes, 2nd edn. Springer, New York (2004)

Reed Muller Sensing Matrices and the LASSO
(Invited Paper)

Robert Calderbank[1] and Sina Jafarpour[2]

[1] Department of Electrical Engineering and Department of Mathematics.
Princeton University
calderbk@math.princeton.edu
[2] Department of Computer Science. Princeton University
sina@cs.princeton.edu

Abstract. We construct two families of deterministic sensing matrices where the columns are obtained by exponentiating codewords in the quaternary Delsarte-Goethals code $DG(m, r)$. This method of construction results in sensing matrices with low coherence and spectral norm. The first family, which we call Delsarte-Goethals frames, are 2^m - dimensional tight frames with redundancy 2^{rm}. The second family, which we call Delsarte-Goethals sieves, are obtained by subsampling the column vectors in a Delsarte-Goethals frame. Different rows of a Delsarte-Goethals sieve may not be orthogonal, and we present an effective algorithm for identifying all pairs of non-orthogonal rows. The pairs turn out to be duplicate measurements and eliminating them leads to a tight frame. Experimental results suggest that all $DG(m, r)$ sieves with $m \leq 15$ and $r \geq 2$ are tight-frames; there are no duplicate rows. For both families of sensing matrices, we measure accuracy of reconstruction (statistical $0-1$ loss) and complexity (average reconstruction time) as a function of the sparsity level k. Our results show that DG frames and sieves outperform random Gaussian matrices in terms of noiseless and noisy signal recovery using the LASSO.

Keywords: Compressed Sensing, Reed-Muller Codes, Delsarte-Goethals Set, Random Sub-dictionary, LASSO.

1 Introduction

The central goal of compressed sensing is to capture attributes of a signal using very few measurements. In most work to date, this broader objective is exemplified by the important special case in which the measurement data constitute a vector $f = \Phi\alpha + e$, where Φ is an $N \times \mathcal{C}$ matrix called the *sensing matrix*, α is a signal in $\mathbb{C}^{\mathcal{C}}$, that is well-approximated by a k-sparse vector (a signal with at most k non-zero entries), and e is additive measurement noise.

The role of random measurement in compressive sensing (see [1] and [2]) can be viewed as analogous to the role of random coding in Shannon theory. Both provide worst-case performance guarantees in the context of an adversarial signal/error model. In the standard paradigm, the measurement matrix is required

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 442–463, 2010.

to act as a near isometry on all k-sparse signals (this is the Restricted Isometry Property or RIP introduced in [3]). It has been shown that if a sensing matrix satisfies the RIP property then Basis pursuit [1,4] programs can be used to estimate the best k-term approximation of any signal in $\mathbb{C}^C$, measured in the presence of any ℓ_2 norm bounded measurement noise [5].

It is known that certain probabilistic processes generate sensing matrices that for $k = O(N)$ satisfy k-RIP with high probability (see [6]). This is significantly different from the best known results for deterministic sensing matrices [7] where k-RIP is known only for $k = O(\sqrt{N})$. We normalize the columns of a sensing matrix to have unit ℓ_2 - norm and define the worst case coherence μ to be the maximum absolute value of an inner product of distinct columns. It follows from the Welch bound [8] that $\mu \geq O\left(\frac{1}{\sqrt{N}}\right)$. When $\mu = O\left(\frac{1}{\sqrt{N}}\right)$ it then follows from the Gerschgorin Circle Theorem [9] that the sensing matrix satisfies k-RIP with $k = O\left(\mu^{-1}\right)$. In general however no polynomial-time algorithm is known for verifying that a sensing matrix with the worst-case coherence μ satisfies k-RIP with $k = \Omega\left(\mu^{-1}\right)$.

The RIP property is not an end in itself. It provides guarantees for a particular method of signal reconstruction, but there is significant interest in structured sensing matrices and alternative reconstruction algorithms. One example is the adjacency matrices of expander graphs [10,11] where it is known to be impossible to satisfy RIP with respect to the ℓ_2 norm [12]. Sparse signal recovery is still possible with Basis Pursuit since the adjacency matrix acts like a near isometry on k-sparse signals with respect to the ℓ_1 norm. However error estimates are looser than corresponding estimates for random sensing matrices and resilience to measurement noise is limited to sparse noise vectors.

The coherence between rows of a sensing matrix is a measure of the new information provided by an additional measurement. The coherence between columns of a sensing matrix is fundamental to deriving performance guarantees for reconstruction algorithms such as Basis Pursuit. There are two fundamental measures of coherence: The worst-case coherence μ which measures the maximal coherence between the columns of the sensing matrix, and the spectral norm $\|\Phi\|_2$ which measures the maximal coherence between the rows of the frame. The ideal case is when worst case coherence between columns matches the Welch bound $\left(\mu = O\left(\frac{1}{\sqrt{N}}\right)\right)$ and different measurements are orthogonal. Then, with high probability a k-sparse vector has a unique sparse representation [13], and this representation can be efficiently recovered using a LASSO program [14]. Section §2 introduces notation and reviews prior work on the geometry of sensing matrices and the performance of the LASSO reconstruction algorithm.

In this paper we consider sensing matrices based on the $\mathbb{Z}_4$-linear representation of Delsarte Goethals codes. The columns are obtained by exponentiating codewords in the quaternary Delsarte-Goethals code; they are uniformly and very precisely distributed over the surface of an N-dimensional sphere. Coherence between columns reduces to properties of these algebraic codes. Section §2 reviews the construction of Delsarte-Goethals (DG) sets of $\mathbb{Z}_4$-linear quadratic forms which is the starting point for the construction of the corresponding codes;

each quadratic form determines a codeword where the entries are the values taken by quadratic form. Section §3 introduces Delsarte-Goethals frames and Delsarte-Goethals sieves; the columns of these sensing matrices are obtained by exponentiating DG codewords. We then determine the worst case coherence and spectral norm for these sensing matrices.

Candès and Plan [14] specified coherence conditions under which a LASSO program will successfully recover a k-sparse signal when the k non-zero entries are above the noise variance. We use these results to provide an average case error analysis for stochastic noise in both the data and measurement domains. The Delsarte Goethals (DG) sensing matrices are essentially tight frames so that white noise in the data domain maps to white noise in the measurement domain.

Section §4 presents the results of numerical experiments that compare DG frames and sieves with random Gaussian matrices of the same size. The SpaRSA package [15] is used to implement the LASSO recovery algorithm in all cases. DG frames and sieves outperform random matrices in terms of probability of successful sparse recovery but reconstruction time for the DG sieve is greater than that for the other sensing matrices. We remark that there are alternative fast reconstruction algorithms that exploit the structure of DG sensing matrices. The witnessing algorithm proposed in [16] requires less storage, provides support-localized detection, and does not require independence among the support entries. On the other hand, LASSO reconstruction tends to be more robust to noise in the data domain.

2 Background and Notation

This Section introduces notation and reviews the theory of sparse reconstruction.

2.1 Notation

Given a vector $v = (v_1, \cdots, v_n)$ in $\mathbb{R}^n$, $\|v\|_2$ denotes the Euclidean norm of v, and $\|v\|_1$ denotes the ℓ_1 norm of v defined as $\|v\|_1 \doteq \sum_{i=1}^{n} |v_i|$. We further define $\|v\|_\infty \doteq \max\{|v_1|, \cdots, |v_n|\}$, and $\|v\|_{\min} \doteq \min\{|v_1|, \cdots, |v_n|\}$. Also the Hamming weight of v is defined as $\|v\|_0 \doteq \{i : v_i \neq 0\}$. Whenever clear from the context, we drop the subscript from the ℓ_2 norm. Also $v_{i\to j}$ denotes the vector v restricted to entries $i, i+1, \cdots, j$, that is $v_{i\to j} \doteq (v_i, v_{i+1}, \cdots, v_j)$.

The transpose of a matrix A is denoted by $A^\top$. If A is a matrix with complex entries, then we denote the conjugate transpose of A by $A^\dagger$. Given a complex valued matrix A with rank r, let $\boldsymbol{\sigma} = [\sigma_1, \cdots, \sigma_r]$ denote the vector of the singular values of A. The spectral norm $\|A\|$ of a matrix A is the largest singular value of A: that is $\|A\| \doteq \|\boldsymbol{\sigma}\|_\infty$. The condition number of A is the ratio between its largest and its smaller singular values: $\varsigma(A) \doteq \frac{\|\boldsymbol{\sigma}\|_\infty}{\|\boldsymbol{\sigma}\|_{\min}}$. Finally the nuclear norm of A, denoted as $\|A\|_1$ is the ℓ_1 norm of the singular value vector $\boldsymbol{\sigma}$.

Throughout this paper we shall use the notation φ_j for the j^{th} column of the sensing matrix Φ; its entries will be denoted by $\varphi_j(x)$, with the row label x varying from 0 to $N-1$. In other words, $\varphi_j(x)$ is the entry of Φ in row x and

column j. We denote the set $\{1, \cdots .\mathcal{C}\}$ by $[\mathcal{C}]$. Let S be a subset of $[\mathcal{C}]$. Φ_S is obtained by restricting Φ to those columns that are listed in S.

A vector $\alpha \in \mathbb{R}^{\mathcal{C}}$ is k-sparse if it has at most k non-zero entries. The support of the k-sparse vector α, denoted by $\mathrm{Supp}(\alpha)$, contains the indices of the non-zero entries of α. Let $\pi = \{\pi_1, \cdots, \pi_{\mathcal{C}}\}$ be a uniformly random permutation of $[\mathcal{C}]$. In this paper, our focus is on the average case analysis, and we always assume that α is a k-sparse signal with $\mathrm{Supp}(\alpha) = \{\pi_1, \cdots, \pi_k\}$. We further assume that conditioned on the support, the values of the k non-zero entries of α are sampled from a distribution which is absolutely continuous with respect to the Lebesgue measure on $\mathbb{R}^k$.

2.2 Incoherent Tight Frames

An $N \times \mathcal{C}$ matrix Φ with normalized columns is called a dictionary. A dictionary is a tight-frame with redundancy $\frac{\mathcal{C}}{N}$ if for every vector $v \in \mathbb{R}^{\mathcal{C}}$, $\|\Phi v\|^2 = \frac{\mathcal{C}}{N}\|v\|^2$. If $\Phi\Phi^\dagger = \frac{\mathcal{C}}{N}\mathrm{I}_{N\times N}$, then Φ is a tight-frame with redundancy $\frac{\mathcal{C}}{N}$ (see [17]).

Proposition 1. *Let Φ be an $N \times \mathcal{C}$ dictionary. Then $\|\Phi\|^2 \geq \frac{\mathcal{C}}{N}$, and equality holds if and only if Φ is a tight frame with redundancy $\frac{\mathcal{C}}{N}$.*

Proof. Let $\boldsymbol{\sigma}$ be the singular value vector of Φ. We have

$$\|\Phi\|^2 = \|\boldsymbol{\sigma}\|_\infty^2 \geq \frac{1}{N}\sum_{i=1}^{N}\sigma_i^2 = \frac{1}{N}\mathrm{Tr}\left(\Phi\Phi^\dagger\right) = \frac{\mathcal{C}}{N}. \tag{1}$$

The inequality in Equation (1) changes to equality if and only if all the eigenvalues of $\Phi\Phi^\dagger$ are equal to $\frac{\mathcal{C}}{N}$. This is equivalent to the requirement $\Phi\Phi^\dagger = \frac{\mathcal{C}}{N}\mathrm{I}_{N\times N}$.

The mutual coherence between the columns of an $N \times \mathcal{C}$ sensing matrix is defined as

$$\mu \doteq \max_{i\neq j}\left|\varphi_i^\dagger\varphi_j\right|. \tag{2}$$

Strohmer and Heath [8] showed that the mutual coherence of any $N \times \mathcal{C}$ dictionary is at least $\frac{1}{\sqrt{N}}$. Designing dictionaries with small spectral norms (tight frames in the ideal case), and with small coherence ($\mu = O\left(\frac{1}{\sqrt{N}}\right)$ in the ideal case) is useful in compressed sensing for the following reasons.

Uniqueness of Sparse Representation (ℓ_0 minimization). The following results are due to Tropp [13] and show that with overwhelming probability the ℓ_0 minimization program successfully recovers the original k-sparse signal.

Theorem 1. *Assume the dictionary Φ satisfies $\mu \leq \frac{c}{\log \mathcal{C}}$, where c is an absolute constant. Further assume $k \leq \frac{c\,\mathcal{C}}{\|\Phi\|^2 \log \mathcal{C}}$. Let S be a random subset of $[\mathcal{C}]$ of size k, and let Φ_S be the corresponding $N \times k$ submatrix. Then there exists an absolute constant c_0*

$$\Pr\left[\left\|\Phi_S^\dagger\Phi_S - I\right\| \geq c_0\left(\mu\log\mathcal{C} + 2\sqrt{\frac{\|\Phi\|^2\,k}{\mathcal{C}}}\right)\right] \leq 2\,\mathcal{C}^{-1}.$$

Theorem 2. *Assume the dictionary Φ satisfies $\mu \leq \frac{c}{\log \mathcal{C}}$, where c is an absolute constant. Further assume $k \leq \frac{c\,\mathcal{C}}{\|\Phi\|^2 \log \mathcal{C}}$. Let α be a k-sparse vector, such that the support of the k nonzero coefficients of α is selected uniformly at random. Then with probability $1 - O\left(\mathcal{C}^{-1}\right)$ α is the unique k-sparse vector mapped to $u = \Phi\alpha$ by the measurement matrix Φ.*

Sparse Recovery via LASSO (ℓ_1 minimization). Uniqueness of sparse representation is of limited utility given that ℓ_0 minimization is computationally intractable. However, given modest restrictions on the class of sparse signals, Candès and Plan [14] have shown that with overwhelming probability the solution to the ℓ_0 minimization problem coincides with the solution to a convex lasso program.

Theorem 3. *Assume the dictionary Φ satisfies $\mu \leq \frac{c}{\log \mathcal{C}}$, where c is an absolute constant. Further assume $k \leq \frac{c_1\,\mathcal{C}}{\|\Phi\|^2 \log \mathcal{C}}$, where c_1 is a constant. Let α be a k-sparse vector, such that*

1. *The support of the k nonzero coefficients of α is selected uniformly at random.*
2. *Conditional on the support, the signs of the nonzero entries of α are independent and equally likely to be -1 or 1.*

Let $u = \Phi\alpha + e$, where e contains N iid $\mathcal{N}(0, \sigma^2)$ Gaussian elements. Then if $\|\alpha\|_{\min} \geq 8\sigma\sqrt{2\log \mathcal{C}}$, with probability $1 - O(\mathcal{C}^{-1})$ the lasso estimate

$$\alpha^* \doteq \arg\min_{\alpha^+ \in \mathbb{R}^{\mathcal{C}}} \frac{1}{2}\|u - \Phi\alpha^+\|^2 + 2\sqrt{2\log \mathcal{C}}\,\sigma^2\,\|\alpha^+\|_1$$

has the same support and sign as α, and $\|\Phi\alpha - \Phi\alpha^*\|^2 \leq c_2\,k\,\sigma^2$, where c_2 is a constant independent of α.

Stochastic noise in the data domain. The tight-frame property of the sensing matrix makes it possible to map iid Gaussian noise in the data domain to iid Gaussian noise in the measurement domain:

Lemma 1. *Let ε be a vector with $\mathcal{C}$ iid $\mathcal{N}(0, \sigma_d^2)$ entries and e be a vector with N iid $\mathcal{N}(0, \sigma_m^2)$ entries. Let $\hbar = \Phi\varepsilon$ and $\nu = \hbar + e$. Then ν contains N entries, sampled iid from $\mathcal{N}\left(0, \sigma^2\right)$, where $\sigma^2 = \frac{\mathcal{C}}{N}\sigma_d^2 + \sigma_m^2$.*

Proof. The tight frame property implies

$$\mathbb{E}\left[\hbar\hbar^\dagger\right] = E[\Phi\varepsilon\varepsilon^\dagger\Phi^\dagger] = \sigma_d^2\Phi\Phi^\dagger = \frac{\mathcal{C}}{N}\sigma_d^2\,I.$$

Therefore, $\nu = \hbar + e$ contains iid Gaussian elements with zero mean and variance σ^2.

Next we construct two families of low-coherence tight frames from Delsarte-Goethals codes.

2.3 Delsarte-Goethals Sets of Binary Symmetric Matrices

The finite field $\mathbb{F}_{2^m}$ is obtained from the binary field $\mathbb{F}_2$ by adjoining a root ξ of a primitive irreducible polynomial g of degree m. The elements of $\mathbb{F}_{2^m}$ are polynomials in ξ of degree at most $m-1$ with coefficients in $\mathbb{F}_2$, and we will identify the polynomial $x_0 + x_1\xi + \cdots + x_{m-1}\xi^{m-1}$ with the binary m-tuple $(x_0, \cdots, x_{m-1})$. The *Frobenius map* $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is defined by $f(x) = x^2$ and the *Trace map* $\mathrm{Tr} : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is defined by

$$\mathrm{Tr}(x) \doteq x + x^2 + \cdots + x^{2^{m-1}}.$$

The identity $(x+y)^2 = x^2 + y^2$ implies that $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$; the trace is a linear map over the binary field $\mathbb{F}_2$. The trace inner product given by $(v, w) = \mathrm{Tr}(vw)$ is non-degenerate; if $\mathrm{Tr}(vz) = 0$ for all z in $\mathbb{F}_2^m$ then $v = 0$. Every element a in $\mathbb{F}_{2^m}$ determines a symmetric bilinear form $\mathrm{Tr}[xya]$ to which is associated a binary symmetric matrix $P^0(a)$.

$$\mathrm{Tr}[xya] \doteq (x_0 \cdots x_{m-1})P^0(a)(y_o \cdots y_{m-1})^\top.$$

The *Kerdock set* $\boldsymbol{K_m}$ is the m-dimensional binary vector space formed by the matrices $P^0(a)$. For example, let $m = 3$, and assume the finite field $\mathbb{F}_8$ is generated by adjoining a root ξ of the polynomial $g(x) = x^3 + x + 1$. Then K_3 is spanned by

$$P^0(100) = \begin{pmatrix} 1\,0\,0 \\ 0\,0\,1 \\ 0\,1\,0 \end{pmatrix}, \quad P^0(010) = \begin{pmatrix} 0\,0\,1 \\ 0\,1\,0 \\ 1\,0\,1 \end{pmatrix}, \text{ and } P^0(001) = \begin{pmatrix} 0\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \end{pmatrix}$$

Theorem 4. *Every nonzero matrix in K_m is nonsingular.*

Proof. If $xP^0(a) = 0$ then $\mathrm{Tr}[xya] = 0$ for all $y \in \mathbb{F}_{2^m}$. Now the non-degeneracy of the trace implies $a = 0$.

Next we define higher order bilinear forms, each associated with a binary symmetric matrix. Given a positive integer t where $0 < t \leq \frac{m-1}{2}$ and given a field element a

$$\mathrm{Tr}\left[\left(xy^{2^t} + x^{2^t}y\right)a\right]$$

defines a symmetric bilinear form that is represented by a binary symmetric matrix $P^t(a)$ as above:

$$\mathrm{Tr}\left[\left(xy^{2^t} + x^{2^t}y\right)a\right] \doteq (x_0 \cdots x_{m-1})P^t(a)(y_o \cdots y_{m-1})^\top \tag{3}$$

The *Delsarte-Goethals set* $DG(m, r)$ is then defined as

$$DG(m,r) \doteq \left\{ \sum_{t=0}^{r} P^t(a_t) \,|\, a_t \in \mathbb{F}_{2^m},\ t = 0, 1, \cdots, r \right\}.$$

The Delsarte-Goethals sets are nested

$$K_m = DG(m,0) \subset DG(m,1) \subset \cdots \subset DG\left(m, \frac{m-1}{2}\right),$$

and every bilinear form is associated with some matrix in $DG\left(m, \frac{m-1}{2}\right)$.

For example, let $m = 3$ and $g(x) = x^3 + x + 1$, the set $DG(3,1)$ is spanned by K_3, and

$$P^1(100) = \begin{pmatrix} 0\,0\,0 \\ 0\,0\,1 \\ 0\,1\,0 \end{pmatrix}, \quad P^1(010) = \begin{pmatrix} 0\,1\,0 \\ 1\,0\,0 \\ 0\,0\,0 \end{pmatrix}, \text{ and } P^1(001) = \begin{pmatrix} 0\,1\,1 \\ 1\,0\,0 \\ 1\,0\,0 \end{pmatrix}.$$

Theorem 5. *Every nonzero matrix in $DG(m,r)$ has rank at least $m - 2r$.*

Proof. If x is in the null space of $\sum_{t=0}^{r} P^t(a_t)$, then for all $y \in \mathbb{F}_{2^m}$

$$\mathrm{Tr}\left[xya_0 + \sum_{t=1}^{r}\left(xy^{2^t} + x^{2^t}y\right)a_t\right] = 0.$$

Since $\mathrm{Tr}(x) = \mathrm{Tr}(x^2) = \cdots = \mathrm{Tr}\left(x^{\frac{1}{2}}\right)$ we have

$$\mathrm{Tr}\left[\left((xa_0)^{2^r} + \sum_{t=1}^{r}(xa_t)^{2^{t-r}} + a_t^{2^r}\,x^{2^{t+r}}\right)y^{2^r}\right] = 0.$$

Non-degeneracy of the trace now implies

$$(xa_0)^{2^r} + \sum_{t=1}^{r}(xa_t)^{2^{t-r}} + a_t^{2^r}\,x^{2^{t+r}} = 0.$$

The LHS is a polynomial of degree at most 2^{2r} so there are at most 2^{2r} solutions. Hence the rank of the binary symmetric matrix $\sum_{t=0}^{r} P^t(a_t)$ is at least $m - 2r$.

3 Delsarte-Goethals Sensing

3.1 Delsarte-Goethals Frames

We start by picking an odd number m. The 2^m rows of the sensing matrix Φ are indexed by the binary m-tuples x, and the $2^{(r+2)m}$ columns are indexed by the pairs P, b, where P is an $m \times m$ binary symmetric matrix in the Delsarte-Goethals set $DG(m,r)$, and b is a binary m-tuple. The entry $\varphi_{P,b}(x)$ is given by

$$\varphi_{P,b}(x) = \frac{1}{\sqrt{N}}\imath^{xPx^\top + 2bx^\top} \tag{4}$$

Note that all arithmetic in the expressions $xPx^\top + 2bx^\top$ takes place in the ring of integers modulo 4. Given P, b the vector $xPx^\top + 2bx^\top$ is a codeword in

the Delsarte-Goethals code (defined over the ring of integers modulo 4). This representation of Kerdock and Delsarte-Goethals codes is a simplification of the representation given by Hammons et al [18] in that it avoids calculation in Galois rings. An alternative method of constructing the matrices P is to lift bilinear forms defined on ${\mathbb{F}_2}^m$ to the Teichmuller set of a Galois ring. We refer the reader to [19] and [20] for further details. For a fixed matrix P, the 2^m columns $\varphi_{P,b}$, $b \in \mathbb{F}_2^m$ form an orthonormal basis. The name Delsarte-Goethals frame (DG frame) reflects the fact that Φ is a union of orthonormal bases. Hence, it is a tight-frame with redundancy $\frac{\mathcal{C}}{N}$. Delsarte-Goethals frames are highly incoherent (see [17]):

Proposition 2. *Let m and r be non-negative integers where m is odd and $r \leq \frac{m-1}{2}$. Then the worst case coherence μ of the sensing matrix derived from the $DG(m,r)$ set satisfies $\mu \leq \frac{1}{N^{\frac{1}{2}-\frac{r}{m}}}$.*

Sensing matrices derived from Delsarte-Goethals sets are incoherent tight frames so the results of Section §2 can be brought to bear. The $N \times N^2$ sensing matrix derived from the Kerdock set is the union of N mutually unbiased bases and the worst case coherence matches the lower bound derived by Levenshtein [21] (see also Strohmer and Heath [8]).

3.2 Delsarte-Goethals Sieves

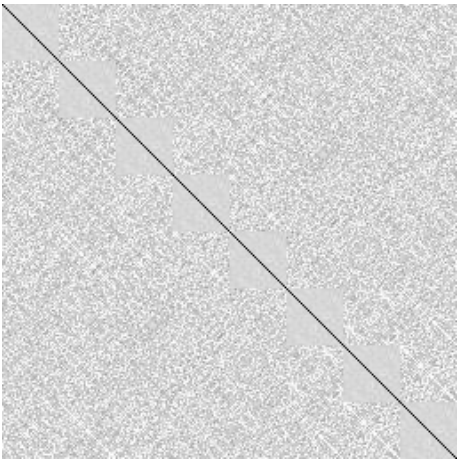
Chirp Detection [17] and Witness Averaging [22] are fast reconstruction algorithms that exploit the structure of Delsarte-Goethals frames. By sieving the testimony of witnesses [22] it is possible to detect the presence or absence of a signal at any given position in the data domain without explicitly reconstructing the entire signal.

There is however an aliasing problem with DG frames. When two signals modulate columns in the same orthonormal basis, spurious tones are generated by both the chirp detection and witness interrogation algorithms. This can be resolved by decimating the DG frame so that no two columns share the same binary symmetric matrix P. The simplest way to do this is to retain columns

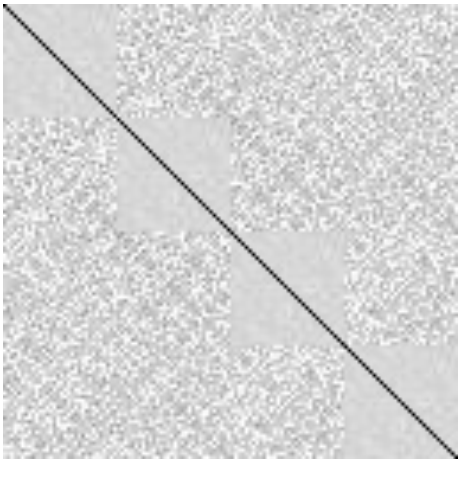
$$\varphi_P(x) = \frac{1}{\sqrt{N}} \imath^{xPx^\top}. \tag{5}$$

for which $b = 0$. The subsampled matrix has $N = 2^m$ rows and $\mathcal{C} = 2^{(r+1)m}$ columns. We call these subsampled matrices Delsarte-Goethals sieves ($DG(m,r)$ sieves) since it is still possible to sieve the testimony of witnesses. Note that each column of a DG sieve, is a column of the corresponding DG sieve, and the worst case coherence bound follows from Proposition 2. Figure 1 shows the distribution of the absolute value of pairwise inner products between columns of the $DG(5,1)$ sieve. All entries on the main diagonal are equal to 1, and around the the diagonal there are squares corresponding to translates of the Kerdock set K_m.

Table 1 shows that subsampling may increase the spectral norm. This will make it more difficult to reconstruct the signal either by chirp detection or by sieving the testimony of witnesses. We need to understand this increase in order to be able to apply the results of Section §2.



(a) Inner product between the first 512 columns of the $DG(5,1)$ matrix



(b) Inner product between the first 256 columns of the $DG(5,1)$ matrix

Fig. 1. The inner product between the columns of a $DG(5,1)$ matrix. The point at position (i,j) shows the inner product between the columns φ_i and φ_j. Lighter color shows higher inner product value.

Table 1. Spectral norms of $DG(m,1)$ frames and $DG(m,1)$ sieves as a function of m

$DG(m,1)$	$m=3$	$m=5$	$m=7$	$m=9$
Frame	2.8284	5.6569	11.3137	22.6274
Sieve	5.6568	11.1295	25.0386	55.0338

3.3 Spectral Norm of DG Matrices

Given a sensing matrix, the results presented in Section §2 show that if the the worst case coherence and spectral norm are sufficiently small then ℓ_0 minimization has a unique solution which coincides with the solution of a convex LASSO program. The worst case coherence μ of the initial $DG(m,r)$ frame satisfies $\mu \leq N^{\frac{r}{m}-\frac{1}{2}}$. To make sure that every row sum vanishes, we further exclude the $m+1$ rows, indexed by powers of 2, from the DG sieve. This exclusion changes the worst case coherence by at most $\frac{m+1}{N}$ $\left(\text{Now } \mu \leq N^{\frac{r}{m}-\frac{1}{2}} + \frac{m+1}{N}\right)$. The experimental results presented below suggest that the number of pairs of rows in a DG sieve that fail to be orthogonal is very small. Removing these rows results in an equiangular tight frame that is not a union of orthonormal bases.

Table 1 lists the spectral norm of $DG(m,r)$ frames and $DG(m,r)$ sieves for $m = 3, 5, 7$ and 9. The spectral norm of a sieve is almost twice that of the corresponding frame and we shall see that the reason is a small number of duplicate rows. Removing these rows results in an equiangular tight frame. We now describe how to find these duplicate rows. Let x, y be two distinct elements of the finite field ${\mathbb{F}_2}^m$, and let $\varphi(x)$, $\varphi(y)$ denote the two rows in a Delsarte-Goethals sieve Φ indexed by x and y. Setting $y = x + e$ we obtain

$$\varphi(x)^\dagger \varphi(y) = \frac{1}{N} \sum_{P \in DG(m,r)} \imath^{(x+e)P(x+e)^\top - xPx^\top} = \frac{1}{N} \sum_{P \in DG(m,r)} \imath^{2ePx^\top + ePe^\top} \quad (6)$$

$$= \frac{1}{N} \prod_{t=0}^{r} \left(\sum_{a \in \mathbb{F}_2^m} \imath^{2eP^t(a)x^\top + eP^t(a)e^\top} \right).$$

If rows $\varphi(x)$ and $\varphi(y)$ are not orthogonal then each term in the product is nonzero. When $t > 0$ we now show that the t^{th} term in the product is a sum of linear characters. Since the index of summation ranges over the group, the sum is either zero or the linear character is trivial (each term in the sum is equal to 1).

Lemma 2. *Let $t \geq 1$ and let x and $x + e$ be two distinct elements of $\mathbb{F}_2^m$. Then either $\sum_{a \in \mathbb{F}_2^m} \imath^{e\,P^t(a)(2x+e)^\top}$ is zero, or for every field element a: $(x+e)P^t(a)(x+e)^\top - xP^t(a)x^\top = 0 \pmod 4$.*

Proof. When $t > 0$ every matrix $P^t(a)$ has zero diagonal and the map $a \to (e+2x)P^t(a)e^\top$ is a linear map from the additive group $\mathbb{F}_2^m$ to $2\,\mathbb{Z}_4$. If this map is not identically zero then the character sum vanishes. □

The next proposition follows from non-degeneracy of the trace.

Proposition 3. *If $t > 0$ then for every field element f*

$$f\,P^t(a)f^\top = 2\mathrm{Tr}\left(f^{2^t+1}\,a\right) + 2z_a f^\top \;(\ mod\ 4\,), \tag{7}$$

where $z_a = \left[\mathrm{Tr}\left(\xi^{j(2^t+1)}\,a\right)\ \ j = 0, \cdots, m-1\right]$ *is a vector of length* m.

Proof. The $\mathbb{Z}_4$-linear quadratic form $xP^t(a)x^\top$ determines the bilinear form $2xP^t(a)y^\top$ and the $\mathbb{Z}_4$-linear quadratic form $2\mathrm{Tr}\left(ax^{(2^t+1)}\right)$ determines the bilinear form $2\mathrm{Tr}\left(\left(xy^{2t} + yx^{2t}\right)a\right)$. It follows from (3) that these two bilinear forms are the same.

Since the $\mathbb{Z}_4$-linear quadratic forms $fP^t(a)f^\top$ and $2\mathrm{Tr}\left(af^{2^t+1}\right)$ determine the same bilinear form they differ by a linear function $2z_a\,f^\top$. Since the quadratic form $fP^t(a)f^\top$ vanishes at all standard coordinate vectors we are able to determine the entries of the vector $2z_a$ that describes the linear function. □

Next we use non-degeneracy of the trace to find duplicate rows $\varphi(x)$ and $\varphi(x+e)$.

Lemma 3. *The existence of field elements x, e such that*

$$(x+e)P^t(a)(x+e)^\top - xP^t(a)x^\top = 0\,(mod\ 4) \quad \textit{for all } a \textit{ in } \mathbb{F}_2^m, \tag{8}$$

is equivalent to the existence of a solution $\frac{x}{e}$ to the equation

$$1 + \frac{x}{e} + \left(\frac{x}{e}\right)^{2^t} + \sum_{j=0}^{m-1} e_j \left(\frac{\xi^j}{e}\right)^{2^t+1} = 0. \tag{9}$$

Proof. Since the trace is a linear map we may replace (8) by the condition that for all a in $\mathbb{F}_2^m$

$$\mathrm{Tr}\left[a\left((x+e)^{2^t+1} + x^{2^t+1} + \sum_{j=0}^{m-1} e_j \xi^{j\left(2^t+1\right)}\right)\right] = 0.$$

Now the non-degeneracy of the trace implies that

$$(x+e)^{2^t+1} + x^{2^t+1} + \sum_{j=0}^{m-1} e_j \xi^{j\left(2^t+1\right)} = 0.$$

Expanding $(x+e)^{2^t+1}$, we obtain

$$e^{2^t+1} + x\,e^{2^t} + x^{2^t}\,e + \sum_{j=0}^{m-1} e_j \xi^{j\left(2^t+1\right)} = 0.$$

Since e is non-zero, dividing the equation by e^{2^t+1} completes the proof. □

The solutions to the equation $z + z^{2^t} = 0$ form a subfield of $\mathbb{F}_2^m$ and the number of solutions is $\gcd(2^t - 1, 2^m - 1)$ which is just $2^{\gcd(t,m)} - 1$. Note that when m is odd and $t = 1$ or $t = 2$, there are exactly two solutions ($z = 0$ and $z = 1$). We now list the conditions satisfied by x and e if the row $\varphi(x)$ is not orthogonal to the row $\varphi(x + e)$.

Theorem 6. *Let x and $x + e$ be two distinct elements of the finite field $\mathbb{F}_2^m$. Then $\varphi(x)^\dagger \varphi(x + e) \neq 0$ if and only if the following conditions simultaneously hold:*

- *(C1) For every $t \geq 1$: $\frac{x}{e} + \left(\frac{x}{e}\right)^{2^t} = 1 + \sum_{j=0}^{m-1} e_j \left(\frac{\xi^j}{e}\right)^{2^t+1}$.*
- *(C2) $\sum_{a \in \mathbb{F}_2^m} \imath^{e\, P^0(a)(2x+e)^\top} \neq 0$.*

Theorem 6 provides an efficient way for identifying the non-orthogonal rows of the sieve matrices without requiring to calculate the gram matrices $\Phi^\dagger \Phi$ explicitly. For every element e, we first find the solution for the case $t = 1$. If such a solution exists then we just need to *check* that condition (C1) is valid for other values of t. If all conditions passed then we just verify condition (C2). This method significantly reduces the computational cost of eliminating the non-orthogonal rows.

The next formula is for $t = 1$

$$\frac{x}{e} + \left(\frac{x}{e}\right)^2 = \lambda \quad \text{where } \lambda = 1 + \frac{\sum_{j=0}^{m-1} e_j \xi^{3j}}{e^3}.$$

This is a quadratic equation with roots $\frac{x}{e}$ and $\frac{x}{e} + 1$ where $\frac{x}{e} \doteq \sum_{\substack{\ell:\, odd \\ 1 \leq \ell \leq m-2}} \lambda^{2^\ell}$. On the other hand

$$\lambda + \lambda^2 = \frac{x}{e} + \left(\frac{x}{e}\right)^4 = \alpha \quad \text{where } \alpha = 1 + \frac{\sum_{j=0}^{m-1} e_j \xi^{5j}}{e^5}.$$

Thus we can also retrieve the explicit solution $\lambda = \sum_{\substack{\ell:\, odd \\ 1 \leq \ell \leq m-2}} \alpha^{2^\ell}$. In other words, the following equivalence between the two field elements (which are both functions of e) must be satisfied:

$$\sum_{\substack{\ell:\, odd \\ 1 \leq \ell \leq m-2}} \left(1 + \frac{\sum_{j=0}^{m-1} e_j \xi^{5j}}{e^5}\right)^{2^\ell} = 1 + \frac{\sum_{j=0}^{m-1} e_j \xi^{3j}}{e^3}. \tag{10}$$

Remark 1. Solutions to condition (C1) correspond to codewords of weight 2 in the binary code that is dual to the code determined by matrices in $DG(m, r)$ with zero diagonal. The number of solutions can be calculated using the MacWilliams Identities and we provide details in Appendix §A. The difficulty in proving the result for arbitrary m is that the number of codewords of weight 2^{m-1} is not determined and so the number of codewords of weight 2 in the dual code cannot be calculated by simply applying the MacWilliams identities. If we try to finesse this by choosing columns with a particular weight then we lose linearity and lose control of the distance distribution.

Table 2 records the number of duplicate measurements that need to be deleted in order to transform a $DG(m,1)$ sieve into a tight frame. We calculated the number of duplicate rows for $DG(m,2)$, where $m \leq 15$, and found that there were no solutions to (C1) that also satisfied (C2); that is all $DG(m,2)$ sieves with $m \leq 15$ are tight frames. Hence

Conjecture: Every $DG(m,r)$ sieve with $r \geq 2$ is a tight-frame.

Figure 2 displays for $m = 7$ and 9 the average condition number of a random $N \times k$ submatrix of the $DG(m,1)$ sieve and the $DG(m,0)$ frame. The spectral norm of the hollow gram matrix $\|\Phi^{\dagger}\Phi - \mathrm{I}_N\|_2$ was calculated for 2000 randomly chosen submatrices Φ_k and the average was recorded. The comparison with Gaussian sensing matrices was made by drawing 10 iid Gaussian matrices, calculating for each matrix the average spectral norm over randomly chosen submatrices, and then recording the median value.

Table 2. Number of row deletions required to transform a $DG(m,1)$ sieve into a tight frame

$DG(m,1)$	$m=5$	$m=7$	$m=9$	$m=11$	$m=13$	$m=15$
# of non-orthogonal rows	11	25	45	83	203	381
% of non-orthogonal rows	0.3438	0.1953	0.0879	0.0405	0.0248	0.0116

Remark 2. Here we compare the empirical results of Figure 2 with the theoretical results of Theorem 2. First we considered the $DG(7,0)$ frame, with $\mathcal{C} = 2^{14}$ and $N = 2^7$. The worst case coherence of Φ is $\mu = 2^{-\frac{7}{2}}$, and the square of the spectral norm of Φ is 2^7. So the constant c in Theorem 3 needs to be at least $\mu \log \mathcal{C} = \frac{14 \log 2}{8\sqrt{2}} \approx 0.85$. Hence, as long as k is at most $\frac{0.85 \times 128}{14 \log 2} \approx 11$, Theorem 2 predicts probability of non-uniqueness on the order of 2^{-14}. Experimental results presented in Figure 2a are more positive; all 2000 trials resulted in sub-dictionaries with full rank, even for k as large as 20.

Next we considered the $DG(7,1)$ sieve with $\mathcal{C} = 2^{14}$ and $N = 103$[1]. The worst case coherence of Φ is $\mu \approx 2^{-\frac{5}{2}}$, and the square of the spectral norm of Φ is $\|\Phi\|^2 \approx \frac{16384}{103} = 159.6$. As a result, the constant c needs to be at least $\frac{14 \log 2}{4\sqrt{2}} \approx 1.70$. Therefore, as long as k is less than $\frac{1.70 \times 103}{14 \log 2} \approx 10$ Theorem 2 predicts probability of non-uniqueness on the order of 2^{-14}. Again, we see that the theoretical bound is not tight, and for k as large as 20 all trials provide uniqueness of sparse representation.

Remark 3. The bounds of Proposition 1 only apply to the condition number of random submatrices and do not provide additional information about the distribution of eigenvalues. However Gurevich and Hadani [23] have analyzed

[1] The 25 duplicate rows were removed from the matrix.

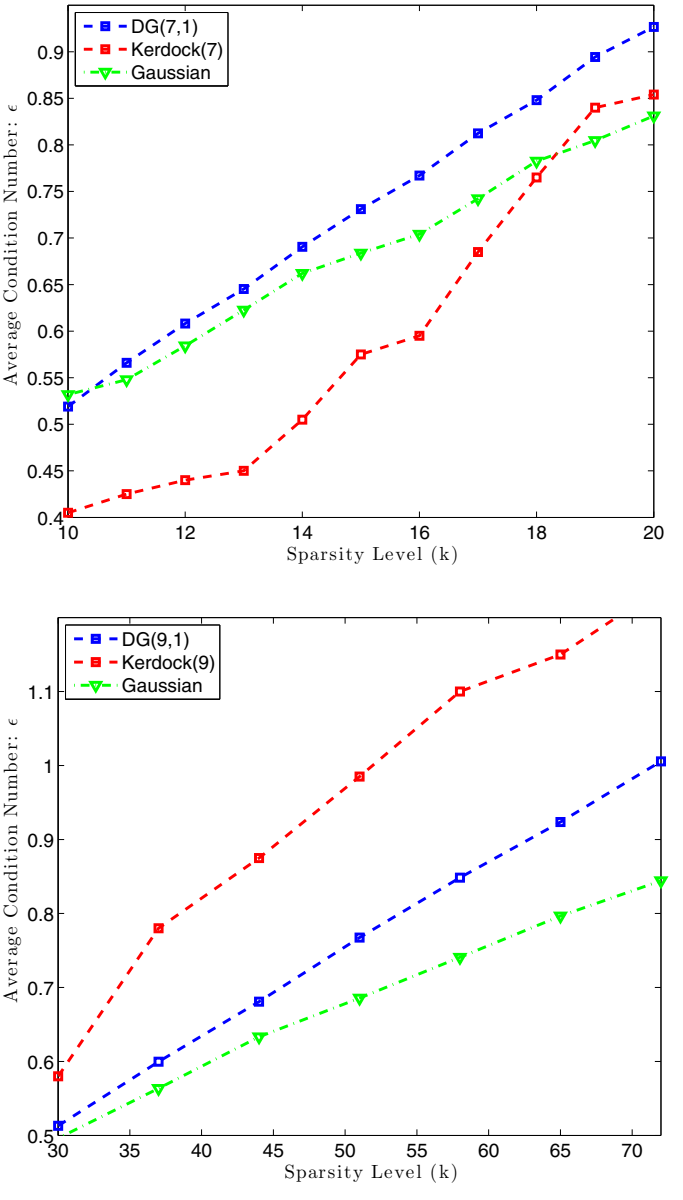


Fig. 2. Average spectral norm of $\Phi_k^{\dagger}\Phi_k - \mathrm{I}_{k\times k}$, where Φ_k is a random sub dictionary of Φ. Here the comparison is between Gaussian, $DG(m,1)$ sieve, and $DG(m,0)$ base matrices. Each experiment is repeated 2000 times.

the spectrum of certain incoherent dictionaries that are unions of disjoint orthonormal bases. They have shown that the eigenvalues of the Gram matrix of a random subdictionary are asymptotically distributed around 1 according to the

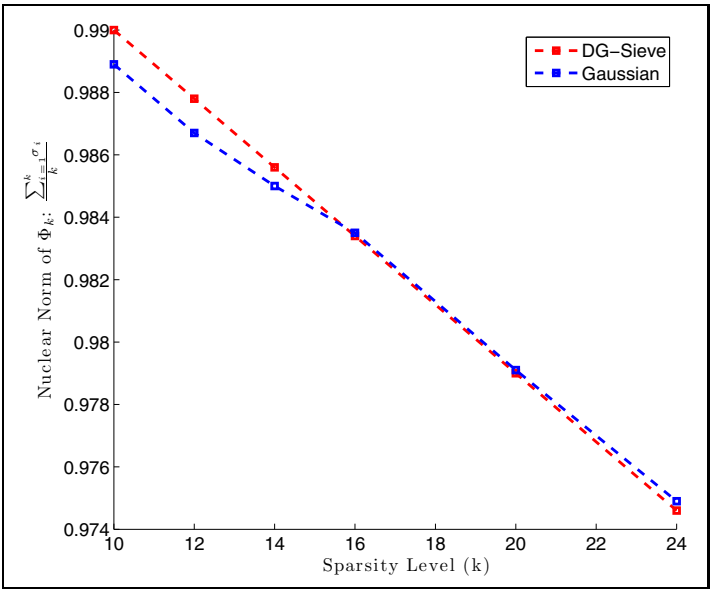


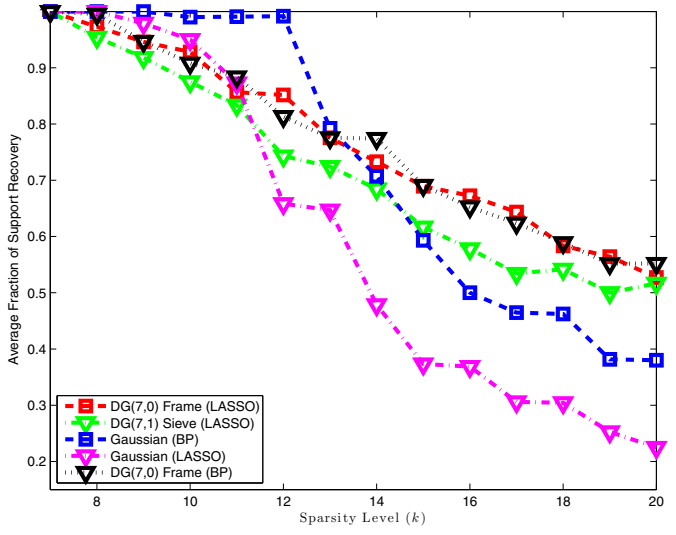
Fig. 3. Average nuclear norm $\left(\frac{1}{k}\sum_{i=1}^{k}\sigma_i\right)$ of random sub-dictionaries of of $DG(7,1)$ and Gaussian matrices of the same size as a function of the sparsity level k

Wigner semicircle law. Our experimental results suggest that this property is shared by DG sieves which are not unions of orthonormal bases. Figure 3 shows that the distribution of the singular values of a random submatrix of a DG sieve is symmetric around 1, and very similar to the distribution for a Gaussian matrix of the same size.

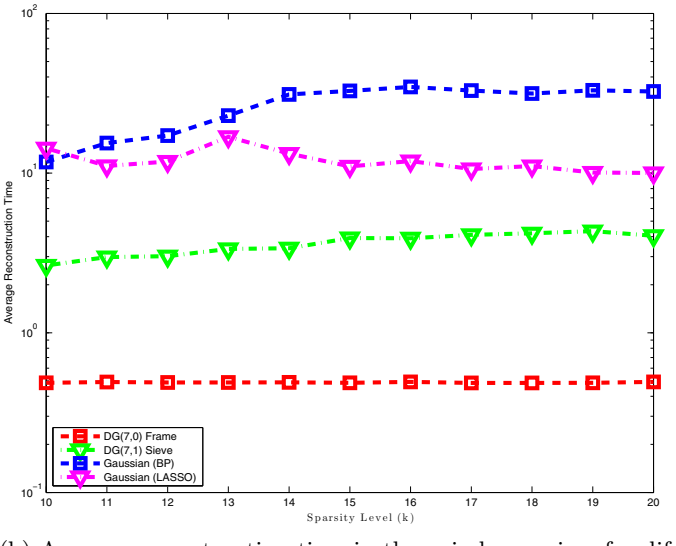
4 Numerical Experiments

In this Section we present numerical experiments to evaluate the performance of the DG frames and sieves. The performance of DG frames and sieves is compared with that of random Gaussian sensing matrices of the same size. The SpaRSA algorithm [15] with ℓ_1 regularization parameter $\lambda = 10^{-9}$ is used for signal reconstruction in the noiseless case, and the parameter is adjusted according to Theorem 3 in the noisy case. The reason for using SpaRSA is that is designed to solve complex valued LASSO programs.

Remark 4. Given a random sensing matrix satisfying RIP, it is known that Basis Pursuit leads to more accurate reconstruction than the LASSO [1]. It is for this reason that we also compare results for LASSO applied to DG matrices with results for Basis Pursuit applied to Gaussian matrices. The ℓ_1-magic package [24] is used to solve the Basis Pursuit optimization program. The results for Gaussian matrices shown in Figure 4 are consistent with the observation made in [25] that

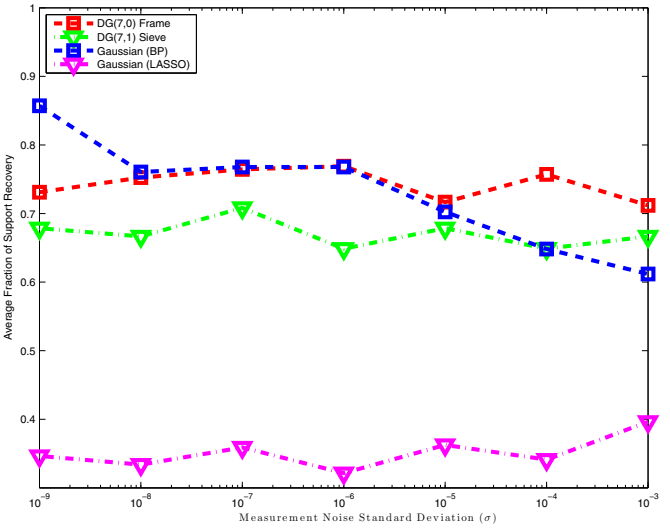


(a) Average fraction of the support that is reconstructed successfully as a function of the sparsity level k

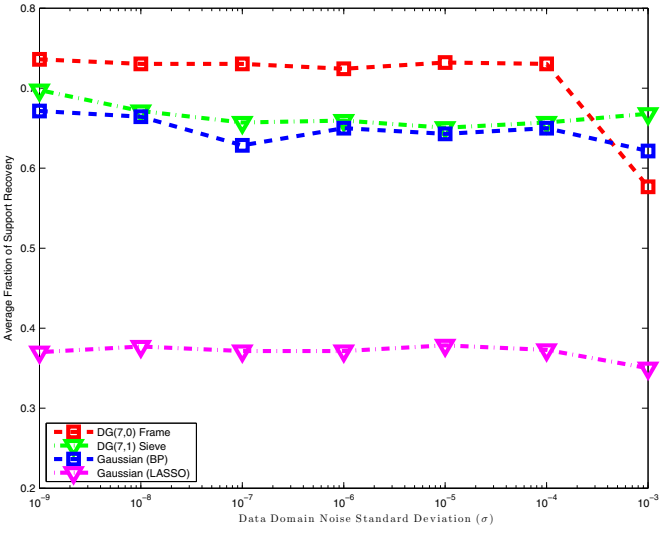


(b) Average reconstruction time in the noiseless regime for different sensing matrices.

Fig. 4. Comparison between $DG(7,0)$ frame, $DG(7,1)$ sieve, and Gaussian matrices of the same size in the noiseless regime. The regularization parameter for LASSO is set to 10^{-9}.



(a) The impact of the noise in the measurement domain on the accuracy of the sparse approximation for different sensing matrices.



(b) The impact of the noise in the data domain on the accuracy of the sparse approximation for different sensing matrices.

Fig. 5. Average fraction of the support that is reconstructed successfully as a function of the noise level in the measurement domain (left), and in the data domain (right). Here the sparsity level is 14. The regularization parameter for LASSO is determined as a function of the noise variance according to Theorem 3.

when the signal is not very sparse, interior point methods (ℓ_1 - magic) are less sensitive than gradient descent methods (SpaRSA)

For Gaussian matrices, we sampled 10 iid random matrices independently to eliminate the exponentially small chance of getting a sample Φ with $\mu = \omega(N)$ or $\|\Phi\|^2 = \omega\left(\frac{\mathcal{C}}{N}\right)$, and the median of the results among all 10 random matrices is reported. The use of 10 random trials to eliminate pathological sensing matrices is standard practice (see [11] for example).

The experiments relate accuracy of sparse recovery to the sparsity level and the Signal to Noise Ratio (SNR). Accuracy is measured in terms of the statistical $0-1$ loss metric which captures the fraction of signal support that is successfully recovered. The reconstruction algorithm outputs a k-sparse approximation $\hat{\alpha}$ to the k-sparse signal α, and the statistical $0-1$ loss is the fraction of the support of α that is not recovered in $\hat{\alpha}$. Each experiment was repeated 2000 times and Figure 4 records the average loss.

Figure 4 plots statistical $0-1$ loss and complexity (average reconstruction time) as a function of the sparsity level k. We select k-sparse signals with uniformly random support, with random signs, and with the amplitude of non-zero entries set equal to 1. Three different sensing matrices are compared; a Gaussian matrix, a $DG(7,0)$ frame and a $DG(7,1)$ sieve. After compressive sampling the signal support is recovered using the SpaRSA algorithm with $\lambda = 10^{-9}$. For random matrices the signal support is also recovered by ℓ_1-minimization.

Figure 5a plots statistical $0-1$ loss as a function of noise in the measurement domain and Figure 5b does the same for noise in the data domain. In the measurement noise study, a $\mathcal{N}(0,\sigma^2)$ iid measurement noise vector is added to the sensed vector to obtain the N dimensional vector f. The original k-sparse signal α is then approximated by solving the LASSO program with $\lambda = 2\sqrt{2\log\mathcal{C}}\sigma^2$, and basis pursuit with $\epsilon = 2N\sigma^2$. Following Lemma 1, we use a similar method to study noise in the data domain. Figure 5 shows that DG frames and sieves outperform random Gaussian matrices in terms of noisy signal recovery using the LASSO.

5 Conclusion

We have constructed two families of deterministic sensing matrices, $DG(m,r)$ frames and $DG(m,r)$ sieves, by exponentiating codewords from $\mathbb{Z}_4$ - linear Delsarte-Goethals codes. We have verified that the worst-case coherence and the spectral norm of these sensing matrices satisfy the conditions necessary for uniqueness of sparse representation and fidelity of ℓ_1 reconstruction via the LASSO algorithm. We have presented numerical results that confirm performance predicted by the theory. These results show that DG frames and sieves outperform random Gaussian matrices in terms of noiseless and noisy signal recovery using the LASSO. Our focus here is on ℓ_1 reconstruction using the LASSO algorithm but we note that the particular structure of the DG matrices leads to faster algorithms and to additional features such as local decoding and stronger guarantees on resilience to noise in the data domain.

Acknowledgements

The authors would like to thank Marco Duarte and Waheed Bajwa for sharing many valuable insights, and Waheed in particular for his help with the SpaRSA package. The work of R. Calderbank and S. Jafarpour is supported in part by NSF under grant DMS 0701226, by ONR under grant N00173-06-1-G006, and by AFOSR under grant FA9550-05-1-0443.

References

1. Candès, E., Romberg, J., Tao, T.: Stable signal recovery from incomplete and inaccurate measurements. Communications on Pure and Applied Mathematics 59(8), 1207–1223 (2006)
2. Donoho, D.: Compressed Sensing. IEEE Transactions on Information Theory 52(4), 1289–1306 (2006)
3. Candès, E., Tao, T.: Near optimal signal recovery from random projections: Universal encoding strategies. IEEE Transactions on Information Theory 52(12), 5406–5425 (2006)
4. Candès, E., Romberg, J., Tao, T.: Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. IEEE Transactions on Information Theory 52(2), 489–509 (2006)
5. Cohen, A., Dahmen, W., DeVore, R.: Compressed sensing and best k-term approximation. Journal of American Mathematical Society 22, 211–231 (2009)
6. Baraniuk, R., Davenport, M., DeVore, R., Wakin, M.: A simple proof of the restricted isometry property for random matrices. Constructive Approximation 28(3), 253–263 (2008)
7. DeVore, R.A.: Deterministic constructions of compressed sensing matrices. Journal of Complexity 23(4-6), 918–925 (2007)
8. Strohmer, T., Heath, R.W.: Grassmannian frames with applications to coding and communication. Applied and Computational Harmonic Analysis 14(3), 257s–275s (2003)
9. Bajwa, W., Haupt, J., Raz, G., Wright, S., Nowak, R.: Toeplitz-structured compressed sensing matrices. In: Statistical Signal Processing. IEEE/SP 14th Workshop on Publication, pp. 294–298 (August 2007)
10. Jafarpour, S., Xu, W., Hassibi, B., Calderbank, R.: Efficient compressed Sensing using Optimized Expander Graphs. IEEE Transactions on Information Theory 55(9), 4299–4308 (2009)
11. Berinde, R., Gilbert, A., Indyk, P., Karloff, H., Strauss, M.: Combining geometry and combinatorics: a unified approach to sparse signal recovery. In: 46th Annual Allerton Conference on Communication, Control, and Computing, pp. 798–805 (September 2008)
12. Chandar, V.: A negative result concerning explicit matrices with the restricted isometry property (2008) (preprint)
13. Tropp, J.: The Sparsity Gap: Uncertainty Principles Proportional to Dimension. In: Proc. 44th Ann. IEEE Conf. Information Sciences and Systems, CISS (to appear 2010)
14. Candès, E., Plan, Y.: Near-ideal model selection by ℓ_1 minimization. Annals of Statistics 37, 2145–2177 (2009)

15. Wright, S., Nowak, R., Figueiredo, M.: Sparse reconstruction by separable approximation. IEEE Transactions on Signal Processing 57(7), 2479–2493 (2009)
16. Calderbank, R., Howard, S., Jafarpour, S.: Sparse reconstruction via the Reed-Muller sieve. Accepted to the International Symposium on Information Theory, ISIT (2010)
17. Calderbank, R., Howard, S., Jafarpour, S.: Construction of a large class of Matrices satisfying a Statistical Isometry Propery. IEEE Journal of Selected Topics in Signal Processing, Special Issues on Compressive Sensing 4(2), 358–374 (2010)
18. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Sole, P.: The $\mathbb{Z}_4$-linearity of Kerdock Codes, Preparata, Goethals, and related codes. IEEE Transactions on Information Theory 40(2), 301–319 (1994)
19. Calderbank, A.R.: Reed-Muller Codes and Symplectic Geometry. In: Recent trends in Coding Theory and its Applications. AMS / IP Studies in Advanced Mathematics. American Mathematical Society, Providence (2006)
20. Calderbank, A.R., Cameron, P.J., Kantor, W.M., Seidel, J.J.: $\mathbb{Z}_4$–Kerdock Codes, orthogonal spreads and extremal euclidean line sets. Proceedings of London Math. Society 75, 436–480 (1997)
21. Levenshtein, V.I.: Bounds on the maximum cardinality of a code with bounded modulus of the inner product. Soviet Math. Dokl. 25, 526–531 (1982)
22. Calderbank, R., Howard, S., Jafarpour, S.: A sub-linear algorithm for Sparse Reconstruction with $\ell 2/\ell 2$ Recovery Guarantees (2009) (preprint)
23. Gurevich, S., Hadani, R.: The statistical restricted isometry property and the Wigner semicircle distribution of incoherent dictionaries. Submitted to the Annals of Applied Probability (2009)
24. Candès, E., Romberg, J.: ℓ_1-magic: Recovery of sparse signals via convex programming (2005), http://www.acm.caltech.edu/l1magic
25. Tropp, J., Wright, S.: Computational methods for sparse solution of linear inverse problems. Technical Report No. 2009-01, California Institute of Technology (2009)
26. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)

A The Number of Solutions of Condition (C1)

Let $DG_0(m,r)$ denote the set of all zero-diagonal matrices in $DG(m,r)$:

$$DG_0(m,r) = \left\{ \sum_{t=1}^{r} P^t(a_t) \,|a_t \in \mathbb{F}_2^m \, t = 1, \cdots, r \right\}.$$

For every matrix P in $DG_0(m,r)$, the vector $xPx^\top$ is a codeword of the linear binary code $\overline{DG}_0(m,r)$ which is a sub-code of the Delsarte-Goethals code. Note that $\overline{DG}_0(m,r)$ has 2^{rm} codewords of length 2^m. The following lemma shows how the number of solutions to (C1) is related to the properties of this binary code.

Lemma 4. *Let $\{W_0, \cdots, W_N\}$ denote the weight distribution of $\overline{DG}_0(m,r)$. Then the number of pairs $(x, x+e)$ satisfying (C1) is equal to*

$$\frac{1}{2^{rm}} \sum_{i=0}^{N} W_i \mathcal{K}_2(i), \tag{11}$$

where $\mathcal{K}_\ell(z)$ is the ℓ^{th} Krawtchouk polynomial, defined as

$$\mathcal{K}_\ell(z) = \sum_{r=0}^{\ell} \binom{z}{r}\binom{N-z}{\ell-r}(-1)^r. \tag{12}$$

Proof. Lemma 3 implies that the number pairs $(x, x+e)$ satisfying Condition (C1) is equal to the number of duplicate rows in $\overline{DG}_0(m,r)$. The condition that the rows x and $x+e$ are identical is equivalent to the condition that the vector with entry 1 in positions x and $x+e$, and zero elsewhere belongs to the dual code. The lemma now follows from the MacWilliams Identities [26] that relate relate the number of codewords of weight 2 in the dual of $\overline{DG}_0(m,r)$ to the weight distribution of $\overline{DG}_0(m,r)$.

Next we show that for the case $r = 1$, the number of solutions to (C1) only depends on the number of codewords with weight 2^{m-1} in $\overline{DG}_0(m,1)$:

Theorem 7. *Let m be an odd number and let r equal 1. Then the number of solutions to (C1) is $2^m - 1 - s$ where s is the number of codewords with weight 2^{m-1} in $\overline{DG}_0(m,1)$.*

Proof. We start by calculating the rank of matrices in $DG_0(m,1)$: Let a be a fixed element of $\mathbb{F}_2^m$. A field element x is in the null space of P_a if and only if for every field element y, $xP_ay^\top = 0$. Using Equation 3, this condition can be translated to the condition

$$\mathrm{Tr}\left((xy^2 + x^2y)a\right) = 0 \text{ for all } y.$$

Since $\mathrm{Tr}(x) = \mathrm{Tr}(x^2)$ the condition further reduces to

$$\mathrm{Tr}\left((xa + x^4a^2)y^2\right) = 0 \text{ for all } y.$$

Non-degeneracy of the trace implies that $x^4 + \frac{x}{a} = 0$, which, since m is odd, has the unique solution $x^3 = \frac{1}{a}$.

Now let $S = \sum_{x\in\mathbb{F}_2^m} \imath^{xP_ax^\top}$. Since $xP_ax^\top$ is a binary codeword, we have $S^2 = (N - 2w_a)^2$, where w_a is the weight of the codeword determined by P_a. It has been proved in [17] that $S^2 = 2^m \sum_{e:eP_a=0} \imath^{eP_ae^\top}$. We provide the proof here for completeness:

We have

$$S^2 = \sum_{x,y} \imath^{xP_ax^\top + yP_ay^\top} = \sum_{x,y} \imath^{(x+y)P_a(x+y)^\top + 2xP_ay^\top}$$

Changing variables to $z = x \oplus y$ and y gives

$$S^2 = \sum_z \imath^{zP_az^\top} \sum_y (-1)^{zP_ay^\top} = 2^m \sum_{z:zP_a=0} \imath^{zP_az^\top}.$$

The null space of P_a has only two elements 0 and $a^{-\frac{1}{3}}$. As a result

$$S^2 = 2^m \left(1 + \imath^{a^{-\frac{1}{3}}P_a a^{\frac{1}{3}\top}}\right).$$

There are two cases; S^2 is either 0 or 2^{m+1}.

Case 1: S is zero. This case provides one possible weight value: $w_a = 2^{m-1}$.

Case 2: $|S|^2 = 2^{m+1}$. Therefore $2^m - 2w_a = \pm 2^{\frac{m+1}{2}}$. This case provides two distinct weight values: $w_a = 2^{m-1} \pm 2^{\frac{m-1}{2}}$. Hence $DG_0(m,1)$ has exactly four distinct weights $\langle 0, 2^{m-1} - 2^{\frac{m-1}{2}}, 2^{m-1}, 2^{m-1} + 2^{\frac{m-1}{2}} \rangle$. Let $\langle 1, t, s, t' \rangle$ denote the corresponding weight distribution. We can use the MacWilliams identities to find the values of t and t' as a function of s. First, note that the dual code has exactly one codeword of weight 0. Using MacWilliams identities with Krawtchouk polynomial $\mathcal{K}_0(z) = 1$, gives the equation $1+t+s+t' = \mathcal{C}$. Second, since all matrices in $DG_0(m,r)$ are zero-diagonal, for every field element a and for every index j in $\{0, \cdots, m\}$, $\xi^j P_a {\xi^j}^\top = 0$, the dual code has exactly $m+1$ codewords of weight 1. Again, MacWilliams identities, with Krawtchouk polynomial $\mathcal{K}_1(z) = N - 2z$ gives the equation $(m+1)N = N + \sqrt{2N}(t'-t)$. This equation can be simplified to $t - t' = m\, 2^{\frac{m-1}{2}}$. Solving t and t' with respect to s gives $t = \frac{2^m - 1 - s + m2^{\frac{m-1}{2}}}{2}$ and $t' = \frac{2^m - 1 - s - m2^{\frac{m-1}{2}}}{2}$. The theorem then follows from substituting the values t, s, t' into Equation (12), and simplifying the expression using the Krawtchouk polynomial $\mathcal{K}_2(z) = \frac{(N-2z)^2 - N}{2}$.

Author Index