Cryptography and Communications (2023) 15:257–308
https://doi.org/10.1007/s12095-022-00585-4

Status of three classes of sequences

G. Gong[1] · **Z.L. Wang**[2]

Received: 25 July 2021 / Accepted: 26 April 2022 / Published online: 2 August 2022

Abstract
Pseudorandom sequences, sometimes shortened as sequences, have played a key role in the applications of digital communications, cryptography and computer science. This research field is an example of scientific research directly born from the real world applications. Specifically, the research on sequences stems from the application of the sequences generated by maximal length linear feedback shift registers to detect returning signals from Explorer 1, the satellite launched on January 31, 1958 by US, shortly after Sputnik, launched by Soviet Union on October 4, 1957 which is the first satellite in the human being civilization. With more than seven decades of the developments of theory and practice of sequences, this field has evolved to acquire a wide range of the tools and methodologies from extremely deep mathematic fields (comparing with other engineering subjects), such as algebraic geometry, number theory, combinatorics, representation theory, harmonic analysis, to just mention a few. In this survey, we present the current status of the research in sequence design along three different directions, i.e., the sequences with 2-level autocorrelation, the sequence sets with low ambiguity, and Golay complementary sequence sets and complete complementary codes.

Keywords Pseudorandom sequences · 2-level autocorrelation · Ambiguity function · Golay complementary sequence sets and complete complementary codes

Mathematics Subject Classification (2010) 94A55 · 05B10 · 05B20 · 11L05 · 11L07

1 Introduction

Starting with the launch of Explorer 1, on January 31, 1958 of the first application of pseudorandom sequences in space communications pioneered by Solomon Golomb when he worked in the Communication Research Group at the Jet Propulsion

This article belongs to the Topical Collection: *Surveys (invitation only)*

✉ Z.L. Wang
zlwang@xidian.edu.cn

G. Gong
ggong@uwaterloo.ca

[1] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo Ontario N2L 3G1, Canada

[2] State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China

Laboratory, sequence design has played an important role from radio communication to our current 5G cellular wireless communications for anti-noise and reducing multi-path and multiple access interference. The initial study of sequences has been presented in Golomb's book: Shift Register Sequences [21], which leads the research in sequence design more than seven decades [27]. With respect to digital communications, it has found many applications described in the following incomplete list:

- Radar distance ranging, signal processing, and multi-sensory sensing for higher resolution.
- Interference rejection in multi-path interference, channel estimation.
- Energy density reduction, anti-jaming, low probability interception, and multiple access.
- Reduction of peak-to-average power ratio (PAPR) or peak-to-mean envelope power ratio (PMEPR) for orthogonal frequency division multiplexing (OFDM) systems.
- It also can offer a certain degree of *privacy*.

Pseudorandom sequences also have many applications in cryptography, computer science, game theory, DNA processing, etc., to just list a few. In this survey, we focus on sequence design for wireless communications and some relations to cryptography. The current research on sequence design can be classified into three different categories: a) sequences with low periodic correlation; b) complementary sequence sets (CSS) and complete complementary codes (CCC), measured by aperiodic correlation; and c) sequence sets with low ambiguity functions for both periodic and aperiodic sequences.

It is almost impossible without a very voluminous space to survey recent developments of sequences. For sequences with low correlation, we have the following comments.

(a) There is a large volume of research on the constructions of sequence sets with low correlation and large sizes for code-division multiple access (CDMA) applications. A number of survey papers, authored by renowned researchers have been published in the literature. For example, an excellent survey paper by Kumar and Helleseth [32], entitled as Sequences with Low Correlation, appeared in Handbook of Coding Theory (1998), has covered all the developments from the constructions to the bounds for optimality. A recent survey on sequences with optimal autocorrelation and the constructions for de Bruijn sequences is authored by Helleseth and Li [33], an earlier survey on binary and quaternary sequences by Lück, Schotten and Hadinejad-Mahram [44], and a survey on sequences with good aperiodic correlation by Katz [36], to just list a few. The reader is referring to the references therein for the original contributions.

(b) Given a channel condition, the signal sets with low correlation or zero correlation confined in a certain interval instead of the entire period [62] are referred to as low or zero correlation zone sequences, which have stimulated large publications in the literature in theory, for example [25, 64, 65] and the references therein. However, it is problematic to be implemented in practical systems due to the heavy hardware cost for real-time channel estimation.

In this survey, we attempt to present some work and comments on the sequences with 2-level autocorrelation, sequence sets with low ambiguity, and CSSs and CCCs.

1.1 Sequences with 2-level autocorrelation and their applications

As we have mentioned above, the research on sequences with good correlation started with linear feedback shift register (LFSR) sequences [21], and first used in Explorer 1 to detect transmitted signals from the Explorer 1 back to the earth. This event was explained by Golomb in his paper [22] wonderfully. Successfully, Golomb applied it to estimate the distance from the earth to Venus [45]. Those two applications utilize the autocorrelation property of m-sequences, i.e., all the values of the out-of-phase autocorrelation are equal to -1 (the so-called an (ideal) 2-level autocorrelation function). A sequence with 2-level autocorrelation resembles a white Gaussian noise random process, so it has the best capability to distinguish itself from interference caused by multi-path fading. All the known constructions on binary sequences with 2-level autocorrelation are collectively surveyed in Golomb and Gong's book [19], published in 2005. Unfortunately, until now, there are no new constructions (even conjectures) on 2-level autocorrelation sequences, especially binary sequences. Nevertheless, there is a dramatical progress on proving conjectured ternary 2-level autocorrelation sequences [3, 35].

Impulse response behaviour and cryptographic connections The investigation for the applications of 2-level autocorrelation sequences (behaving approximately an impulse response) for wireless transmission including radar distance range and for cryptography such as generating key stream for stream cipher encryption is always a twin-brain body, which is inseparable since the creation of this area by Golomb. Astonishingly, when he proposed to use maximal length LFSR sequences (i.e., m sequences) in 1957 for the application of the space navigation [21], Golomb [20] also published a paper, entitled as "On the Classification of Boolean Functions" in 1959, in which he has essentially proposed the concepts of correlation immunity and resiliency of Boolean functions in the form of the invariants of Boolean functions, and also studied the invariants using the Rademacher-Walsh expansion (which is equivalent to Hadamard transform or Walsh-Hadamard transform). Those concepts are currently in the core of modern cryptography and cryptanalysis.

One version of the Globe Position System (GPS) employs the LFSRs of degree 10 and degree 13 as general navigation codes (i.e., m-sequences with periods $2^{10}-1=1023$ and $2^{13}-1=8191$ respectively). However, those sequences are too short, attackers can spoof the signals sending from a satellite to a device which can compute its location. The spoofed signal can make a fault location for the victim device. Those attacks have been reported in some diplomatic cases. We understand that there are many other 2-level autocorrelation sequences in those lengths which can provide a stronger capability to resist the spoof attack. However, the problem is how to balance the hardware cost, performance and security in those systems. Unfortunately, in many real world applications, it will be in favor of reducing the cost first.

Indistinguishability from out-of-phase sequences The Welch-Gong (WG) stream cipher was submitted to the eSTREAM Project of the eCRYPT network in 2004 [46]. This cipher is based on the WG sequences with 2-level autocorrelation (see [19]) which remains as secure up to the date. A new authenticated encryption (AE) algorithm, called WAGE (i.e., WG in AE mode), was submitted to the NIST Lightweight Cryptography Standardization Competition in 2019 [1, 2] and was advanced to the round 2 candidate. It differs from the other ciphers due to its capability to switch to the original WG stream cipher where the key

stream has 2-level autocorrelation. This property provides the indistinguishability for any shifts of the key stream. (For the history of WG sequences, the reader is referring to [19] and the references therein.)

Actually, in cryptographic applications, key-stream sequences with low aperiodic autocorrelation are requested, since in general, attacker cannot get the entire space of ciphertexts by conducting chosen plaintext attacks. Nevertheless, it constitutes a challenge to construct binary sequences with low aperiodic autocorrelation. Thus, a thumb rule is that the key stream sequences should have good periodic correlation, because Boehmer [5] observed that having low periodic correlation at all shifts is a necessary but not sufficient condition for having low aperiodic correlation at all shifts.

Paths leading to the proofs of the conjectured ternary sequences One of the most exciting results on 2-level autocorrelation sequences in recent 20 years is the construction of the families of binary 2-level autocorrelation sequences, discovered by Dillion and Dobbertin, published in 2004 [13], which includes the conjectured 3-term, 5-term and WG sequences as special cases of their construction. Their construction is fairly simple which can be easily explained as follows. Let $d = 2^{2k} - 2^k + 1$, which is the so-called Kasami exponent in the power function x^d for $x \in \mathbb{F}_{2^n}$ where $\gcd(k, n) = 1$ and $\mathbb{F}_{2^n}$ is a finite field with 2^n elements. Let a difference set be

$$\Delta = \left\{(x+1)^d + x^d + 1 | x \in \mathbb{F}_{2^n}\right\}.$$

Then a binary sequence $\mathbf{f} = \{f(t)\}$ is defined as: $f(t) = 0$ if $\alpha^t \in \Delta$, $f(t) = 1$ otherwise where α is a primitive element in $\mathbb{F}_{2^n}$, which has 2-level autocorrelation. However, the proof is deeply involved in very complicated manipulations of the difference set Δ. Also there are many remarkably hidden treasures in their paper, such as a set of new almost perfect nonlinear (APN) functions, new permutations of $\mathbb{F}_{2^n}$, and Hadamard equivalent classes. Recently, Carlet [9] has revisited this construction and attempted to establish the result of his new notion, called *component Walsh uniformity*, over the functions given by the difference set Δ.

The method used by Dillion and Dobbertin is the Hadamard equivalence relation. This has been further explored by Golomb and Gong, which showed that all the known binary 2-level autocorrelation sequences can be obtained by repeating applying the decimation and Hadamard transform twice starting with an m-sequence (this transform is referred to as *the second-order decimation-Hadamard transform (DHT)*, which will be defined in Section 2). Their work also shined a light along the path to settle the validity of Lin conjectured ternary 2-level autocorrelation sequences (1998) and to discover Ludkovski-Gong conjectured sequences (2000) which were obtained by applying the 2nd-order DHT to the Lin conjectured sequences. The proof given by Hu, Shao, Gong and Helleseth [35] in 2014 is through the 2nd-order DHT, and the second proof, given by Arasu, Dillion and Player [3] in 2015, is through character sum factorizations. Arasu-Dillion-Player also asserted the validity of Ludkovski-Gong conjectures.

So, we believe that it is time to revisit the research on 2-level autocorrelation sequences, since they not only play important roles in applications in 5G and beyond cellular communications, but also serve as building blocks for the constructions of sequences with optimal autocorrelation, low or zero correlation zone sequences as well as the salient applications in cryptography.

1.2 Sequences with low ambiguity

An auto ambiguity function of a one-dimensional sequence is a two-dimensional function in both time and frequency. The low values of an *ambiguity function* outside of the origin (0, 0) are required for determining the *range* (proportional to the time-delay) and for combating the *Doppler* shift (the velocity to or from the observer, proportional to the frequency shift, resulting in a phase shift) of a transmitted signal. Sequences with low ambiguity function can be achieved by Costas arrays, which yield the so-called *ideal* or *thumb-tack* ambiguity function (which only takes the values 0 or 1 at any shift not (0, 0)). But this is only applied to a single sequence, not a sequence set.

Heisenberg and Weil representation sequences Heisenberg and Weil representation sequences have played a central role in the development of sequence sets with low ambiguity. In 2006, Calderbank's group investigated sequences constructed from the Heisenberg representation [34]. Although the resulting sequences turned out to be the Frank-Chu sequences, this opens another direction of sequence design. In 2008, Gurevich, Hadani, and Sochen [28] introduced sequences constructed from the Weil representation. However, their sequences are not given in a mathematical analytical form, instead given in terms of an algorithm. Following their work, Wang and Gong [68] provided a new construction aiming for an explicit analytic formula for those sequences. Wang-Gong proved that their construction gives a simple elementary expression for the sequences from the Weil representation by Gurevich-Hadani-Sochen [28].

Interestingly, the sequences constructed by Wang and Gong are the element-wise product of Frank-Chu sequences and Legendre sequences, which can be respectively represented by additive characters and multiplicative characters of the finite field $\mathbb{F}_p$. In their paper, they asked for a direct proof for the correlation, ambiguity, and discrete Fourier transform (DFT). Shortly, Schmidt [57] responded this call, and found that the bounds for those metrics can be obtained directly by applying the Weil bound on hybrid character sums without any complex machinery deviation, and the bounds are also improved, compared with those established through the Weil representation by Gurevich, Hadani, and Sochen. We call the class constructed by Wang-Gong the *Weil representation sequences*, since they can also be constructed through the Weil representation.

Wang, Gong and Yu [70] extended the construction of the Weil representation sequences while the bounds on correlation, ambiguity, and DFT remain unchanged. Up to now, those sequence sets are the best with respect to correlation, ambiguity, DFT, and the sizes. In addition of those classes, there is another sequence set, proposed by Ding et al. [14], in which each sequence is the sum of the reciprocal pairs of m-sequences (we may call it a *Kloosterman sequence*, since it corresponds to the Kloosterman's sum). Ding et al. showed the bound on the ambiguity functions of the Kloosterman sequences using Li's beautiful result [40] on the DFT of the Kloosterman sequences.

New wireless transmission systems call for new sequences With rapid developments of 5G and beyond cellular communication systems, it calls new sequences for the applications in massive multi-input multi-output (MIMO), MIMO-OFDM, millimeter-wave (mm-wave) modulation systems, and the combinations of different modulation systems, such as orthogonal time frequency space (OTFS) modulation [29]. Basically, OTFS modulation first maps information symbols into a 2-dimensional signal which lies in a 2-dimensional time-delay and Doppler-shift space (i.e., a delay-Doppler space), then applies the so-called

symplectic Fourier transform (i.e., a special form of 2-dimensional Fourier transform), finally transfers to a time-domain signal for antenna transmission. So, this can be considered as a pre-coded OFDM transmission system. For those combinations of transmission systems, it requests the sequence sets with the capability for PMEPR reduction, low ambiguity, and large sizes. Another class of transmission system is sparse code multiple access. The codebook for those schemes is the combination of spreading code and frequency division multiple access. So similarly, it demands new sequence sets with good correlation and extraordinary larger sizes.

Gong [23] has presented a survey with a lot of deeper results on the sequences with low ambiguity, and Ding et al. [14] has investigated some bounds on ambiguity functions together with some new constructions with low ambiguity. The reader is referring to these two papers and the references therein. In this survey, we revisit the existing work for constructing sequence sets with low ambiguity, and provide some parameterized examples.

1.3 Golay complementary sequence sets and complete complementary codes

There exists no sequences with zero aperiodic autocorrelation at each out-of-phase shift. Innovatively, Golay [18] (1961) proposed to use two sequences which have the zero sum of their autocorrelation values at each out-of-phase shift, i.e., the orthogonality of a shifted sequence against the sequence is established by two sequences when he studied infrared spectrometry [17]. Such two sequences are called a *Golay pair*. About ten years later, Liu and Tseng [66] extended the concept of Golay pairs to a set of the sequences with the zero sum of their out-of-phase autocorrelation values, called *complementary sequence set (CSS)* for the binary case. In a few years later, Sivaswamy [59] (1978) extended it to the polyphase case. The other important concept introduced by Liu and Tseng in the same paper is the mutually orthogonal CSS. A largest set consisting of multiple mutually orthogonal CSSs is referred to as a *complete complementary code* (CCC).

Golay pairs and CSSs have found many applications in physics, combinatorics and telecommunications such as channel measurement, synchronization and spread spectrum communications. In particular, it has been proposed for power reduction in OFDM transmission due to high PMEPR of uncoded OFDM signals [12, 50]. CCCs were proposed to serve as a certain orthogonal transform, similar as the DFT, but the entries in a CCC matrix are sequences and the operation is the computation of cross/autocorrelation [66]. It also found an application in constructing zero correlation zone sequences more recently [52, 64, 65].

How can one systematically generate Golay pairs and CSSs? Golay [18] first proposed two recursive algorithms to construct binary Golay pairs of length 2^m. Davis and Jedwab realized that the algebraic structure of Golay sequences can be given by the specific second-order cosets of the first-order generalized Reed-Muller (GRM) code in their milestone work [12] in 1999. This is the so-called generalized Boolean function (GBF) method. Along this line, Paterson [50, 51], Schmidt [55, 56], and many excellent researchers contributed a large volume of works along this direction in the past years, including the constructions of the Golay pairs with low PMEPR over quadrature amplitude modulation (QAM) constellation which were first investigated by Tarokh et al. [53], just to list a few. For a more complete list of the references, please see [71].

The other approach is based on Hadamard matrices to construct CSSs and CCCs. In fact, the first recursive construction of CSSs and CCCs in 1972 [66] was obtained by Hadamard matrices. However, how to obtain the explicit function form of the sequences derived by

Hadamard-matrix-based methods is a long-standing problem for several decades. So these methods are not as popular as the GBF approaches in the literature. Recently, Budišin [6, 7] and Wang [72] (2016) revisited this method, which has strongly influenced our efforts to follow this path. Recently, we have made a progress [71] for constructing a special type of Hadamard matrices, called *parameter unitary (PU) matrices*, so are CSSs and CCCs, for which we can systematically extract explicit GBFs for the corresponding sequences, constructed from the PU matrices. This work showed that all known constructions on CSSs and CCCs can be explained by our PU-matrix-based constructions and abundant new ones come out.

In the remaining of this survey, we will introduce some basic concepts and definitions on sequences in Section 2. We will provide a summary of the progress of the sequences with 2-level autocorrelation in Section 3, and the known constructions of sequence sets with low ambiguity and some specific parameters in Section 4. Then we will turn our attention to introduce our progress on constructing CSSs and CCCs by the PU-matrix-based approaches in Section 5. Section 6 contains some concluding remarks and a collection of some aforementioned open problems. We list all acronyms appeared in this survey in Appendix for easy reference.

2 Basic concepts and definitions

In this section, we introduce some basic concepts on sequences and notations which will be used throughout the paper.

- $\mathcal{C}$ represents the complex field.
- For integer q, $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ is the residue class ring modulo q. $\mathbb{Z}_q^*$ denotes $\mathbb{Z}_q \backslash \{0\}$.
- $\mathbb{F}_{p^n}$ is a finite field where p is a prime and n is a positive integer, and $\mathbb{F}_{p^n}^*$ consists of nonzero elements of $\mathbb{F}_{p^n}$, and α is a primitive element in $\mathbb{F}_{p^n}$. We also denote $Q = p^n$.
- The trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is defined as

$$Tr(x) = x + x^p + \cdots + x^{p^{n-1}}, \ x \in \mathbb{F}_{p^n}.$$

- $\omega_k = e^{\frac{2\pi\sqrt{-1}}{k}} = e^{\frac{2\pi i}{k}} (i = \sqrt{-1})$ is a k th primitive root of unity.
- For every element $\beta \in \mathbb{F}_{p^n}^*$, there exists t with $0 \leqslant t \leqslant p^n - 2$, such that $\beta = \alpha^t$. In other words, $t = \log_\alpha \beta$, the discrete logarithm of β under the base α.
- We assume that $\log 0 = 0$ as a convention, and set $\omega_k^{\log_\alpha 0} = 1$.

We use notation $\mathbf{s} = \{s(t)\}$ to denote a complex valued sequence with infinite terms, i.e., $s(t) \in \mathcal{C}$. If it is a periodic sequence with period L, i.e., $s(t + L) = s(t)$, $\forall t$, we also denote it by a vector $\mathbf{s} = (s(0), \cdots, s(T-1))$. A sequence $\mathbf{f} = \{f(t)\}$ with infinite terms is a q-ary sequence with period L if $f(t) \in \mathbb{Z}_q$ where q is a positive integer, i.e.,

$$\mathbf{f} = (f(0), f(1), \cdots, f(L-1)), f(t) \in \mathbb{Z}_q.$$

In this survey, we associate a q-ary sequence with a function f, which is a map from $\mathbb{Z}_L$ to $\mathbb{Z}_q$. The representation of f depends on L, which will be introduced in more detail in the later sections. We always use $\mathbf{f}$, the bold f to represent the sequence and f, the function.

2.1 Periodic correlation and perfect sequences

Definition 1 Given two complex valued sequences, say $\mathbf{s}_0$ and $\mathbf{s}_1$ of period L, their periodic crosscorrelation function is defined as

$$R_{\mathbf{s}_0,\mathbf{s}_1}(\tau) = \sum_{t=0}^{L-1} s_1(t+\tau)\overline{s_0(t)},\ \tau = 0,\ \pm 1,\ \pm 2, \cdots$$

where $\overline{s_0(t)}$ is the complex conjugate of $s_0(t)$, and $t+\tau$ is reduced by modulo L. It becomes the autocorrelation when $\mathbf{s}_0 = \mathbf{s}_1 = \mathbf{s}$, denoted as $R_{\mathbf{s}}(\tau)$, i.e.,

$$R_{\mathbf{s}}(\tau) = \sum_{t=0}^{L-1} s(t+\tau)\overline{s(t)},\ \tau = 0,\ \pm 1,\ \pm 2, \cdots,$$

or simply as $R(\tau)$ if the contest is clear. For two q-ary sequences $\mathbf{f}_0$ and $\mathbf{f}_1$, their crosscorrelation function is defined as the crosscorrelation of $s_0(t) = \omega_q^{f_0(t)}$ and $s_1(t) = \omega_q^{f_1(t)}$, and it defines the autocorrelation of the sequence when they are equal.

In digital communications, generally, we consider a q-ary sequence $\{f(t)\}$ for representing information symbols, and its autocorrelation function is defined for the complex sequence $\left\{\omega_q^{f(t)}\right\}$ instead of $\{f(t)\}$ due to modulation for transmission.

Note that a periodic cross/autocorrelation function is also periodic with period L. So, we only need to consider $0 \le \tau < L$. The autocorrelation $R(\tau)$ at τ is also referred to as an *in-phase autocorrelation* if $\tau \equiv 0 \bmod L$, and *an out-of-phase autocorrelation* if $\tau \not\equiv 0 \bmod L$.

Remark 1 The cross/auto correlation function can be defined for two sequences with different periods, i.e., the correlation window length is the gcd of two periods.

Example 1 Let $\mathbf{f} = (1001011)$, a binary sequence with period 7. Then the autocorrelation of $\mathbf{f}$ is given by

$$R(\tau) = \sum_{t=0}^{6} (-1)^{s(t+\tau)+s(t)}.$$

Since this is an m-sequence of period 7, we have

$$R(\tau) = \begin{cases} 7, & \text{for } \tau \equiv 0 \bmod 7 \\ -1, & \text{otherwise.} \end{cases}$$

A q-ary sequence $\mathbf{f}$ is called a *perfect sequence* if all the out-of-phase (periodic) autocorrelation is equal to zero. Namely, the autocorrelation function is a delta function:

$$R(\tau) = \begin{cases} L, & \text{for } \tau \equiv 0 \bmod L \\ 0, & \text{otherwise.} \end{cases}$$

However, for the binary case, the only known perfect sequence, up to equivalence is $\mathbf{a} = (0111)$ (see [44] for details). A perfect sequence, treated as a random process,

is a white Gaussian noise, i.e., autocorrelation is a delta function. For nonbinary sequences, a Frank-Chu sequence is an integer sequence of period L in $\mathbb{Z}_{2L}$, the residue ring modular $2L$, mapped to a phase-sequence with a $2L$ th primitive root of unity with perfect autocorrelation, i.e., the out-of-phase of autocorrelation is equal to zero or equivalently, any out-of-phase sequence is orthogonal to the sequence (see [48, 60, 61] for the most recent constructions on p-ary perfect sequences). Frank-Chu sequences are proposed for channel estimation in 4G-LTE systems due to this orthogonality.

For an m-sequence with period $L = 2^n - 1$, we have the normalized autocorrelation:

$$\frac{R(\tau)}{L} = \begin{cases} 1, & for\ \tau \equiv 0 \mod L \\ -\frac{1}{L} \to 0 & (\tau \mod L) \neq 0, (n \to \text{large}). \end{cases}$$

This property of m-sequences resembles a white Gaussian noise, which makes it so popular in digital communications after Golomb successfully used it for detecting returning signals from Explorer 1. Examples include GPS, radar distance range, spread spectrum, and hardware testing, etc., which utilize this property.

A q-ary sequence of period L with the same autocorrelation as an m-sequence, is called an *(ideal) 2-level autocorrelation sequence*. All known binary 2-level autocorrelation sequences are collected in Golomb and Gong's book [19] which still holds the record up to the date, since there are no new 2-level autocorrelation sequences since then. For nonbinary cases, there is no discovery on new constructions for sequences with 2-level autocorrelation. However, there is a great advance for proving the conjectured ternary 2-level autocorrelation sequences, which will be presented in Section 3.

In addition of the effort for finding perfect nonbinary sequences for the applications in wireless communications, there are two major approaches to approximate perfect binary sequences: one is to use 2-level autocorrelation sequences, and the other is to use Golay pair or CSSs, which will be introduced in the next subsection.

Remark 2 For the optimal autocorrelation function of a binary sequence $\mathbf{f}$ of period L, it depends on the value of L:

L	R(τ)
$L \equiv 0 \bmod 4$	$R(\tau) \in \{L, 0\}$
$L \equiv 3 \bmod 4$	$R(\tau) \in \{L, -1\}$
$L \equiv 1 \bmod 4$	$R(\tau) \in \{L, 1, -3\}$
$L \equiv 2 \bmod 4$	$R(\tau) \in \{L, 2, -2\}$

The first two cases are the cases of perfect sequences and 2-level autocorrelation sequences respectively. For the last two cases, the constructions are largely from residue classes [4, 15]. In general, the last two cases are more costly in their implementations. This observation is solely from their mathematical constructions and computational complexity. Nevertheless, there has been no report in the literature about their implementations yet, which may be worth to do some research on this problem, although it leans to more engineering perspective. In Section 4, we will provide the power residue sequences which is optimal in Case 3.

2.2 Aperiodic correlation and Golay complementary pairs/sets

Given a complex valued sequence of length L, $\mathbf{s} = (s(0), s(1), \cdots, s(L-1))$, we extend it to a sequence with an infinite length by setting

$$s(t) = 0 \text{ for both } t < 0 \text{ and } t \geq L. \tag{1}$$

The aperiodic correlation is defined for this aperiodic extension of $\mathbf{s}$.

Definition 2 For two complex valued sequences $\mathbf{s}_0$ and $\mathbf{s}_1$ of length L, the *aperiodic crosscorrelation function* of $\mathbf{s}_0$ and $\mathbf{s}_1$ at shift τ is defined by

$$C_{\mathbf{s}_0,\,\mathbf{s}_1}(\tau) \;=\; \sum_{t=0}^{L-1} s_1(t+\tau)\overline{s_0(t)},\; -L \;<\; \tau \;<\; L.$$

If $\mathbf{s}_0 = \mathbf{s}_1 = \mathbf{s}$, it becomes the *aperiodic autocorrelation* of sequence $\mathbf{s}$ at shift τ, i.e.,

$$C_{\mathbf{s}}(\tau) \;= C_{\mathbf{s},\,\mathbf{s}}(\tau) \;=\; \sum_{t=0}^{L-1} s(t+\tau)\overline{s(t)},\; -L \;<\; \tau \;< L$$

or simply as $C(\tau)$. For two q-ary sequences $\boldsymbol{f}_0$ and $\boldsymbol{f}_1$ of length L, the *aperiodic crosscorrelation function* of $\boldsymbol{f}_0$ and $\boldsymbol{f}_1$ at shift τ is defined as the aperiodic crosscorrelation of $\mathbf{s}_j = \left\{\omega_q^{f_j(t)}\right\}, j = 0, 1$, the aperiodic autocorrelation of a q-ary sequence $\mathbf{f}$ is also defined in analogue.

In this survey, we use $R_{\mathbf{f}_0,\mathbf{f}_1}(\tau)$ and $R(\tau)$ to represent periodic crosscorrelation and autocorrelation functions respectively, and $C_{\mathbf{f}_0,\mathbf{f}_1}(\tau)$ and $C(\tau)$, aperiodic crosscorrelation and autocorrelation functions.

Aperiodic correlation functions correspond to the functionality of matched filters in wireless transmission.

Example 2 We take $q = 4$, $L = 4$, $\mathbf{f} = (0,1,0,3)$. In this case, we have $\omega_4 = i, i = \sqrt{-1}$. So, $\left\{i^k | k = 0, 1, 2, 3\right\} = \{1, i, -1, -i\}$. Aperiodic autocorrelation computation in the fashion of a matched filter detection is shown as follows.

$f(t+\tau)$	$-f(t)$		τ	$C(\tau)$
	0 3 0 1			
0 1 0 3				
0 1 0	3		3	$-i$
0 1	0 3		2	0
0	1 0 3		1	$-i$
	0 1 0 3		0	4 (matched)
	0 1 0	3	-1	i
	0 1	0 3	-2	0
	0	1 0 3	-3	i

Due to the following property, we only need to compute autocorrelation $C(\tau)$ for $0 < \tau < L$.

$$C(\tau) = \overline{C(-\tau)}, \forall \tau.$$

Proposition 1

A perfect sequence can also be defined by aperiodic autocorrelation in a similar way as the periodic case. Unfortunately, there is no single sequence with zero aperiodic autocorrelation at every shift. The best case is the so-called *Barker sequences*, i.e., the magnitude of the out-of-phase aperiodic autocorrelation values are bounded by 1, i.e., $|C(\tau)| \leq 1$ for $\tau \neq 0$, $-L < \tau < L$ (see [19] for more details about Barker sequences).

Definition 3 A set of q-ary sequences $S = \{\boldsymbol{f}_0, \boldsymbol{f}_1, \cdots, \boldsymbol{f}_{N-1}\}$ is called a *complementary sequence set* (CSS) of size N if

$$\sum_{u=0}^{N-1} C_{\boldsymbol{f}_u}(\tau) = 0 \text{ for } \tau \not\equiv 0 \ (\mathrm{mod} L). \tag{2}$$

If the set size $N = 2$, such a set is called a *Golay (complementary) pair*. Each sequence in a Golay pair is called a *Golay sequence*.

Remark 3 In a wireless transmission system, a transmitter may use two sequences, i.e., a Golay pair for transmitting the same information symbols using each sequence. At the receiver side, it will employ two correlators to compute their respective autocorrelation functions of each received signal (i.e., the sequence) with the corresponding locally generated sequences. So, this resembles the space redundancy, i.e., a 2×2 MIMO transmission system.

Example 3 For binary sequences $\mathbf{f}_0 = (0001)$ and $\mathbf{f}_1 = (0010)$, we have

$\mathbf{f}_0 = (0001)$	$\{C_{\mathbf{f}_0}(\tau)\}_{\tau=1}^{3} = \{1, 0, -1\}$
$\mathbf{f}_1 = (0010)$	$\{C_{\mathbf{f}_1}(\tau)\}_{\tau=1}^{3} = \{-1, 0, 1\}$

Thus, they form a Golay pair.

In the following definitions, the given sequences being complex sequences or q-ary sequences depend on the context. Two CSSs

$$S_0 = \{\boldsymbol{f}_{0,0}, \boldsymbol{f}_{0,1}, \cdots, \boldsymbol{f}_{0,N-1}\}, \text{and}$$
$$S_1 = \{\boldsymbol{f}_{1,0}, \boldsymbol{f}_{1,1}, \cdots, \boldsymbol{f}_{1,N-1}\}$$

are said to be *mutually orthogonal* if

$$\sum_{v=0}^{N-1} C_{\boldsymbol{f}_{0,v}, \boldsymbol{f}_{1,v}}(\tau) = 0 \text{ for } \forall \tau. \tag{3}$$

Definition 4 Let $S_u = \{\boldsymbol{f}_{u,0}, \boldsymbol{f}_{u,1}, \cdots, \boldsymbol{f}_{u,N-1}\}$ be CSSs of size N for $0 \le u < N$, which are pairwise mutually orthogonal. Such a collection of S_u is called *complete mutually orthogonal complementary sets* (CMOCS) or *complete complementary codes* (CCC).

Example 4 Let $N = 2$ and let binary sequences sets be given as follows.

$$S_0 = \{\mathbf{f}_{00} = (0001), \mathbf{f}_{01} = (0010)\}$$
$$S_1 = \{\mathbf{f}_{10} = (0100), \mathbf{f}_{11} = (0111)\}.$$

From Example 3, the first set is a Golay pair. We can easily verify that S_1 is also a Golay pair, and two sets are mutually orthogonal. So $\{S_0, S_1\}$ forms a CCC.

For quaternary sequences of length 4, we have the following example for CCC:

$$S = \begin{bmatrix} \mathbf{f}_{0,0} = (0,1,0,3), & \mathbf{f}_{0,1} = (0,1,2,1) \\ \mathbf{f}_{1,0} = (0,3,0,1), & \mathbf{f}_{1,1} = (0,3,2,3) \end{bmatrix}.$$

In other words, each row is a Golay pair and two rows are mutually orthogonal.

We have the following relation between the periodic and aperiodic correlation functions.

Proposition 2

$$R(\tau) = C(\tau) + \overline{C(L-\tau)} = C(\tau) + C(\tau - L), \forall \tau.$$

2.3 The discrete Fourier transform

The discrete Fourier transform (DFT) of a q-ary sequence $\mathbf{f} = \{f(t)\}$ of period L is defined as

$$\hat{f}(k) = \sum_{t=0}^{L-1} \omega_q^{f(t)} e^{\frac{-\sqrt{-1}2\pi kt}{L}} = \sum_{t=0}^{L-1} \omega_q^{f(t)} \omega_L^{-kt}, 0 \le k < L.$$

(Recall that $\omega_L = e^{\frac{\sqrt{-1}2\pi}{L}}$.) The inverse DFT (IDFT) is given by

$$\omega_q^{f(t)} = \frac{1}{L} \sum_{k=0}^{L-1} \hat{f}(k) \omega_L^{tk}, 0 \le t < L.$$

DFT can also be given in a matrix form:

$$\begin{pmatrix} \hat{f}(0) \\ \hat{f}(1) \\ \hat{f}(2) \\ \vdots \\ \hat{f}(L-1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_L^{-1} & \omega_L^{-2} & \cdots & \omega_L^{-(L-1)} \\ 1 & \omega_L^{-2} & \omega_L^{-4} & \cdots & \omega_L^{-2(L-1)} \\ \vdots & & & & \\ 1 & \omega_L^{-(L-1)} & \omega_L^{-2(L-1)} & \cdots & \omega_L^{-(L-1)^2} \end{pmatrix} \cdot \begin{pmatrix} \omega_q^{f(0)} \\ \omega_q^{f(1)} \\ \omega_q^{f(2)} \\ \vdots \\ \omega_q^{f(L-1)} \end{pmatrix}$$

where the exponents of ω_L is reduced by modulo L, since $\omega_L^L = 1$. The $L \times L$ matrix in the above identity is referred to as *the DFT matrix*.

Example 5 For the m-sequence of period 7, $\mathbf{f} = \{f(t)\} = (1110100)$, we have $\{(-1)^{f(t)}\} = (-1, -1, -1, 1, -1, 1, 1)$. The DFT of $\mathbf{f}$ is given by

$$\begin{pmatrix} \hat{f}(0) \\ \hat{f}(1) \\ \hat{f}(2) \\ \hat{f}(3) \\ \hat{f}(4) \\ \hat{f}(5) \\ \hat{f}(6) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega_7^6 & \omega_7^5 & \omega_7^4 & \omega_7^3 & \omega_7^2 & \omega_7 \\ 1 & \omega_7^5 & \omega_7^3 & \omega_7 & \omega_7^6 & \omega_7^4 & \omega_7^2 \\ 1 & \omega_7^4 & \omega_7 & \omega_7^5 & \omega_7^2 & \omega_7^6 & \omega_7^3 \\ 1 & \omega_7^3 & \omega_7^6 & \omega_7^2 & \omega_7^5 & \omega_7 & \omega_7^4 \\ 1 & \omega_7^2 & \omega_7^4 & \omega_7^6 & \omega_7 & \omega_7^3 & \omega_7^5 \\ 1 & \omega_7 & \omega_7^2 & \omega_7^3 & \omega_7^4 & \omega_7^5 & \omega_7^6 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ -1 \\ -1 \\ 1 \\ -1 \\ 1 \\ 1 \end{pmatrix}$$

where $\omega_7 = e^{i2\pi/7}$ and $i = \sqrt{-1}$. After the evaluation, we have

$$\begin{pmatrix} \hat{f}(0) \\ \hat{f}(1) \\ \hat{f}(2) \\ \hat{f}(3) \\ \hat{f}(4) \\ \hat{f}(5) \\ \hat{f}(6) \end{pmatrix} = 2 \cdot \begin{pmatrix} -1/2 & & \\ \omega_7^4 & +\omega_7^2 & +\omega_7 \\ \omega_7 & +\omega_7^4 & +\omega_7^2 \\ \omega_7^5 & +\omega_7^6 & +\omega_7^3 \\ \omega_7^2 & +\omega_7 & +\omega_7^4 \\ \omega_7^6 & +\omega_7^3 & +\omega_7^5 \\ \omega_7^3 & +\omega_7^5 & +\omega_7^6 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 + 2.646i \\ -1 + 2.646i \\ -1 - 2.646i \\ -1 + 2.646i \\ -1 - 2.646i \\ -1 - 2.646i \end{pmatrix}.$$

2.4 Ambiguity functions

Given a complex sequence $\mathbf{s} = \{s(t)\}$ of period L, a *phase-shift* of $\mathbf{s}$ is given by $\{s(t)\omega_L^{kt}\}$ for a fixed $k : 0 \le k < L$. A phase-shift of a q-ary sequence $\mathbf{f}$ is defined for $\mathbf{s} = \omega_q^{\mathbf{f}}$, i.e., $\left\{\omega_q^{f(t)}\omega_L^{kt}\right\}$.

Definition 5 Let $\mathbf{s}_0$ and $\mathbf{s}_1$ be two complex valued sequences. Then the periodic cross ambiguity function of $\mathbf{s}_0$ and $\mathbf{s}_1$ at (τ,k) is defined as

$$A_{\mathbf{s}_0,\mathbf{s}_1}(\tau, k) = \sum_{t=0}^{L-1} s_1(t+\tau)\overline{s_0(t)}\omega_L^{-kt}, 0 \le \tau, k < L, \tag{4}$$

which is a 2-dimensional function in variables τ, delayed time, and k, the Doppler variable where $t + \tau$ is reduced by modulo L. When $\mathbf{s}_0 = \mathbf{s}_1 = \mathbf{s}$, it is referred to as the auto ambiguity function of the sequence $\mathbf{s}$, or simply the ambiguity function, i.e.,

$$A_{\mathbf{s}}(\tau, k) = \sum_{t=0}^{L-1} s(t+\tau)\overline{s(t)}\omega_L^{-kt}, 0 \le \tau, k < L,$$

or simply as $A(\tau,k)$. For two q-ary sequences $\mathbf{f}_0$ and $\mathbf{f}_1$, the cross ambiguity function of $\mathbf{f}_0$ and $\mathbf{f}_1$ is defined for $\mathbf{s}_0 = \left\{\omega_q^{f_0(t)}\right\}$ and $\mathbf{s}_1 = \left\{\omega_q^{f_1(t)}\right\}$. It becomes the auto ambiguity function of $\mathbf{f}$ when $\mathbf{f}_0 = \mathbf{f}_1 = \mathbf{f}$.

Remark 4 For the concept of ambiguity functions, there are several different definitions: in signal processing, it uses $\overline{A}(\tau, k)$; it may conjugate the term $s(t + \tau)$ instead of $s(t)$ (e.g., in [68]). However, we adopt the above definition in order to keep the conventional notation in sequence design. This will be clearly seen in the following definition for q-ary sequences. But for all the different definitions, the set consisting all values of $A(\tau,k)$ is not changed.

Remark 5 From the definition of the ambiguity function, when $k=0$, the cross/auto ambiguity function becomes the cross/auto correlation. Thus a bound on the ambiguity function is also the bound of correlation. However, in some cases, the correlation has a better bound than the ambiguity function.

We may write the auto ambiguity function as a 2-dimensional array:

$$A=\begin{pmatrix} A(0,0) & A(0,1) & A(0,2) & \cdots & A(0,L-1) \\ A(1,0) & A(1,1) & A(1,2) & \cdots & A(1,L-1) \\ A(2,0) & A(2,1) & A(2,2) & \cdots & A(2,L-1) \\ \vdots & & & & \\ A(L-1,0) & A(L-1,1) & A(L-1,2) & \cdots & A(L-1,L-1) \end{pmatrix}.$$

We define a time-shift matrix of $\mathbf{s}$ as

$$T=\begin{pmatrix} s(0) & s(1) & s(2) & \cdots & s(L-2) & s(L-1) \\ s(1) & s(2) & s(3) & \cdots & s(L-1) & s(0) \\ \vdots & & & & & \\ s(L-1) & s(0) & s(1) & \cdots & s(L-3) & s(L-2) \end{pmatrix}$$

and the phase-shift matrix of the sequence $\mathbf{s}$ is given by

$$P=\begin{pmatrix} s(0) & s(0) & s(0) & \cdots & s(0) \\ s(1) & s(1)\omega_L^1 & s(1)\omega_L^2 & \cdots & s(1)\omega_L^{L-1} \\ s(2) & s(2)\omega_L^2 & s(2)\omega_L^4 & \cdots & s(2)\omega_L^{2(L-1)} \\ \vdots & & & & \\ s(L-1) & s(L-1)\omega_L^{L-1} & s(L-1)\omega_L^{2(L-1)} & \cdots & s(L-1)\omega_L^{(L-1)^2} \end{pmatrix}.$$

Then we have the following representation

$$A=T\overline{P}$$

where $\overline{P}$ is the conjugate of the phase-shift matrix P by conjugating each entry in P. The cross ambiguity function also can be represented similarly.

Example 6 For the m-sequence of period 7, $\mathbf{f}=\{f(t)\}=(1110100)$, $s(t)=(-1)^{f(t)}$. The time-shift matrix and the conjugate of the phase-shift matrix of the m-sequence are given as follows.

$$T=\begin{pmatrix} -1 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

and

$$\overline{P} = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -\omega_7^6 & -\omega_7^5 & -\omega_7^4 & -\omega_7^3 & -\omega_7^2 & -\omega_7 \\ -1 & -\omega_7^5 & -\omega_7^3 & -\omega_7 & -\omega_7^6 & -\omega_7^4 & -\omega_7^2 \\ 1 & \omega_7^4 & \omega_7 & \omega_7^5 & \omega_7^2 & \omega_7^6 & \omega_7^3 \\ -1 & -\omega_7^3 & -\omega_7^6 & -\omega_7^2 & -\omega_7^5 & -\omega_7 & -\omega_7^4 \\ 1 & \omega_7^2 & \omega_7^4 & \omega_7^6 & \omega_7 & \omega_7^3 & \omega_7^5 \\ 1 & \omega_7 & \omega_7^2 & \omega_7^3 & \omega_7^4 & \omega_7^5 & \omega_7^6 \end{pmatrix}.$$

Thus, the ambiguity function of the m-sequence $\mathbf{f}$ is given by $A = T\overline{P}$, as shown below

$$A = T\overline{P} = \begin{pmatrix} 7.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ -1.0000 & 2.8019 & -0.2470 & 1.4450 & 1.4450 & -0.2470 & 2.8019 \\ -1.0000 & -0.2470 & 1.4450 & 2.8019 & 2.8019 & 1.4450 & -0.2470 \\ -1.0000 & -2.3569 & 2.0489 & -2.6920 & -2.6920 & 2.0489 & -2.3569 \\ -1.0000 & 1.4450 & 2.8019 & -0.2470 & -0.2470 & 2.8019 & 1.4450 \\ -1.0000 & -2.6920 & -2.3569 & 2.0489 & 2.0489 & -2.3569 & -2.6920 \\ -1.0000 & 2.0489 & -2.6920 & -2.3569 & -2.3569 & -2.6920 & 2.0489 \end{pmatrix}$$
$$+ \begin{pmatrix} 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.3862 & -2.8176 & -2.4314 & 2.4314 & 2.8176 & -0.3862 \\ 0.0000 & -2.8176 & 2.4314 & -0.3862 & 0.3862 & -2.4314 & 2.8176 \\ 0.0000 & -1.5637 & -1.9499 & -0.8678 & 0.8678 & 1.9499 & 1.5637 \\ 0.0000 & 2.4314 & 0.3862 & 2.8176 & -2.8176 & -0.3862 & -2.4314 \\ 0.0000 & 0.8678 & -1.5637 & 1.9499 & -1.9499 & 1.5637 & -0.8678 \\ 0.0000 & -1.9499 & 0.8678 & 1.5637 & -1.5637 & -0.8678 & 1.9499 \end{pmatrix} \cdot i$$

and

$$|A(\tau, k)| = \begin{pmatrix} 7.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 1.0000 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 \\ 1.0000 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 \\ 1.0000 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 \\ 1.0000 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 \\ 1.0000 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 \\ 1.0000 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 & 2.8284 \end{pmatrix}$$

which is shown in Fig. 1.

For a sequence given by

$$\mathbf{g} = (1010110)$$
$$\left\{(-1)^{g(t)}\right\} = (-1, 1, -1, 1, -1, -1, 1).$$

Note this is the sum of two m-sequences of period 7, so we can compute its ambiguity function using the matrix method as follows. The time-shift matrix $T_{\mathbf{g}}$ is given by

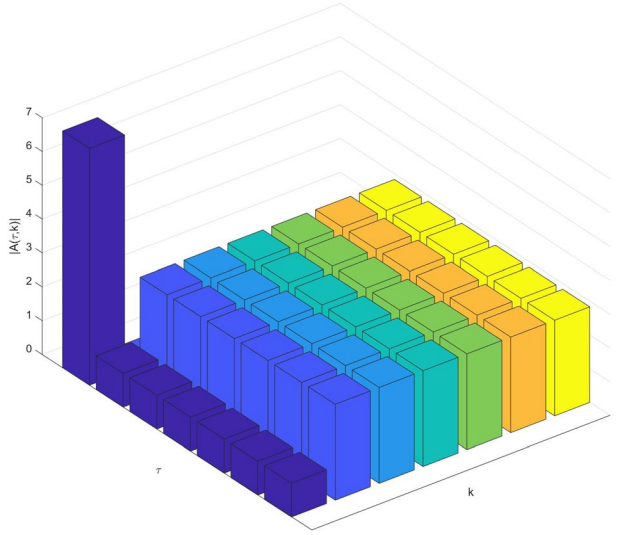


Fig. 1 $|A(\tau,k)|$ for m-sequence $\mathbf{f} = (1110100)$

$$T_{\mathbf{g}} = \begin{pmatrix} -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix}$$

and the conjugate of the phase shift matrix, $P_{\mathbf{g}}$, as follows.

$$\overline{P_{\mathbf{g}}} = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & \omega_7^6 & \omega_7^5 & \omega_7^4 & \omega_7^3 & \omega_7^2 & \omega_7 \\ -1 & -\omega_7^5 & -\omega_7^3 & -\omega_7 & -\omega_7^6 & -\omega_7^4 & -\omega_7^2 \\ 1 & \omega_7^4 & \omega_7 & \omega_7^5 & \omega_7^2 & \omega_7^6 & \omega_7^3 \\ -1 & -\omega_7^3 & -\omega_7^6 & -\omega_7^2 & -\omega_7^5 & -\omega_7 & -\omega_7^4 \\ -1 & -\omega_7^2 & -\omega_7^4 & -\omega_7^6 & -\omega_7 & -\omega_7^3 & -\omega_7^5 \\ 1 & \omega_7 & \omega_7^2 & \omega_7^3 & \omega_7^4 & \omega_7^5 & \omega_7^6 \end{pmatrix}.$$

Thus, the ambiguity function of the sequence $\mathbf{g} = (1010110)$ is

$$A_{\mathbf{g}} = T_{\mathbf{g}}\overline{P_{\mathbf{g}}} = \begin{pmatrix} 7.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ -5.0000 & -1.8019 & 1.2470 & -0.4450 & -0.4450 & 1.2470 & -1.8019 \\ 3.0000 & 3.6039 & -2.4940 & 0.8901 & 0.8901 & -2.4940 & 3.6039 \\ -1.0000 & -4.0489 & 0.6920 & 0.3569 & 0.3569 & 0.6920 & -4.0489 \\ -1.0000 & 2.8019 & -0.2470 & 1.4450 & 1.4450 & -0.2470 & 2.8019 \\ 3.0000 & -0.8019 & 2.2470 & 0.5550 & 0.5550 & 2.2470 & -0.8019 \\ -5.0000 & -0.4450 & -1.8019 & 1.2470 & 1.2470 & -1.8019 & -0.4450 \end{pmatrix}$$
$$+ \begin{pmatrix} 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.8678 & -1.5637 & 1.9499 & -1.9499 & 1.5637 & -0.8678 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & -1.9499 & 0.8678 & 1.5637 & -1.5637 & -0.8678 & 1.9499 \\ 0.0000 & 3.5135 & 1.0821 & -0.6959 & 0.6959 & -1.0821 & -3.5135 \\ 0.0000 & -3.5135 & -1.0821 & 0.6959 & -0.6959 & 1.0821 & 3.5135 \\ 0.0000 & 1.9499 & -0.8678 & -1.5637 & 1.5637 & 0.8678 & -1.9499 \end{pmatrix} \cdot i$$

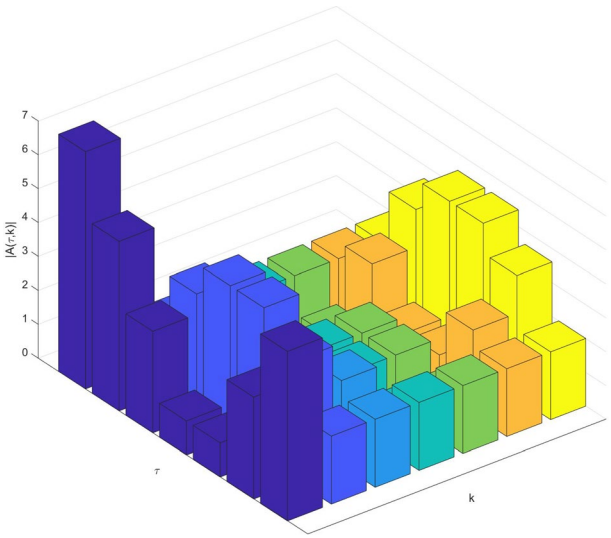
and

$$|A_{\mathbf{g}}(\tau, k)| = \begin{pmatrix} 7.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 5.0000 & 2.0000 & 2.0000 & 2.0000 & 2.0000 & 2.0000 & 2.0000 \\ 3.0000 & 3.6039 & 2.4940 & 0.8901 & 0.8901 & 2.4940 & 3.6039 \\ 1.0000 & 4.4940 & 1.1099 & 1.6039 & 1.6039 & 1.1099 & 4.4940 \\ 1.0000 & 4.4940 & 1.1099 & 1.6039 & 1.6039 & 1.1099 & 4.4940 \\ 3.0000 & 3.6039 & 2.4940 & 0.8901 & 0.8901 & 2.4940 & 3.6039 \\ 5.0000 & 2.0000 & 2.0000 & 2.0000 & 2.0000 & 2.0000 & 2.0000 \end{pmatrix}$$

which is shown in Fig. 2.

We can also define the aperiodic ambiguity functions of sequences as follows.

Fig. 2 $|A_{\mathbf{g}}(\tau,k)|$ for $\mathbf{g} = (1010110)$



Definition 6 Let $\mathbf{s}_0$ and $\mathbf{s}_1$ be two complex-valued sequences of length L and extended into infinite length by (1), i.e., $s_i(t) = 0, i = 0,1$ for $t < 0$ and $t \geq L$. The aperiodic cross ambiguity function of $\mathbf{s}_0$ and $\mathbf{s}_1$ at (τ,k) is defined as

$$A_{\mathbf{s}_0,\mathbf{s}_1}(\tau,k) = \sum_{t=0}^{L-1} s_1(t+\tau)\overline{s_0(t)}\omega_L^{-kt},\ -L < \tau < L, 0 \leq k < L \tag{5}$$

and it defines the auto ambiguity function of the sequence $\mathbf{s}$ when $\mathbf{s}_0 = \mathbf{s}_1 = \mathbf{s}$, i.e.,

$$A_{\mathbf{s}}(\tau,k) = \sum_{t=0}^{L-1} s(t+\tau)\overline{s(t)}\omega_L^{-kt}, -L < \tau < L, 0 \leq k < L. \tag{6}$$

The aperiodic cross ambiguity function of two q-ary sequences $\mathbf{f}_0$ and $\mathbf{f}_1$ is defined for $\mathbf{s}_k = \omega^{\mathbf{f}_k}, k = 0, 1$ and it defines the aperiodic auto ambiguity function when $\mathbf{f}_0 = \mathbf{f}_1$.

Note that Turyn [67] defined the aperiodic cross ambiguity function of two sequences of length L using continuous phase shift, i.e., the phase shift term $\omega_L^{-kt} = e^{\frac{-i2\pi kt}{L}}$ is replaced by $e^{it\theta}$ where $0 \leq \theta < 2\pi$. The phase shift term in the ambiguity function in [23] also considered a more general case, i.e., it can be any discrete phase shift, not restricted to L phases. Currently, there are no constructions for a sequence (or signal) set (it may not be a CSS) even for low aperiodic correlation, not to mention low aperiodic ambiguity. But there are some constructions for the sequence sets with low periodic ambiguity. We will introduce those constructions in Section 4.

Remark 6 In fact, periodic and aperiodic correlation and ambiguity functions can be given by the same formulae. The difference is that an infinite extension of $\mathbf{s} = (s(0), s(1), \cdots, s(L-1))$ of length L is a periodic extension for the periodic case, and the zero extension for the aperiodic case.

3 Two-level autocorrelation sequences

The research on constructions for 2-level autocorrelation sequences has been gloriously active for more than 7 decades. Those sequences correspond to the combinatorial design, i.e., cyclic Hadamard difference sets. The constructions are mainly based on finite fields except for the binary case. For the references, the reader is referring to [19].

3.1 The second-order decimation-Hadamard transform

Since one of the proofs of Lin conjecture and Ludkovski-Gong conjectured sequences with 2-level autocorrelation are obtained by applying the second-order decimation-Hadamard transform (DHT), which was introduced by Golomb and Gong in 2002. Below we introduce the definitions together with its extension of the multiplexing case.

Definition 7 Let $f(x)$ be a function from $\mathbb{F}_Q$ to $\mathbb{F}_p$ ($Q = p^n$). The Hadamard transform of f is defined as

$\widehat{f}(\lambda) = \sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)-f(x)}, \lambda \in \mathbb{F}_Q$, and its inverse transform is
$\omega_p^{f(\lambda)} = \frac{1}{Q}\sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)}\overline{\widehat{f}(\lambda)}$

Definition 8 For integers $0 < v,t < Q-1$ with $\gcd(v, Q-1) = 1$ and $\gcd(t, Q-1) = 1$, the first-order DHT is defined as the Hadamard transform of $f(x^v)$, i.e.,

$$\widehat{f}(v)(\lambda) = \sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)-f(x^v)}, \lambda \in \mathbb{F}_Q,$$

and the second-order DHT is defined as the Hadamard transform of $\widehat{f}(v)(x^t)$, i.e.,

$$\widehat{f}(v,t)(\lambda) = \sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)}\overline{\widehat{f}(v)(x^t)}, \lambda \in \mathbb{F}_Q.$$

Definition 9 If

$$\widehat{f}(v,t)(\lambda) \in \left\{ Q\omega_p^t | 0 \le t < p \right\}, \lambda \in \mathbb{F}_Q,$$

then we define a function $g : \mathbb{F}_Q \mapsto \mathbb{F}_p$ as

$$\omega_p^{g(x)} = \widehat{f}(v,t)(\lambda), \lambda \in \mathbb{F}_Q$$

where (v,t) is called a realizable pair of $f(x)$ and $g(x)$, a realization of $f(x)$.

From Parseval formula, the following result follows immediately (see [19]).

Proposition 3 For the pair $f(x)$ and $g(x)$ in Definition 9, the p-ary sequence $\{f(\alpha^t)\}$ has 2-level autocorrelation if and only if the p-ary sequence $\{g(\alpha^t)\}$ has 2-level autocorrelation.

If $d = \gcd(v, Q-1) > 1$, then x^v is not a permutation of $\mathbb{F}_Q$. So we need multiple pieces of the first-order DHT in order to get $g(x)$, which is called a *multiplexing DHT*, defined as follows.

Definition 10 For integers $0 < v,t < Q-1$ with $d = \gcd(v, Q-1) > 1$ and $\gcd(t, Q-1) = 1$, the first-order *multiplexing* DHT is defined as

$$\widehat{f}(v)(\lambda,\gamma) = \sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)-f(\gamma x^v)}, \lambda \in \mathbb{F}_Q, \gamma \in \mathbb{F}_Q^*,$$

and the second-order *multiplexing* DHT is

$$\widehat{f}(v,t)(\lambda,\gamma) = \sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)}\overline{\widehat{f}(v)(x^t,\gamma)}, \lambda \in \mathbb{F}_Q, \gamma \in \mathbb{F}_Q^*.$$

Furthermore, if

$$\widehat{f}(v,t)(\lambda,\gamma) \in \left\{ Q\omega_p^t | 0 \le t < p \right\}, \lambda \in \mathbb{F}_Q, \gamma \in \mathbb{F}_Q^*,$$

then we define a function $g : \mathbb{F}_Q \mapsto \mathbb{F}_p$ as

$$\omega_p^{g(\alpha^{kv+j})} = \widehat{f}(v,t)\left(\alpha^k, \alpha^j\right), 0 \le k < s, 0 \le j < d, \text{where} s = \frac{Q-1}{d}, g(0) = 0$$

(recall that α is a primitive element of $\mathbb{F}_Q$) and (v,t) is called a *realizable pair* of $f(x)$, and $g(x)$, a *multiplexing realization* of $f(x)$.

Proposition 4 [35] With the notation in Definition 10, the p-ary sequence $\{f(\alpha^t)\}$ has 2-level autocorrelation if and only if the multiplexing p-ary sequence $\{g(\alpha^t)\}$ has 2-level autocorrelation.

The following concept was introduced by Golomb and Gong as an alternative way to define a Hadamard equivalent relation, based on the concept introduced by Dillon and Dobbertin.

Definition 11 If $g(x)$ is a realization of $f(x)$ by the second-order DHT or multiplexing DHT, then we say that g is Hadamard equivalent to f.

3.2 Known constructions

The known primary constructions of binary sequences of period L:

1. Number theory based construction: L is prime and $L \equiv 3 \bmod 4$, we have quadratic residue sequences or called Legendre sequences (1932); furthermore, if $L = 4a^2 + 27$, we have Hall's sextic residue sequences (Hall 1957).
2. Finite fields based constructions for $L = 2^n - 1$ where n is a positive integer:
   - m-sequences by Singer (1938 in the form of cyclic Hadamard difference sets) and Golomb (1954).
   - For $n \ge 6$, n composite, we have GMW sequences, constructed by Goldon, Mills and Welch in 1962 in the language of cyclic Hadamard difference sets, and Scholtz and Welch provided a sequence version in 1984).
   - Hyper-oval constructions by Maschietti (1998) for which there are three constructions using three types of monomial hyper-ovals, i.e., Segre, and Glynn I and II cases.
   - Dillon-Dobbertin's Kasami power function construction (2004): Dillon and Dobbertin in their milestone work published in 2004 using the Kasami exponents to construct binary sequences with 2-level autocorrelation, which include the conjectured 3-term, 5-term sequences and Welch-Gong (WG) sequences as subclasses.

The known primary constructions for $p > 2$-ary case:

1. For $p > 2$, m-sequences (Zieler, 1959), GMW sequences (1962), and HG sequences [31] (2002) (also found by Dillion independently) including Helleseth-Kumar-Martin's ternary sequences as a special case.
2. For $p = 3$, conjectured sequences:
   - Lin conjecture (1998): Let $n = 2m + 1$ and

$$f(x) = Tr(x + x^d), \text{where} d = 2 \cdot 3^m + 1.$$

Lin, in his Ph.D thesis, conjectured that $\{f(\alpha^t)\}$ has 2-level autocorrelation where α is a primitive element of $\mathbb{F}_{3^n}$. The conjecture has been proved by two different research groups, one is given by Hu, Shao, Gong and Helleseth [35] in 2014, and the other, by Arasu, Dillon and Player [3] in 2015.

– Ludkovski and Gong conjectures [42] (2001): Starting with a Lin conjectured sequence, applying the 2nd-order DHT, four classes of new ternary 2-level autocorrelation sequences are obtained, namely A, B, C and D where the class D contains classes B and C. Ludkovski and Gong differentiated them from the class D because of the similarity to their counter part $p = 2$. The validity of these two classes of the ternary sequences is also established by Arasu-Dillon-Player in the same paper [3].

The known secondary construction For p-ary case (p prime), there is a secondary construction for p-ary 2-level autocorrelation sequences of period $p^n - 1$, which is given by compositing a 2-level autocorrelation sequence with period $p^m - 1$ where m is a proper factor of n and an m-sequence over $\mathbb{F}_{p^m}$ of degree n/m or generalized GMW sequence over $\mathbb{F}_{p^m}$. (See [19] for details.) Note that No [47] observed that it can composite with a sequence over $\mathbb{F}_{p^m}$ with the uniform difference condition. However, the known sequences over $\mathbb{F}_{p^m}$ having the uniform difference condition are only the aforementioned m-sequences and GMW sequences.

3.3 Some observations on the proofs for the conjectures

Ludkovski-Gong conjectured sequences are the realizations of f, the 2-term function in Lin conjecture, with the two different classes of the realizable pairs. The condition on k with $\gcd(m-k, n) = 1$, marked by * in Table 1 was added by Arasu-Dillon-Player [3] in their proof.

The validity of Lin conjecture and Ludkovski-Gong conjecture is confirmed after more than one and half decades later since the conjectures were formed. Both proofs for Lin conjecture are rather technical. The proof given by Hu-Shao-Gong-Helleseth is to apply the second-order multiplexing DHT, and the method used by Arasu-Dillon-Player is to use the character sum factorization approach, which is much more general and powerful. They not only proved the validity of Lin conjecture and Ludkovski-Gong conjectures, but also showed that the Dillon-Dobbertin construction for binary 2-level autocorrelation sequences and the Helleseth-Gong/Dillon construction for p-ary 2-level autocorrelation sequences can be represented by their character sum factorizations. This is extremely remarkable!

In fact, the character sum factorization approach is tightly related to the second-order DHT approach. The triple exponents involved in the character sum factorization in Arasu-Dillon-Player's work for the Dillon-Dobbertin construction correspond to the realization pair in the second-order DHT. We observe that one of the triple exponents in the character

Table 1 Ludkovski-Gong conjectured sequences realized from Lin conjecture

Form	Realizable pairs (v, t)
A	$v = \frac{3^n-1}{2}, t = \begin{cases} v+u & if n \equiv 1 \pmod 4 \\ u & if n \equiv 3 \pmod 4 \end{cases}, u = \frac{3^m-1}{2}$
D	$(v = 1, t_k), t_k = 3^m\left(\frac{3^{k+1}-1}{2}\right) - \frac{3^k-1}{2}, \gcd(m-k, n) = 1^*$

sum factorization for each of Lin conjecture, Ludkovski-Gong conjectures, and Helleseth-Gong and Dillon construction is not coprime with the period $L = p^n - 1$.

So we can show that all those three constructions can be realized from m-sequences by applying the second-order multiplexing DHT. This means that all known p-ary 2-level autocorrelation sequences are Hadamard equivalent through the second-order multiplexing DHT! For binary cases, all the known constructions through finite fields are Hadamard equivalent through the second-order DHT (see [19]) or the second-order multiplexing DHT for Dillon-Dobberin's construction for n even. In other words, starting with an m-sequence, using the realizable pairs (multiplexing or not), we can obtain all the known 2-level autocorrelation sequences. This is rather surprising for p-ary ($p > 2$) cases. Those include the secondary constructions as well as Hadamard equivalence of quadratic residue sequences, which are investigated by Yu and Gong [74].

Observation 1 Except for the Hall sextic residue sequences, all the known p-ary (p prime) 2-level autocorrelation sequences can be realized by p-ary m-sequences by applying the second-order DHT or multiplexing DHT.

Remark 7 For $n = 7$, from Section 9.4.4 in [19], the Hall sextic residue sequence is also Hadamard equivalent to the m-sequences. However, there is no proof for the result in general n for period $2^n - 1$ being prime and $n \equiv 3 \bmod 4$. This is an unsolved problem.

In terms of the Hadamard equivalence (multiplexing or not), the above observation and Remark 7 imply that excluding the Hall sextic residue sequences, there is only one class of 2-level autocorrelation sequences, i.e., m-sequences.

3.4 Open problem on linear span of Ludkovski-Gong conjectured sequences by Gong and Helleseth

Nevertheless, all the currently conjectured 2-level autocorrelation sequences have been proved! However, we still have important unsolved problems for Ludkovski-Gong conjectured sequences, i.e., their trace representations (the sum of the monomial trace terms) and linear spans (the linear span of a q-ary sequence of period L is defined as the number of stages of the shortest LFSR which generates the sequence). In 2004, Gong and Helleseth conjectured the linear span of the class D sequences, presented below.

Observation 2 (Gong and Helleseth (2004) [26]) Let $g_k(x)$ be the realization of $f(x) = Tr(x + x^d)$, the 2-term function in Lin conjecture, with realization pair $(1,t_k)$ where $\gcd(m-k,n) = 1$ in Table 1. Then the linear span of $\mathbf{g}_k$, denoted as $LS(\mathbf{g}_k)$, is given by

$$LS(\mathbf{g}_k) = nl_k \tag{7}$$

where l_k is the number of trace terms, determined by the Fibonacci sequence $\{F_k\}$ as follows:

$$\begin{cases} l_1 &= F_{2(m-1)} \\ l_k &= F_{2k}, \quad k = 2, 3, \cdots, m-2 \\ l_{m-1} &= F_{2m} \end{cases}$$

when n prime or $n \not\equiv 0 \bmod 3$, and

$$\begin{cases} l_k &= F_{2k},\ k = 2, 3, \cdots, m-2 \\ l_{m-1} &= F_{2m} \end{cases}$$

where $n \equiv 0 \bmod 3$.

Since $\{F_k\}$ is the Fibonacci sequence, we have the following linear recursive relation:

$$F_{2k} = 3F_{2(k-1)} - F_{2(k-2)}, k = 2, 3, \cdots, m. \tag{8}$$

In other words, the number of trace terms of the sequence $\mathbf{g}_k, k = 2,3,\cdots,m-1$ are linearly recursively related by (8).

3.5 The exhaustive search approach

The exhaustive search for binary 2-level autocorrelation sequences have been done for $L = 2^n - 1$ for $n \leq 10$. So the next case will be $n = 11$. For $n = 11$, there are 187 coset leaders modulo $L = 2^{11} - 1 = 2047$. Hence the exhaustive searching space is given by $2^{187} - 187 \times 186/2 - 187$, which is beyond current computing power. A succeeding case after that is $n = 12$. Since $\mathbb{F}_{2^{12}}$ has subfields and several subgroups of the multiplicative group determined by the factors of $2^{12} - 1$, by applying Baumert's tricks (see [4, Section III], for example [4, Lemma 3.8] on page 63), it may result in a smaller search complexity than the case for $n = 11$. We encourage anyone who is interested to attempt that.

The other direction would be for conducting partial searches for 2-level autocorrelation sequences. For example, a partial search for $10 < n < 20$ has been done for Hadamard equivalent classes by applying the second-order DHT of Definition 8 and reported in [24] for $n \leq 17$ and for $n = 18,19$ succeedingly done, but not including the cases by applying the second-order multiplexing DHT of Definition 10. Nevertheless, this partial search confirmed that all known 2-level autocorrelation sequences can be classified for $10 < n < 20$ under the Hadamard equivalence.

4 Sequences with low ambiguity

In this section, we present a summary for the currently best-known designs for sequence sets with low ambiguity and large sizes. For two sequences, if one cannot be obtained by applying both the time shift operator and phase shift operator, then they are said to be *time-phase shift distinct*, a definition introduced by Ding et al. [14], otherwise, the time-phase shift equivalent.

For example, let S consist of the following five quaternary sequences of period 4:

$$\begin{aligned} \mathbf{f}_0 &= (1, 2, 0, 3) \\ \mathbf{f}_1 &= (0, 3, 1, 2) \\ \mathbf{f}_2 &= (1, 3, 2, 2) \\ \mathbf{f}_3 &= (1, 0, 0, 1) \\ \mathbf{f}_4 &= (0, 0, 3, 1). \end{aligned}$$

By observation, since $q = L = 4$, we have $\mathbf{f}_1$ is a time-shift of $\mathbf{f}_0$ at shift $\tau = 2$, $\mathbf{f}_2$ is a phase-shift of $\mathbf{f}_0$ with $k = 1$, and $\mathbf{f}_3$ is a phase-shift of $\mathbf{f}_0$ with $k = 2$, and $\mathbf{f}_4$ is a time-shift at $\tau = 2$ and phase-shift at $k = 1$ from $\mathbf{f}_0$, i.e., at $(\tau,k) = (2,1)$ from $\mathbf{f}_0$, i.e.,

$$\begin{aligned}\mathbf{f}_1 &= \{f_0(t+2)\}_{t=0}^{3}\\ \mathbf{f}_2 &= \mathbf{f}_0 + (0,1,2,3) = (1,2,0,3) + (0,1,2,3)\\ \mathbf{f}_3 &= \mathbf{f}_0 + (0,2,0,2) = (1,2,0,3) + (0,2,0,2)\\ \mathbf{f}_4 &= \{f_0(t+2)\}_{t=0}^{3} + (0,1,2,3) = (0,3,1,2) + (0,1,2,3).\end{aligned}$$

Thus, by the time-phase shift relation, S has only one sequence $\mathbf{f}_0$, and the others are time-phase shift equivalent to $\mathbf{f}_0$. (Note that in general, we cannot do the computation like the examples shown above when $q \neq L$, since the phase-shift of $\mathbf{f}$ is given by $\left\{\omega_q^{f(t)}\omega_L^{kt}\right\}$.)

We now assume that $S = \{\mathbf{s}_0,\cdots,\mathbf{s}_{N-1}\}$ is a set consisting of N complex sequences of period L, which are time-phase shift distinct. We use the following notations for different bounds.

– $G_{\max}$: the maximum magnitude of the auto ambiguity function of S, defined by

$$G_{\max} = \max_{0\le j<N, 0\le\tau,k<L}\{|A_{\mathbf{s}_j}(\tau,k)|\}.$$

– $A_{\max}$: the maximum magnitude of the cross ambiguity function $A_{\mathbf{s}_k,\mathbf{s}_j}(\tau,k)$, i.e.,

$$A_{\max} = \max_{0\le k,j<N, 0\le\tau,k<L}|A_{\mathbf{s}_k,\mathbf{s}_j}(\tau,k)|, (\tau,k)\neq(0,0)\ \textit{if}\ k = j.$$

We may extend S to T by including all time-shift distinct sequences from S and define

– $R_{\max}$, the maximum out-of-phase autocorrelation of the sequences in T, i.e.,

$$R_{\max} = \max_{\mathbf{s}\in T, 0\le\tau<L}|C_{\mathbf{s}}(\tau)|.$$

– $C_{\max}$: the maximum magnitude of cross correlation of any two sequences in T, i.e.,

$$C_{\max} = \max_{\mathbf{s}_k,\mathbf{s}_j\in T, 0\le\tau<L}|C_{\mathbf{s}_k,\mathbf{s}_j}(\tau)|, \tau\neq 0\ \textit{if}\ k = j.$$

Ding et al. [14] have detailed discussions on how to get a time-shift distinct sequence set from a time-phase shift distinct sequence set with the following property.

Property 1 Let $S = \{\mathbf{s}_0,\cdots,\mathbf{s}_{N-1}\}$ be a time-phase shift distinct sequence set. Then $T = \left\{\left\{\omega_L^{kt}\cdot s_j(t)\right\}_{0\le t<L} : 0\le k,j<N,\right\}$ is a time-shift distinct sequence set. Moreover, we have

$$S\subseteq T, \text{with } |T| = L\cdot|S|, R_{\max} = G_{\max}, \text{and } C_{\max} = A_{\max}.$$

In this section, the four classes of the sequence sets that we will introduce have their $R_{\max}$ and $A_{\max}$ bounded by directly applying the Weil bounds with only one exception. Now we will present the Weil bounds on character sums first.

4.1 The Weil bounds and W. Li bound

Restate that $Q = p^n$.

Definition 12 For each $j = 0,1,\cdots,p-1$, we define an additive character of $\mathbb{F}_Q$ as the function ψ_j, given by

$$\psi_j(x) = e^{2\pi ijTr(x)/p} = \omega_p^{jTr(x)}, x \in \mathbb{F}_Q.$$

We also denote it as $\psi(x)$ when $j = 1$. Let $M|(Q-1)$. For each $j = 0,1,\cdots,M-1$, a multiplicative character χ_j of order $M/\gcd(j,M)$ is defined by

$$\chi_j(\alpha^k) = e^{2\pi ijk/M} = \omega_M^{jk}, \alpha^k \in \mathbb{F}_Q^*$$

or equivalently

$$\chi_j(x) = \omega_M^{(j\log_\alpha x) \bmod M}, x \in \mathbb{F}_Q^*.$$

The original definition in the Weil bounds is for $\chi_j(0) = 0$ and we modify it as $\chi_j(0) = 1$ for consistence with sequence design.

Let $f(x)$ and $g(x)$ be polynomials over $\mathbb{F}_Q[x]$ where f has degree d with $\gcd(d, Q) = 1$. Assume that s and e are the numbers of distinct roots of $g(x)$ in the algebraic closure of $\mathbb{F}_Q$ and $\mathbb{F}_Q$ respectively. We assume that both f and g are nontrivial with respect to the additive character and multiplicative character respectively.

Fact 1 (The Weil bound (Weil 48, Delegne 74)) With the above notation, the following inequalities hold.

$$\begin{aligned}
&\text{The additive character sum:} \left|\sum_{x\in\mathbb{F}_Q} \psi(f(x))\right| \le (d-1)\sqrt{Q}.\\
&\text{The multiplicative character sum:} \left|\sum_{x\in\mathbb{F}_Q} \chi(g(x))\right| \leqslant (s-1)\sqrt{Q}+e.\\
&\text{The hybrid character sum:} \left|\sum_{x\in\mathbb{F}_Q} \chi(g(x))\psi(f(x))\right| \leqslant (d+s-1)\sqrt{Q}+e.
\end{aligned}$$

We also have the following bound for the exponential sum involved the function in Kloosterman's sum, which is given by W. Li.

Fact 2 (W. Li [40] (1995)) For any $1 \le j < Q-1$, $a, b \in \mathbb{F}_Q$,

$$\left|\sum_{x\in\mathbb{F}_Q^*} \chi_j(x)\psi\left(ax+bx^{-1}\right)\right| \le 2\sqrt{Q}.$$

4.2 Autocorrelation of power residue sequences and Sidel'nikov sequences

From the discussions on 2-level autocorrelation sequences in Section 3, it implies that for those sequences, there exist some polynomials of $\mathbb{F}_{p^n}$, say $f(x)$ such that the sum of additive character $\psi(f(\lambda x) - f(x))$ is equal to zero for every $\lambda \in \mathbb{F}_Q (Q = p^n)$ with $\lambda \neq 1$, i.e.,

$$\sum_{x\in\mathbb{F}_Q}\psi(f(\lambda x)-f(x))=0,\lambda\in\mathbb{F}_Q,\lambda\neq 1.$$

However $f(x)$ may have a high degree except for m-sequences given by $f(x)=x$. So, the Weil bound cannot be used in those cases. Two natural questions which we would like to ask: whether there are sequences constructed from multiplicative characters over $\mathbb{F}_{p^n}$ (including $n=1$), which are analogue to: Case 1) m-sequences; Case 2) 2-level autocorrelation sequences where $f(x)$ has a high degree. We can confirm that there exist some solutions to the first question, but it is unknown whether there is a solution to the second question. In fact, for Case 1), there are two constructions for $f(x)$ has degree 1: one is for $\mathbb{F}_p$, called power residue sequences and the other is for $\mathbb{F}_{p^n}, n>1$, Sidel'nikov sequences, which have optimal or low autocorrelation, which will be introduced as follows.

Definition 13 With the notation in Section 4.1, we define the following two sequences:

$\mathbb{F}_p$	$\mathbb{F}_Q, Q=p^n$
$\chi_j(f(t))=\omega_M^{ju(t)}$	$\chi_j(g(t))=\omega_M^{jv(t)}$
$u(t)=\log_\alpha f(t) \bmod M$	$v(t)=\log_\alpha g(\alpha^t) \bmod M$
$0\le t<p, M\|p-1$	$0\le t<Q-1, M\|Q-1$
$f(x)=x$, *a power residue sequence*	$g(x)=x+1$, *a Sidel'nikov sequence*

Note that the elements of a power residue sequence are ordered in the additive group of $\mathbb{F}_p$, while the elements of a Sidel'nikov sequence are ordered in the multiplicative group of $\mathbb{F}_Q$.

Theorem 1 (Sidel'nikov [58], Lempel et al. [39], Sarwate [54]) The autocorrelation function of a power residue sequence is bounded by

$$|C_{\mathbf{u}}(\tau)|\le 3,\tau\not\equiv 0 \bmod p.$$

In particular, for $M=2$,

$$C_{\mathbf{u}}(\tau)\in\begin{cases}\{-1\} & \tau\not\equiv 0 \bmod p \text{ if } p\equiv 3 \bmod 4\\ & (\textit{which gives quadratic residue sequences}\\ & \textit{with } 2-\textit{level autocorrelation})\\ \{1,-3\} & \tau\not\equiv 0 \bmod p \text{ if } p\equiv 1 \bmod 4.\end{cases}$$

And the autocorrelation function of a Sidel'nikov sequence is bounded by

$$|C_{\mathbf{v}}(\tau)|\le 4,\tau\not\equiv 0 \bmod (Q-1).$$

In particular, for $M=2$,

$$C_{\mathbf{v}}(\tau)\in\begin{cases}\{-2,2\} & \tau\not\equiv 0 \bmod (Q-1) \text{ if } Q\equiv 3 \bmod 4\\ \{0,-4\} & \tau\not\equiv 0 \bmod (Q-1) \text{ if } Q\equiv 1 \bmod 4.\end{cases}$$

Remark 8 The autocorrelation of the power residue sequences is optimal from Remark 2. Note that the ambiguity, crosscorrelation, and DFT of power residue sequences and Sidel'nikov sequences are also known. The reader is referring to [38] and [37] for

crosscorrelation, and [23, Theorems 4.8 and 4.12] for the summary of the other properties of those sequence sets.

4.3 Best known constructions for sequence sets

As we have introduced the history of the Weil representation sequences in Section 1.3, in the following, we directly list the bounds on ambiguity and correlation given by Schmidt. Note that "best" means that those constructions produce "best known" sequence sets with both low ambiguity and correlation as well as large sizes. Those results can be obtained by applying the Weil bounds.

Construction 1 (Weil Representation Sequence Sets, Wang and Gong (2011) [68] and Schmidt (2011) [57]). Let α be a primitive element of finite field $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ and $\mathbb{F}_p^* = \{1, 2, \cdots, p-1\}$. Recall $\omega_k = e^{\frac{i2\pi}{k}}$, k a positive integer. Let $\mathbf{s}_{(x,y,z)}$ with the elements given by

$$\begin{aligned} s_{(x,y,z)}(t) &= \omega_{p-1}^{x\cdot\log_\alpha t}\omega_p^{yt^2+zt}, \\ &0 \le t < p, 1 \le x < p-1, 0 \le y, z < p. \end{aligned} \tag{9}$$

Let

$$\begin{aligned} S_1 &= \{\mathbf{s}_{(x,y,0)} | 1 \le x < p-1, 0 \le y < p\}, \\ T_1 &= \{\mathbf{s}_{(x,y,z)} | 1 \le x < p-1, 0 \le y, z < p\}. \end{aligned} \tag{10}$$

We then have

- The sequence set S_1 contains $(p-2)p$ time-phase shift distinct sequences, and its extension, T_1 contains $(p-2)p^2$ time-shift distinct sequences.
- Each of those sequences has length p and the alphabetic set has size $(p-1)p$.
- The correlation, ambiguity and DFT are bounded by

$$\boxed{\begin{array}{l} R_{\max} = G_{\max} \le 2\sqrt{p} + 2, \\ C_{\max} = A_{\max} \le 3\sqrt{p} + 2, \text{ and} \\ |\hat{\mathbf{s}}(k)| \le 2\sqrt{p} + 1, \ \forall\ 0 \le k < p, \forall \mathbf{s} \in T_1. \end{array}} \tag{11}$$

Remark 9 If we only consider correlation, then the number of time-shift distinct sequences in T_1 is approximately a cubic function of the length p.

Construction 2 (Wang-Gong-Yu (2013 [70])) With the notation above, let $M|p-1$ and

$$s_{(x,y,z)}(t) = \omega_M^{x\cdot\log_\alpha t}\omega_p^{yt^2+zt}, 0 \le t < p, 1 \le x < M, 0 \le y, z < p. \tag{12}$$

We define S_2 by varying (x,y) in (12) and setting $z = 0$ and T_2 by varying all (x,y,z). Then we have the following results.

- There are $(M-1)p$ time-phase shift distinct sequences in S_2 and $(M-1)p^2$ time-shift distinct sequences in T_2.
- Each sequence has length p and the alphabetic set with size Mp.
- The bounds are given by (11).

Note that Construction 1 is the case of Construction 2 for $M = p-1$.

Construction 3 (Wang-Gong-Yu (2013), Gong (2012) [23]). For $1 \le x < M, 1 \le y < L$ where $L = p^n - 1$, α a primitive element of $\mathbb{F}_{p^n}$ with $h(\alpha) = 0$ where $h(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, $c_i \in \mathbb{F}_p$, a primitive polynomial of degree n over $\mathbb{F}_p$, M, a factor of L. The elements of $\mathbf{s}_{(x,y)}$ are defined as follows.

$$\boxed{\begin{array}{l} v(t) = \log_\alpha(\alpha^t + 1), \\ u(t+n) = \sum_{i=0}^{n-1} c_i u(t+i), t \ge 0, \\ \text{where } (u(0), \cdots, u(n-1)) \text{ is an initial state} \\ s_{(x,y)}(t) = \omega_M^{x v(t) \bmod M} \omega_p^{u(t+y)}, 0 \le t < L. \end{array}} \tag{13}$$

We define S_3 a set consisting of the sequences $\mathbf{s}_{(x,y)}$ by varying all (x,y). Then

- There are $(M-1)L$ time-phase shift distinct sequences in S_3.
- Each sequence has length L and the alphabetic set with size Mp.
- The bounds on correlation, ambiguity function and DFT given by (11) where p is replaced by $Q = p^n$.

Note that $\mathbf{u}$ is a p-ary m-sequence of period L, i.e., an m-sequence over a finite field $\mathbb{F}_p$ of degree n, with $u(t) = Tr(\beta\alpha^t), \beta \in \mathbb{F}_{p^n}$, the trace representation of $\mathbf{u}$. Furthermore, $v(t) = \log_\alpha(\alpha^t + 1) \bmod M$ is an M-ary Sidel'nikov sequence (Sidel'nikov 1969) of period $L = p^n - 1$. So this design yields a sequence which is the term-wise product of a modulated p-ary m-sequence and a modulated M-ary Sidel'nikov sequence.

All three constructions have the same bounds on the autocorrelation and auto ambiguity function, crosscorrelation, cross ambiguity function and DFT.

We have the following construction, which is given by Ding et al. [14] using Fact 2.

Construction 4 (W. Li (1995) [40] and Ding et al. (2013) [14]) Let

$$s_a(t) = \omega_p^{Tr(a\alpha^t + \alpha^{-t})}, a \in \mathbb{F}_Q$$

and $S_4 = \{\mathbf{s}_a, \mathbf{s}_{-1} | a \in \mathbb{F}_Q\}$ where $\mathbf{s}_{-1} = \{Tr(\alpha^t)\}$. Then S_4 has $Q+1$ time-phase shift distinct sequences, and correlation, ambiguity, and DFT are bounded by $2\sqrt{Q}$, i.e.,

$$G_{\max}, A_{\max}, |\hat{\mathbf{s}}_a(k)| \le 2\sqrt{Q}.$$

Remark 10 Note the sequence $\mathbf{s}_{-1}$ is not included in the construction given in [14]. But the bound will not be changed by adding this sequence according to Fact 2.

The choices for Constructions 2 and 3 lie in the trade-off for getting a small alphabetic size at the cost of the decreasing the size of the sequence set, which are listed in Table 2. Construction 4 gives a sequence set with the smallest alphabetic size p for period $p^n - 1$. However, the sizes of the sequence set from each of the other three constructions can be in

the order of the square of the size of Construction 4 at the price of increasing alphabetic sizes (Tables 3 and 4).

In the following, we show some examples from Construction 3, which have more efficient hardware implementation. We call the table with entries $(t,v(t))$ a *trinomial table* if $v(t)$ is computed as follows

$$\alpha^t + 1 = \alpha^{v(t)}, 0 \le t < p^n - 1.$$

In other words, $v(t) = \log_\alpha(\alpha^t + 1)$.

Example 7 Both the following two cases produce 6-ary sequences from Construction 3.

Case 1. For $q = 2^4 - 1 = 15$ and 3 is a divisor of 15: let α be a primitive element in $\mathbb{F}_{2^4}$ with $\alpha^4 + \alpha + 1 = 0$. The sequences $\{v(t)\}$ and $\{u(t)\}$ are defined as follows.

By varying (x,y) in the range of $0 < x < 3, 0 \le y < 15$, S_3 has 30 time-phase shift distinct 6-ary sequences of period 15.

Case 2. For $q = 3^3 - 1$, let α be a primitive element of $\mathbb{F}_{3^3}$ with $\alpha^3 + 2\alpha^2 + 1 = 0$. The sequences $\{v(t)\}$ and $\{u(t)\}$ are defined as follows.

Hence this produces a sequence set of the 6-ary sequences of period 26 with 27 time-phase shift distinct sequences.

Example 8 For $Q = 2^8$, we give an example for Construction 3. The trinomial table for $n = 8$ is a list of the $v(t)$ values such that

$$\alpha^t + 1 = \alpha^{v(t)}, t = 0, 1, \cdots, 254$$

which is given in Table 5. Let α be a primitive element in $GF(2^8)$ with $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$. Then $\{u(t)\}$ is given by

$$u(t) = Tr(\gamma\alpha^t), \gamma \in \mathbb{F}_{2^8}$$

or equivalently,

$$\begin{aligned} u(t+8) &= u(t+4) + u(t+3) + u(t+2) + u(t), t = 0, 1, \cdots, \\ &(u(0), \cdots, u(7)) = (0, 0, 0, 0, 0, 1, 0, 0, 0). \end{aligned}$$

Let S_3 be the set consisting of the following sequences for all (x,y):

$$s_{(x,y)}(t) = \omega_{255}^{xv(t)} \times (-1)^{u(t+y)}, 0 < x < 255, 0 \le y < 255.$$

We now construct two sequences to illustrate their correlation and ambiguity.

$$\begin{aligned} s_0(t) &= \omega_{255}^{v(t)} \times (-1)^{u(t)}, \qquad (x,y) = (1,0) \\ s_1(t) &= \omega_{255}^{v(t)} \times (-1)^{u(t+1)}, \quad (x,y) = (1,1) \end{aligned}$$

where $\{u(t)\}$ and $\{v(t)\}$ are given in Tables 4 and 5 respectively. The properties of S_3 is presented in Table 3. For comparisons, we also list the properties of the sequence set from Construction 4. Construction 3 produces 64770 time-phase shift distinct sequences, i.e., the product sequences of Sidel'nikov sequences with 254 phases and binary m-sequences. Construction 4 only contains 257 time-phase shift distinct sequences, but has a smaller maximal ambiguity value than that from Construction 3.

Note that if there are enough resources in memory, then the trinomial table can be stored. In this case, the implementation cost is similar as the case for Construction 4.

Table 2 Good parameters for sequence sets with low ambiguity and DFT

Constructions	Parameter M	$\|S\|$	Period	Alphabet size	HW cost
1: $L=p$	$p-1$	$(p-1)p$	p	$(p-1)p$	high
2: $L=p$	$M\|p-1$	Mp	p	Mp	high
3: $L=p^n-1$	$L-1$	$(L-1)L$	L	$p(L-1)$	moderate
4: $L=p^n-1$		$L+2$	L	p	low
3: $L=2^n-1$	$L-1$	$(L-1)L$	L	$2(L-1)$	moderate
3: $L=2^n-1$, $3\|L$	3	$2L$	L	6	moderate, with the smallest alphabet size
3: $L=3^n-1$	$L-1$	$(L-1)L$	L	$3(L-1)$	moderate
3: $L=3^n-1$	2	L	L	6	moderate, with the smallest alphabet size

The sketches of auto/crosscorrelation and ambiguity functions of $\mathbf{s}_0$ and $\mathbf{s}_1$ are given in Figs. 3, 4 and 5.

5 Aperiodic complementary sequences and arrays

In this section, we revisit a recent method to construct CSSs and CCCs by PU matrices and corresponding constructions [71]. We extend the size of generalized PU matrices from 2^n to p^n where p is an arbitrary integer in this survey. Moreover, we adopt the approach from [69] and show a sketch of the proof on extracting the function from a generalized seed PU matrix, which greatly simplifies the proof process in [71].

5.1 A viewpoint from arrays and PU matrices

A q-ary sequence $\boldsymbol{f}=(f(0),f(1),\cdots,f(L-1))$ can be associated with its *generating function* given by

$$F(Z)=\sum_{t=0}^{L-1}\omega_q^{f(t)}Z^t. \tag{14}$$

It is helpful to view the CSS and CCC by the generating functions of the sequences. The complex conjugate of $F(Z)$ is denoted by $\overline{F}(Z)=\sum_{t=0}^{L-1}\omega^{-f(t)}Z^t$.

Suppose that $F_0(Z)$ and $F_1(Z)$ are the generating functions of q-ary sequences $\boldsymbol{f}_0$ and $\boldsymbol{f}_1$, respectively. The polynomial $F_0(Z)\overline{F}_1(Z^{-1})$ records all the aperiodic values:

Table 3 The sequence sets of $\mathbb{F}_{2^8}$

	Number of time-phase shift distinct sequences	Period	Correlation, Ambiguity, DFT	Alphabet size	HW cost
Construction 3	$254 \times 255 = 64770$	255	$G_{\max}, DFT \le 33, A_{\max} \le 50$	510	moderate
Construction 4	257	255	all metrics ≤ 32	2	low

Table 4 m-sequence $\{u(t)\}_{t=0}^{254}$

0 0 0 0 0 1 0 0 0 1 1 1 0 0 0 1 0
0 1 0 1 1 1 0 0 0 0 0 0 1 1 0 0 1
0 0 1 0 0 1 1 0 1 1 1 0 0 1 0 0 0
0 0 1 0 1 0 1 1 0 1 1 0 1 0 1 1 0
0 1 0 1 1 0 0 0 0 1 1 1 1 1 0 1 1
0 1 1 1 1 0 1 0 1 1 1 0 1 0 0 0 1
0 0 0 0 1 1 0 1 1 0 0 0 1 1 1 1 0
0 1 1 1 0 0 1 1 0 0 0 1 0 1 1 0 1
0 0 1 0 0 0 1 0 1 0 0 1 0 1 0 1 0
0 1 1 1 0 1 1 1 0 1 1 0 0 1 1 1 1
0 1 1 1 1 1 1 1 0 1 0 0 1 1 0 0 1 1
0 1 0 1 0 0 0 1 1 0 0 0 0 0 0 1 1 1
0 1 0 1 0 1 0 1 1 1 1 1 1 0 0 1 0 1
0 0 0 0 1 0 0 1 1 1 1 1 1 1 1 1 0 0
0 0 1 0 1 1 1 1 0 0 0 1 1 0 1 0 0

$$F_0(Z)\overline{F}_1(Z^{-1}) = \sum_{\tau=1-L}^{L-1} C_{f_0,f_1}(\tau)Z^{\tau}. \tag{15}$$

Then $S = \{\boldsymbol{f}_0,\boldsymbol{f}_1,\cdots,\boldsymbol{f}_{N-1}\}$ forms a CSS if and only if their generating functions $\{F_0(Z),F_1(Z),\cdots,F_{N-1}(Z)\}$ satisfy

$$\sum_{j=0}^{N-1} F_j(Z)\overline{F}_j(Z^{-1}) = NL. \tag{16}$$

Moreover, two CSSs $S_0 = \{\boldsymbol{f}_{0,0},\boldsymbol{f}_{0,1},\cdots,\boldsymbol{f}_{0,N-1}\}$ and $S_1 = \{\boldsymbol{f}_{1,0},\boldsymbol{f}_{1,1},\cdots,\boldsymbol{f}_{1,N-1}\}$ are *mutually orthogonal* if and only if their respective generating functions

$$\{F_{i,0}(Z), F_{i,1}(Z), \cdots, F_{i,N-1}(Z)\}, i = 0, 1$$

satisfy

$$\sum_{j=0}^{N-1} F_{0,j}(Z)\overline{F}_{1,j}(Z^{-1}) = 0. \tag{17}$$

Complementary arrays An m-dimensional q-ary array of size $L_0 \times L_1 \times \cdots \times L_{m-1}$ can be represented by a function mapping from $\mathbb{Z}_{L_0} \oplus \mathbb{Z}_{L_1} \oplus \cdots \oplus \mathbb{Z}_{L_{m-1}}$ to $\mathbb{Z}_q$: $f(\boldsymbol{x}) = f(x_0,x_1,\cdots,x_{m-1})$ for $x_j \in \mathbb{Z}_{L_j}$. The *(multivariate) generating function* of array $f(\boldsymbol{x})$ is defined by

Table 5 The sequence $\{v(t)\}_{t=0}^{254}$ where $\alpha^t + 1 = \alpha^{v(t)}$

0	25	50	223	100	138	191	112	200	120
21	245	127	99	224	33	145	68	240	92
42	10	235	196	254	1	198	104	193	181
66	45	35	15	136	32	225	179	184	106
84	157	20	121	215	31	137	101	253	197
2	238	141	147	208	63	131	83	107	82
132	186	90	55	70	162	30	216	17	130
64	109	195	236	103	199	113	228	212	174
168	160	59	57	40	170	242	167	175	203
62	209	19	158	202	176	251	190	139	13
4	47	221	74	27	248	39	58	161	71
126	246	7	76	166	243	214	122	164	153
9	43	117	183	180	194	110	12	140	239
69	56	60	250	177	144	34	46	5	98
128	52	218	150	135	16	217	53	206	188
143	178	226	119	201	159	169	41	93	155
81	108	65	182	118	227	114	87	80	156
85	211	229	232	79	88	95	134	151	37
124	29	163	123	38	249	61	204	149	219
97	6	247	28	125	72	23	49	26	75
8	154	94	89	187	207	148	205	54	91
241	171	78	233	116	44	67	146	142	189
252	102	237	3	14	36	152	165	77	172
231	230	173	213	244	22	73	222	51	129
18	210	86	115	234	11	111	192	105	185
133	96	220	48	24					

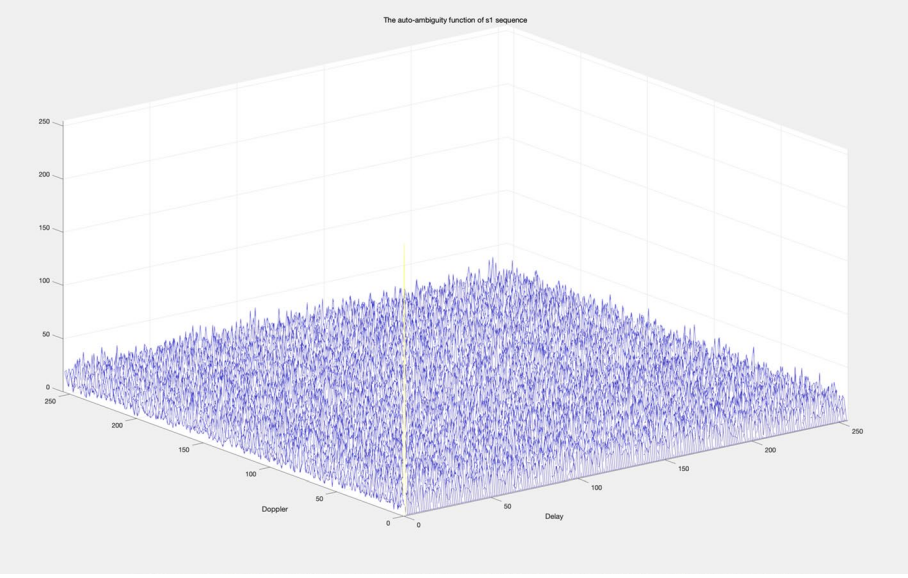


Fig. 3 Auto ambiguity function of sequence $\mathbf{s}_0$

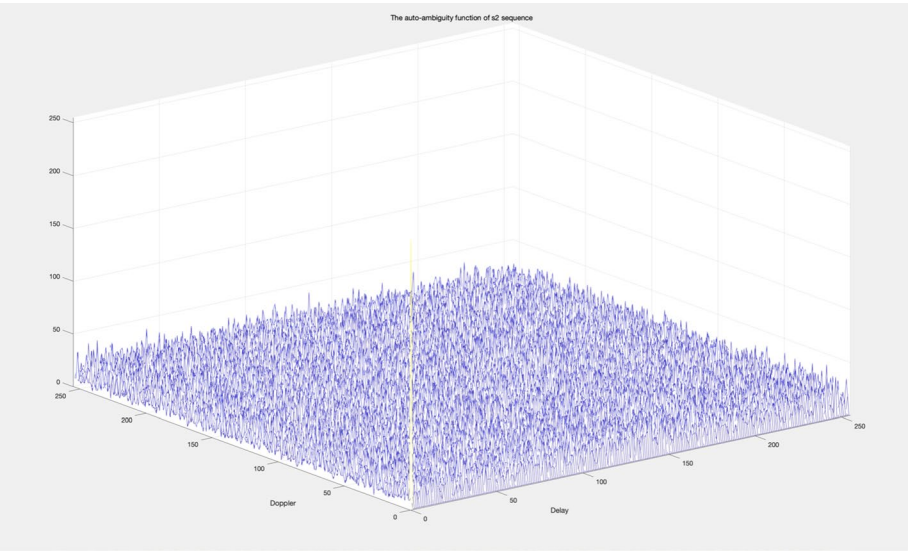


Fig. 4 Auto ambiguity function of sequence $\mathbf{s}_1$

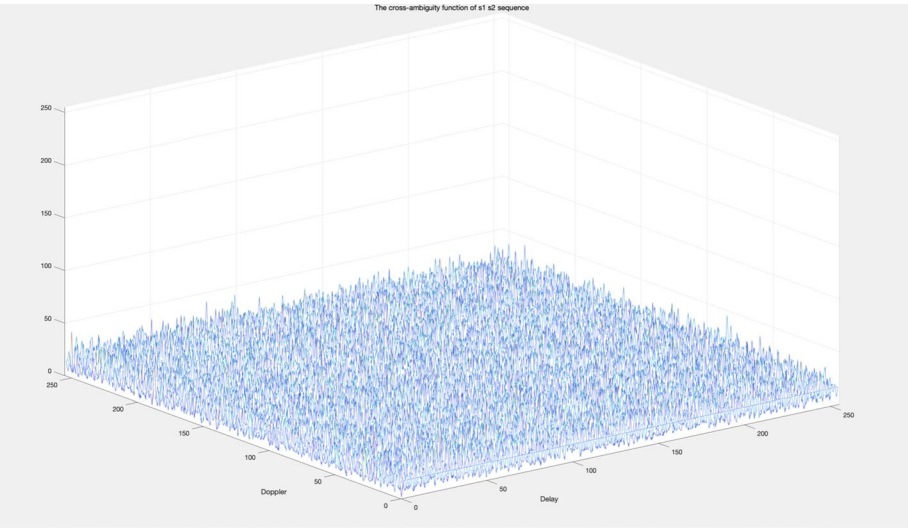


Fig. 5 Cross ambiguity function of the sequences $\mathbf{s}_0$ and $\mathbf{s}_1$

$$F(z) = \sum_{x_0=0}^{L_0-1} \sum_{x_1=0}^{L_1-1} \cdots \sum_{x_{m-1}=0}^{L_{m-1}-1} \omega^{f(\boldsymbol{x})} z_0^{x_0} z_1^{x_1} \cdots z_{m-1}^{x_{m-1}} \tag{18}$$

for $\boldsymbol{z} = (z_0, z_1, \cdots, z_{m-1})$. Denote $\boldsymbol{z}^{-1} = (z_0^{-1}, z_1^{-1}, \cdots, z_{m-1}^{-1})$.

The concept of a Golay complementary pair was generalized to that of a *Golay array pair* (GAP) in [43], and the concepts of CSSs and CCCs were generalized from sequences to arrays in [49].

Definition 14 A set of arrays $\{f_0(\boldsymbol{x}),f_1(\boldsymbol{x}),\cdots,f_{N-1}(\boldsymbol{x})\}$ is called a *complementary array set* (CAS) of size N if their generating functions $\{F_0(z),F_1(z),\cdots,F_{N-1}(z)\}$ satisfy

$$\sum_{u=0}^{N-1} F_u(z)\cdot\overline{F}_u(z^{-1}) = N\cdot p^m. \tag{19}$$

Two CASs

$$\begin{aligned} S_0 &= \{f_{0,0}(\boldsymbol{x}),f_{0,1}(\boldsymbol{x}),\cdots,f_{0,N-1}(\boldsymbol{x})\}\\ S_1 &= \{f_{1,0}(\boldsymbol{y}),f_{1,1}(\boldsymbol{y}),\cdots,f_{1,N-1}(\boldsymbol{y})\}\end{aligned}$$

are said to be *mutually orthogonal* if their generating functions $\{F_{u,0}(z),F_{u,1}(z),\cdots,F_{u,N-1}(z)\}$ $(u=0,1)$ satisfy

$$\sum_{v=0}^{N-1} F_{0,v}(z)\overline{F}_{1,v}(z^{-1}) = 0. \tag{20}$$

Definition 15 Let $S_u=\{f_{u,0}(\boldsymbol{x}),f_{u,1}(\boldsymbol{x}),\cdots,f_{u,N-1}(\boldsymbol{x})\}$ $(0\le u<N)$ be CASs of size N, which are pairwise mutually orthogonal. We call such a collection of S_u $(0\le u<N)$ a *complete mutually orthogonal array set* or a *complete complementary arrays* (CCA).

From arrays to sequences For an array $f(\boldsymbol{x}):\mathbb{Z}_p^m\to\mathbb{Z}_q$, we can specify a sequence $\boldsymbol{f}:\mathbb{Z}_{p^m}\to\mathbb{Z}_q$ of length $L=p^m$ by listing the values of $f(\boldsymbol{x})$ in lexicographic order of $\boldsymbol{x}$:

$$f(t)=f(\boldsymbol{x}) \text{ for } t=\sum_{k=0}^{m-1} x_k\cdot p^k, 0\le x_k<p.$$

We say that the sequence $\boldsymbol{f}$ is evaluated by the array $f(\boldsymbol{x})$.

For an array $f(\boldsymbol{x}):\mathbb{Z}_p^m\to\mathbb{Z}_q$ and its evaluated sequence $\boldsymbol{f}:\mathbb{Z}_{p^m}\to\mathbb{Z}_q$, their generating functions satisfy $F(z)=F(Z)$, if we set $z_k=Z^{p^k}$. The relationship between sequence and array is summarized in Fig. 6.

Example 9 For an array from $\mathbb{Z}_2^2$ to $\mathbb{Z}_4$: $f(x_0,x_1)=2x_0x_1+x_0$, its generating function is given by $F(z_0,z_1)=1+iz_0+z_1-iz_0z_1$. Sequence $\boldsymbol{f}$, evaluated by the array $f(x_0,x_1)$, is obtained by setting $t=x_0+2x_1$: $\boldsymbol{f}=\{0,1,0,3\}$, which is equal to $\mathbf{f}_{0,0}$ given in Example 4 in Section 2.2. Then the generating function of sequence $\boldsymbol{f}$ is given by $F(Z)=1+iZ+Z^2-iZ^3$.

An action of permutation π on the function $f(\boldsymbol{x})$ from $\mathbb{Z}_p^m$ to $\mathbb{Z}_q$ is to permute the variables, i.e.,

$$\pi\cdot f(\boldsymbol{x})=f(\pi\cdot\boldsymbol{x})=f\left(x_{\pi(0)},x_{\pi(1)},\cdots,x_{\pi(m-1)}\right).$$

Fact 3 Let π be any permutation.

- If a set of arrays $\{f_0, f_1, \cdots, f_{N-1}\}$ is a CAS, then the sequences evaluated by functions $\{\pi \cdot f_0, \pi \cdot f_1, \cdots, \pi \cdot f_{N-1}\}$ form a CSS.
- If $S_i = \{f_{i,0}, f_{i,1}, \cdots, f_{i,N-1}\}$ $(0 \le i < N)$ is a CCA, the sequences evaluated by functions $S_i' = \{\pi \cdot f_{i,0}, \pi \cdot f_{i,1}, \cdots, \pi \cdot f_{i,N-1}\}$ $(0 \le i < N)$ form a CCC.

According to Fact 3, a larger number of CSSs and CCCs can be constructed from a single CCA by mapping arrays to sequences. For simplicity, we shall only show the construction of CCAs in this survey.

Remark 11 Note that the results in this subsection can be generalized to arrays of more flexible size $L_0 \times L_1 \times \cdots \times L_{m-1}$ straightforwardly. Moreover, a larger number of lower dimensional CASs and CCAs can also be constructed from a high dimensional CCA.

PU matrices For $0 \le u, v \le N-1$, let $f_{u,v}(\boldsymbol{x})$ be q-ary arrays of dimension m, and $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ a matrix with entry $f_{u,v}(\boldsymbol{x})$, i.e.,

$$\widetilde{\boldsymbol{M}}(\boldsymbol{x}) = \begin{bmatrix} f_{0,0}(\boldsymbol{x}) & f_{0,1}(\boldsymbol{x}) & \cdots & f_{0,N-1}(\boldsymbol{x}) \\ f_{1,0}(\boldsymbol{x}) & f_{1,1}(\boldsymbol{x}) & \cdots & f_{1,N-1}(\boldsymbol{x}) \\ \vdots & \vdots & \ddots & \vdots \\ f_{N-1,0}(\boldsymbol{x}) & f_{N-1,1}(\boldsymbol{x}) & \cdots & f_{N-1,N-1}(\boldsymbol{x}) \end{bmatrix}. \tag{21}$$

The generating functions of the entries in matrix $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ can be presented by a matrix $\boldsymbol{M}(\boldsymbol{z})$ with each entry given by $M_{u,v}(\boldsymbol{z}) = F_{u,v}(\boldsymbol{z})$, the generating function of $f_{u,v}(\boldsymbol{x})$, i.e.,

$$\boldsymbol{M}(\boldsymbol{z}) = \begin{bmatrix} F_{0,0}(\boldsymbol{z}) & F_{0,1}(\boldsymbol{z}) & \cdots & F_{0,N-1}(\boldsymbol{z}) \\ F_{1,0}(\boldsymbol{z}) & F_{1,1}(\boldsymbol{z}) & \cdots & F_{1,N-1}(\boldsymbol{z}) \\ \vdots & \vdots & \ddots & \vdots \\ F_{N-1,0}(\boldsymbol{z}) & F_{N-1,1}(\boldsymbol{z}) & \cdots & F_{N-1,N-1}(\boldsymbol{z}) \end{bmatrix}. \tag{22}$$

$\boldsymbol{M}(\boldsymbol{z})$, given by (22) is called the *generating matrix* of $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$, given by (21).

Definition 16 Let $\boldsymbol{M}(\boldsymbol{z})$ be a square multivariate polynomial matrix of order N. If

$$\boldsymbol{M}(\boldsymbol{z}) \cdot \boldsymbol{M}^{\dagger}(\boldsymbol{z}^{-1}) = c \cdot \boldsymbol{I}_N,$$

where $(\cdot)^{\ddagger}$ denotes the Hermitian transpose, $\boldsymbol{I}_N$ is the identity matrix of order N, and c is a real constant. We say that $\boldsymbol{M}(\boldsymbol{z})$ is a *para-unitary (PU) matrix*.

According to (19) and (20), it is necessary that $\boldsymbol{M}(\boldsymbol{z})$ is a PU matrix if $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ forms a CCA. However, the PU condition is not sufficient since the entries of a PU matrix may not be able to map to polyphase arrays. A PU matrix $\boldsymbol{M}(\boldsymbol{z})$ is called a *desired PU matrix* if it is

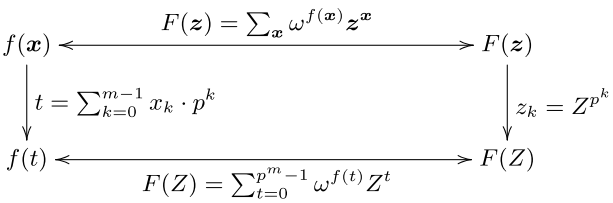


Fig. 6 Relationships between arrays, sequences, and their generating functions

the generating matrix of a function matrix $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$, i.e., each entry is a function from $\mathbb{Z}_p^m$ to $\mathbb{Z}_q$. Then the process to construct CCA can be divided into two steps:

(1) Construct a desired PU matrix $\boldsymbol{M}(\boldsymbol{z})$.
(2) Find the function matrix $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ from its generating matrix $\boldsymbol{M}(\boldsymbol{z})$.

Example 10 It is easy to verify $\boldsymbol{M}(z_0, z_1) \cdot \boldsymbol{M}^{\dagger}(z_0^{-1}, z_1^{-1}) = 8 \cdot \boldsymbol{I}_2$, where

$$\boldsymbol{M}(z_0, z_1) = \begin{bmatrix} 1 + iz_0 + z_1 - iz_0z_1 & 1 + iz_0 - z_1 + iz_0z_1 \\ 1 - iz_0 + z_1 + iz_0z_1 & 1 - iz_0 - z_1 - iz_0z_1 \end{bmatrix}.$$

Then $\boldsymbol{M}(z_0,z_1)$ is a desired PU matrix. We can extract its function matrix

$$\widetilde{\boldsymbol{M}}(x_0, x_1) = \begin{bmatrix} 2x_0x_1 + x_0 & 2x_0x_1 + x_0 + 2x_1 \\ 2x_0x_1 + 3x_0 & 2x_0x_1 + 3x_0 + 2x_1 \end{bmatrix},$$

which forms a CCA. Then the sequences evaluated by the arrays in $\widetilde{\boldsymbol{M}}(x_0, x_1)$, presented by

$$S = \begin{bmatrix} \boldsymbol{f}_{0,0} = (0, 1, 0, 3)\ \boldsymbol{f}_{0,1} = (0, 1, 2, 1) \\ \boldsymbol{f}_{1,0} = (0, 3, 0, 1)\ \boldsymbol{f}_{1,1} = (0, 3, 2, 3) \end{bmatrix},$$

is a CCC, which is the quaternary CCC, given in Example 4 in Section 2.2. Moreover, we can construct many CCCs from the CCA $\widetilde{\boldsymbol{M}}(x_0, x_1)$ according to Fact 3.

5.2 Construction I: ingredients and basic recursive formula

Ingredients of desired PU matrices and function matrices We first introduce two ingredients of PU matrices. One is Butson-type Hadamard matrices, which will be defined below, the simplest desired PU matrices, and the other is delay matrices.

A complex matrix $\boldsymbol{H}$ of order N is called a *Butson-type* Hadamard (BH) matrix [8] if $\boldsymbol{H} \cdot \boldsymbol{H}^{\dagger} = N \cdot \boldsymbol{I}_N$ and all the entries of $\boldsymbol{H}$ are q th roots of unity.

For example, if $N = q$, DFT matrix $\boldsymbol{H}$ with entry $H_{u,v} = \omega^{uv}$ is a BH matrix; if $N = 2^n$ and $q = 2$, *Walsh Hadamard Transform* (WHT) matrix $\boldsymbol{H}$ with entry $H_{u,v} = \omega^{Tr(uv)}$ for $u, v \in \mathbb{F}_{2^n}$ is also a BH matrix.

For given N and q, the set of all BH matrices is denoted by $H(q,N)$. BH matrices are the simplest desired PU matrices. Another type of desired PU matrices of dimension 1 and order 2 can be constructed from the so-called non-standard Golay pairs, introduced in [16, 41].

Now we introduce our second ingredient, i.e., delay matrices.

Definition 17 A *delay matrix* $\boldsymbol{D}_N(z)$ of order N is defined by

$$\boldsymbol{D}_N(z) = diag\left\{z^0, z^1, \cdots, z^{N-1}\right\}. \tag{23}$$

If $N = p^n$, the delay matrix can be presented as a multi-variate polynomial with multi-variables $\boldsymbol{z} = (z_0,z_1,\cdots,z_{n-1})$, obtained by the Kronecker tensor product:

$$\boldsymbol{D}_N(z) = \boldsymbol{D}_p(z_{n-1}) \otimes \cdots \otimes \boldsymbol{D}_p(z_1) \otimes \boldsymbol{D}_p(z_0). \tag{24}$$

This is called a *generalized delay matrix*.

It is straightforward to show that the generalized delay matrix $\boldsymbol{D}_N(z)$ can be explicitly expressed by a diagonal matrix

$$\boldsymbol{D}_N(z) = diag\{\phi_0(z), \phi_1(z), \cdots, \phi_{p^n-1}(z)\},$$

where $(x_0,x_1\cdots,x_{n-1})$ is p-ary expansion of y and $\phi_y(z) = \prod_{j=0}^{n-1} z_j^{x_j}$.

For example, if $N=4$, the delay matrix is given by

$$\boldsymbol{D}_4(z) = diag\left\{z^0, z^1, z^2, z^3\right\},$$

while the generalized delay matrix is represented by

$$\boldsymbol{D}_4(z_0, z_1) = diag\left\{z_1^0 z_0^0, z_1^0 z_0^1, z_1^1 z_0^0, z_1^1 z_0^1\right\} = diag\left\{1, z_0^1, z_1^1, z_1^1 z_0^1\right\}.$$

Next we introduce two ingredients for functions, which will be used to extract functions from the desired PU matrices. One is the phase matrix of a BH matrix, and the other is the Kronecker-delta function.

For a BH matrix $\boldsymbol{H} \in H(q,N)$, define its phase matrix $\widetilde{\boldsymbol{H}}$ by $\widetilde{H}_{u,v} = h(u,v)$ if $H_{u,v} = \omega^{h(u,v)}$, where $h(u,v)$ is a function from $\mathbb{Z}_N^2$ to $\mathbb{Z}_q$ for $u, v \in \mathbb{Z}_N$. Actually, a BH matrix $\boldsymbol{H}$ can be treated as a desired PU matrix, and its phase matrix $\widetilde{\boldsymbol{H}}$ is the corresponding function matrix.

In this survey, we adopt the approach from [69] where a phase matrix of a BH matrix is replaced by the function $h(u,v)$ from $\mathbb{Z}_N^2$ to $\mathbb{Z}_q$ to simplify the proof process. For example, $h(u,v) = u \cdot v$ represents the phase matrix of the DFT matrix of order N for $u, v \in \mathbb{Z}_N$, while $h(u,v) = Tr(u \cdot v)$ is the phase matrix of the WHT matrix of order $N=2^n$ for $u, v \in \mathbb{F}_{2^n}$.

Definition 18 Let δ_u be a Kronecker-delta function from $\mathbb{Z}_N$ to $\mathbb{Z}_q$ given by

$$\delta_u(y) = \begin{cases} 1, \text{if } y = u, \\ 0, \text{if } y \neq u. \end{cases} \tag{25}$$

Moreover, if $N = p^n$, we have

$$\delta_u(y) = \prod_{j=0}^{n-1} \delta_{u_j}(x_j),$$

where $\boldsymbol{x} = (x_0,x_1,\cdots,x_{n-1})$ and $(u_0,u_1,\cdots,u_{n-1})$ are p-ary expansions of y and u respectively, and δ_{u_j} is a Kronecker-delta function from $\mathbb{Z}_p$ to $\mathbb{Z}_q$ defined by (25). In this case, we use function $\delta_u(\boldsymbol{x})$ instead of $\delta_u(y)$ from now on.

Note that the set consisting of all the Kronecker-delta functions, i.e., $\{\delta_u | u \in \mathbb{Z}_N\}$ forms a linear basis of all functions from $\mathbb{Z}_N$ to $\mathbb{Z}_q$. So, we also call it a *Kronecker-delta (function) basis*.

Example 11 For $N = q = 3$, the Kronecker-delta functions from $\mathbb{Z}_3$ (or $\mathbb{F}_3$) to $\mathbb{Z}_3$ are given by

$$\begin{cases} \delta_0(y) &= 2y^2+1, \\ \delta_1(y) &= 2y^2+2y, \\ \delta_2(y) &= 2y^2+y. \end{cases}$$

The monomial basis of all functions from $\mathbb{Z}_3$ to $\mathbb{Z}_3$ is $\{1,y,y^2\}$, while the set of these Kronecker-delta functions is another basis.

Example 12 For $N=4$, the Kronecker-delta functions from $\mathbb{Z}_4$ (or $\mathbb{F}_2^2$) to $\mathbb{Z}_q$ are given by

$$\begin{cases} \delta_0(y) = (1-x_0)(1-x_1), \\ \delta_1(y) = x_0(1-x_1), \\ \delta_2(y) = (1-x_0)x_1, \\ \delta_3(y) = x_0x_1, \end{cases}$$

where (x_1,x_0) is the binary expansion of y. The monomial basis of all generalized Boolean functions from $\mathbb{Z}_4$ to $\mathbb{Z}_q$ is $\{1,x_0,x_1,x_0x_1\}$, while the set of the Kronecker-delta functions is another basis.

Definition 19 The $\boldsymbol{\Delta}$-matrix of order N is a diagonal matrix defined by

$$\boldsymbol{\Delta}_N(y) = diag\{\delta_0(y), \delta_1(y), \cdots, \delta_{N-1}(y)\}.$$

If $N=p^n$, $\delta_u(y)$ can be replaced by the function $\delta_u(\boldsymbol{x})$, where $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$ which is the p-ary expansions of y. Then we use the matrix $\boldsymbol{\Delta}_N(\boldsymbol{x})$ instead of $\boldsymbol{\Delta}_N(y)$.

Example 13 According to Example 12, the $\boldsymbol{\Delta}$-matrix of order 4 can be represented by

$$\boldsymbol{\Delta}_4(x_0,x_1) = \begin{bmatrix} (1-x_0)(1-x_1) & 0 & 0 & 0 \\ 0 & x_0(1-x_1) & 0 & 0 \\ 0 & 0 & (1-x_0)x_1 & 0 \\ 0 & 0 & 0 & x_0x_1 \end{bmatrix}.$$

In the rest of the paper, if the context is clear, we use $\boldsymbol{D}(z),\boldsymbol{\Delta}(\boldsymbol{x}),\boldsymbol{I}$ and $\boldsymbol{J}$ instead of $\boldsymbol{D}_N(z),\boldsymbol{\Delta}_N(\boldsymbol{x}),\boldsymbol{I}_N$ and $\boldsymbol{J}_N$, respectively, where $\boldsymbol{I}_N$ and $\boldsymbol{J}_N$ represent the identity matrix and all 1 matrix of order N, respectively.

A basic recursive formula for desired PU matrices Let $\boldsymbol{A}(z_1)$ and $\boldsymbol{B}(z_2)$ be the generating matrices of the function matrices $\widetilde{\boldsymbol{A}}(\boldsymbol{x}_1)=\{a_{i,j}(\boldsymbol{x}_1)\}$ and $\widetilde{\boldsymbol{B}}(\boldsymbol{x}_2)=\{b_{i,j}(\boldsymbol{x}_2)\}$ of order $N=p^n$ respectively, where $a_{i,j}(\boldsymbol{x}_1)$ and $b_{i,j}(\boldsymbol{x}_2)$ are functions from $\mathbb{Z}_p^{m_1}$ to $\mathbb{Z}_q$ and $\mathbb{Z}_p^{m_2}$ to $\mathbb{Z}_q$ respectively. Note that $\boldsymbol{A}(z_1)$ and $\boldsymbol{B}(z_2)$ are not required to be PU matrices here.

A recursive formula for constructing desired PU matrices from lower dimensions to higher dimensions was shown in [71, Lemma 9]. We extend it to the form given by the following theorem.

Theorem 2 Let $\boldsymbol{C}(z_0,z_1,z_2)$ be a multivariate polynomial matrix defined by

$$\boldsymbol{C}(z_0,z_1,z_2) = \boldsymbol{A}(z_1)\cdot\boldsymbol{D}(z_0)\cdot\boldsymbol{B}(z_2),$$

where $\boldsymbol{z_0}=(z_0,z_1,\ldots,z_{n-1})$. Then $\boldsymbol{C}(z_0,z_1,z_2)$ is the generating matrix of the function matrix $\widetilde{\boldsymbol{C}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2)$ given by

$$\widetilde{\boldsymbol{C}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2)=\widetilde{\boldsymbol{A}}(\boldsymbol{x}_1)\cdot\boldsymbol{\Delta}(\boldsymbol{x}_0)\cdot\boldsymbol{J}+\boldsymbol{J}\cdot\boldsymbol{\Delta}(\boldsymbol{x}_0)\cdot\widetilde{\boldsymbol{B}}(\boldsymbol{x}_2), \tag{26}$$

where $\boldsymbol{x_0}=(x_0,x_1,\ldots,x_{n-1})\in\mathbb{Z}_2^n$.

Moreover, if both $\boldsymbol{A}(z_1)$ and $\boldsymbol{B}(z_2)$ are desired PU matrices, then $\boldsymbol{C}(z_0,z_1,z_2)$ is also a desired PU matrix.

Proof For the case $p=2$, it has been shown in [71, Lemma 9] that each entry of $\widetilde{\boldsymbol{C}}(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2)$ can be presented by

$$c_{u,v}(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2)=\sum_{i=0}^{N-1}\big(a_{u,i}(\boldsymbol{x}_1)+b_{i,v}(\boldsymbol{x}_2)\big)\delta_i(\boldsymbol{x}_0), \tag{27}$$

for $0\le u,v<N$. It is straightforward to show that this result are valid for arbitrary integer p. In addition, one can verify that formulae (27) and (26) are equivalent, which completes the proof.

□

5.3 Construction II: generalized seed PU matrices and function matrices

In this subsection, we set $N=p^n$, where p is not necessarily a prime.

Generalized seed PU matrices and function matrices By recursively substituting the BH matrices as the desired PU matrices in Theorem 2, we can immediately obtain the following desired PU matrices, which are called generalized seed PU matrices.

Theorem 3 Let $\boldsymbol{H}^{\{k\}}$ be arbitrary BH matrices chosen from $H(q,N=p^n)$ for $0\le k\le m$ and $\boldsymbol{D}(z_k)$ be the generalized delay matrices of order N with $\boldsymbol{z}_k=(z_{kn},z_{kn+1},\cdots,z_{kn+n-1})$ for $0\le k<m$. Then the following multivariate polynomial matrix

$$\boldsymbol{M}(\boldsymbol{z})=\boldsymbol{H}^{\{0\}}\cdot\boldsymbol{D}(\boldsymbol{z}_0)\cdot\boldsymbol{H}^{\{1\}}\cdot\boldsymbol{D}(\boldsymbol{z}_1)\cdots\boldsymbol{H}^{\{m-1\}}\cdot\boldsymbol{D}(\boldsymbol{z}_{m-1})\cdot\boldsymbol{H}^{\{m\}} \tag{28}$$

is a desired PU matrix of order N, where $\boldsymbol{z}=(\boldsymbol{z}_0,\boldsymbol{z}_1,\cdots\boldsymbol{z}_{m-1})$. Moreover, the function matrix of $\boldsymbol{M}(\boldsymbol{z})$ is given by

$$\begin{aligned}\widetilde{\boldsymbol{M}}(\boldsymbol{x})\;=\;&\widetilde{\boldsymbol{H}}^{\{0\}}\cdot\boldsymbol{\Delta}(\boldsymbol{x}_0)\cdot\boldsymbol{J}+\boldsymbol{J}\cdot\boldsymbol{\Delta}(\boldsymbol{x}_{m-1})\cdot\widetilde{\boldsymbol{H}}^{\{m\}}\\&+\textstyle\sum_{k=1}^{m-2}\boldsymbol{J}\cdot\boldsymbol{\Delta}(\boldsymbol{x}_k)\cdot\widetilde{\boldsymbol{H}}^{\{k\}}\cdot\boldsymbol{\Delta}(\boldsymbol{x}_{k+1})\cdot\boldsymbol{J},\end{aligned} \tag{29}$$

where $\boldsymbol{x_k}=(x_{kn},x_{kn+1},\cdots,x_{kn+n-1})\in\mathbb{Z}_p^n$, $\boldsymbol{x}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{m-1})\in\mathbb{Z}_p^{mn}$, and $\widetilde{\boldsymbol{H}}^{\{k\}}$ is the phase matrix of $\boldsymbol{H}^{\{k\}}$.

Proof For the case $p=2$, it has been shown in [71, Theorem 6] that $\boldsymbol{M}(\boldsymbol{z})$ is a desired PU matrix of order $N=2^n$. It is straightforward show that this result is valid for arbitrary integer p.

In addition, formula (29) can be proved by iteratively applying formula (26) in Theorem 2.

□

Although PU matrices $\boldsymbol{M}(z)$ have been constructed in Theorem 3, it is difficult to give a general form of the function matrices $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$, since the BH matrices $\widetilde{\boldsymbol{H}}^{\{k\}}$ can be arbitrarily chosen. To solve this problem, a very complicated method to extract the functions in $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ was shown in [71]. In this paper, we provide a sketch of an alternative proof coming from the view in [69] where each BH matrix $\widetilde{\boldsymbol{H}}^{\{k\}}$ is treated as a function from $\mathbb{Z}_N^2$ to $\mathbb{Z}_q$. In this way, the function matrices $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ can be given by the following corollary.

Corollary 1 Let the phase matrix $\widetilde{\boldsymbol{H}}^{\{k\}}$ be presented by the function $h^{\{k\}}(u,v)$ from $\mathbb{Z}_N^2$ to $\mathbb{Z}_q$ for $0 \le k \le m$, then the phase matrix $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ in Theorem 3 can be alternatively expressed by

$$\widetilde{\boldsymbol{M}}(\boldsymbol{x}) = \sum_{k=1}^{m-2} h^{\{k\}}(\boldsymbol{x}_k, \boldsymbol{x}_{k+1}) \cdot \boldsymbol{J} + \begin{bmatrix} h^{\{0\}}(0,\boldsymbol{x_0}) & 0 & \cdots & 0 \\ 0 & h^{\{0\}}(1,\boldsymbol{x_0}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h^{\{0\}}(N-1,\boldsymbol{x_0}) \end{bmatrix} \cdot \boldsymbol{J} + \boldsymbol{J} \cdot \begin{bmatrix} h^{\{m\}}(\boldsymbol{x_{m-1}},0) & 0 & \cdots & 0 \\ 0 & h^{\{m\}}(\boldsymbol{x_{m-1}},1) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h^{\{m\}}(\boldsymbol{x_{m-1}},N-1) \end{bmatrix}.$$

Proof Let the phase matrix $\widetilde{\boldsymbol{H}}$ be presented by the function $h(u,v)$ from $\mathbb{Z}_N^2$ to $\mathbb{Z}_q$. From the definition of the Kronecker-delta functions, we can easily verify the following equalities:

$$\begin{aligned} \boldsymbol{J} \cdot \boldsymbol{\Delta}(\boldsymbol{x}_k) \cdot \widetilde{\boldsymbol{H}} \cdot \boldsymbol{\Delta}(\boldsymbol{x}_{k+1}) \cdot \boldsymbol{J} &= h^{\{k\}}(\boldsymbol{x}_k, \boldsymbol{x}_{k+1}) \cdot \boldsymbol{J}, \\ \widetilde{\boldsymbol{H}} \cdot \boldsymbol{\Delta}(\boldsymbol{x}_0) \cdot \boldsymbol{J} &= diag\big\{h^{\{0\}}(0,\boldsymbol{x_0}), h(1,\boldsymbol{x_0}), \cdots, h(N-1,\boldsymbol{x_0})\big\} \cdot \boldsymbol{J}, \\ \boldsymbol{J} \cdot \boldsymbol{\Delta}(\boldsymbol{x}_{m-1}) \cdot \widetilde{\boldsymbol{H}} &= \boldsymbol{J} \cdot diag\big\{h(\boldsymbol{x_{m-1}},0), h(\boldsymbol{x_{m-1}},1), \cdots, h(\boldsymbol{x_{m-1}},N-1)\big\}. \end{aligned}$$

Then the proof is completed by formula (29).
□

Example 14 For the case $N = 4 = 2^2$, $q = 4$, and $m = 3$, let $\boldsymbol{H}^{\{0\}}$ and $\boldsymbol{H}^{\{2\}}$ be the DFT matrix of order 4, and $\boldsymbol{H}^{\{1\}}$ and $\boldsymbol{H}^{\{3\}}$ be the WHT matrix of order 4, namely,

$$\boldsymbol{H}^{\{0\}} = \boldsymbol{H}^{\{2\}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \sqrt{-1} & -1 & -\sqrt{-1} \\ 1 & -1 & 1 & -1 \\ 1 & -\sqrt{-1} & -1 & \sqrt{-1} \end{bmatrix}$$

and

$$\boldsymbol{H}^{\{1\}} = \boldsymbol{H}^{\{3\}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Then we have

$$\boldsymbol{M}(z) = \boldsymbol{H}^{\{0\}} \cdot \boldsymbol{D}(z_0) \cdot \boldsymbol{H}^{\{1\}} \cdot \boldsymbol{D}(z_1) \cdot \boldsymbol{H}^{\{2\}} \cdot \boldsymbol{D}(z_2) \cdot \boldsymbol{H}^{\{3\}},$$

which is a desired PU matrix of order 4.

Furthermore, the phase matrix of DFT matrix can be represented by the function $h_0(u,v) = uv$ from $\mathbb{Z}_4$ to $\mathbb{Z}_4$ or alternatively in a multivariate polynomial, i.e., we have

$$h_0((u_0,u_1);(v_0,v_1)) = (2u_0+u_1)(2v_0+v_1) = 2u_0v_1 + 2u_1v_0 + u_1v_1,$$

which is a generalized Boolean function from $\mathbb{Z}_2^4$ to $\mathbb{Z}_4$ where (u_0,u_1) and (v_0,v_1) are the binary expansion of u and v, respectively. The phase matrix of WHT matrix can be represented by the function $h_1(u,v) = 2Tr(uv)$ from $\mathbb{F}_{2^2}$ to $\mathbb{Z}_4$ or alternatively

$$h_1((u_0,u_1);(v_0,v_1)) = 2u_0v_0 + 2u_1v_1,$$

which is a generalized Boolean function from $\mathbb{Z}_2^4$ to $\mathbb{Z}_4$. Thus, these functions are given by $h^{\{0\}} = h^{\{2\}} = h_0$ and $h^{\{1\}} = h^{\{3\}} = h_2$. Thus we obtain the function matrix as follows.

$$\begin{aligned}\widetilde{\boldsymbol{M}}(\boldsymbol{x}) \;=\; & (h_1(\boldsymbol{x}_0,\boldsymbol{x}_1) + h_0(\boldsymbol{x}_1,\boldsymbol{x}_2)) \cdot \boldsymbol{J} + \\ & + \begin{bmatrix} h_0((0,0);\boldsymbol{x_0}) & 0 & 0 & 0 \\ 0 & h_0((1,0);\boldsymbol{x_0}) & 0 & 0 \\ 0 & 0 & h_0((0,1);\boldsymbol{x_0}) & 0 \\ 0 & 0 & 0 & h_0((1,1);\boldsymbol{x_0}) \end{bmatrix} \cdot \boldsymbol{J} \\ & + \begin{bmatrix} h_1(\boldsymbol{x_{m-1}};(0,0)) & 0 & 0 & 0 \\ 0 & h_1(\boldsymbol{x_{m-1}};(1,0)) & 0 & 0 \\ 0 & 0 & h_1(\boldsymbol{x_{m-1}};(0,1)) & 0 \\ 0 & 0 & 0 & h_1(\boldsymbol{x_{m-1}};(1,1)) \end{bmatrix} \cdot \boldsymbol{J}.\end{aligned}$$

A general form of the functions A general form of CCA $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$, extracted from the generalized seed PU matrix with form (28), has been recently obtained in [69, 71]. Below we will give an alternative proof for those results by Corollary 1, which are much simpler than those presented in [71].

Two BH matrices, say $\boldsymbol{H}_1$ and $\boldsymbol{H}$ are called *equivalent*, if there exist diagonal unitary matrices $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ where each diagonal entry is a q th root of unity and permutation matrices $\boldsymbol{P}_1, \boldsymbol{P}_2$ such that $\boldsymbol{H}_1 = \boldsymbol{Q}_1 \cdot \boldsymbol{P}_1 \cdot \boldsymbol{H} \cdot \boldsymbol{P}_2 \cdot \boldsymbol{Q}_2$.

Let $h_1(u,v)$ and $h(u,v)$ be the phase matrices induced by BH matrices $\boldsymbol{H}_1$ and $\boldsymbol{H}$, respectively. From the view in [69], there exist permutation functions $g(\cdot)$ and $g'(\cdot)$ of $\mathbb{Z}_N$, $c_y, d_y \in \mathbb{Z}_N$, such that

$$h_1(u,v) = h(g(u), g'(v)) + \sum_{y=0}^{N-1} c_y \delta_y(u) + \sum_{y=0}^{N-1} d_y \delta_y(v). \tag{30}$$

Moreover, for a given BH matrix $\boldsymbol{H}$, arbitrary permutation functions $g(\cdot), g'(\cdot)$, and $\forall c_y, d_y \in \mathbb{Z}_N$, there exists a BH matrix $\boldsymbol{H}_1$ satisfy the (30).

Recall that the Kronecker-delta functions form a linear basis of all functions from $\mathbb{Z}_N$ to Z_q. Therefore the term $\sum_{y=0}^{N-1} c_y \delta_y(u)$ in formula (30) can produce arbitrary function $l(y)$ from $\mathbb{Z}_N$ to Z_q. Thus the general form of CCAs $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ extracted from generalized seed PU matrix in [71] can be obtained immediately. Before we show it, we introduce the definitions of two types of functions.

Definition 20 Let

$$\delta_L(q, N = p^n) = \left\{ \sum_{k=0}^{m-1} l_k(\boldsymbol{x_k}) \middle| \forall l_k(\boldsymbol{x_k}) : \mathbb{Z}_p^n \to \mathbb{Z}_q \right\}$$

where each function in the set is referred to as a δ-*linear term*, and let

$$\delta_Q(q, N = p^n) = \{h(g(\boldsymbol{x_0}), g'(\boldsymbol{x_1}))|g, g', h\},$$

where $g(\cdot), g'(\cdot)$ are arbitrary permutation functions over $\mathbb{Z}_p^n$ and $h(u,v)$ is any representative of a phase BH matrix with respect to the equivalence relationship. A function in this set is called a δ-*quadratic term*.

Remark 12 The functions in $\delta_L(q,N = p^n)$ and $\delta_Q(q,N = p^n)$ are called δ-linear terms and δ-quadratic terms, respectively, since these functions are linear and quadratic functions with respect to Kronecker-delta functions, respectively.

A general form of any entry of $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$, denoted by $f(\boldsymbol{x})$, can be explicitly represented by a combination of these δ-linear terms and δ-quadratic terms.

Theorem 4 [71, Theorem 3] All the functions extracted from the generalized seed PU matrices with form (28) can be represented in a general form

$$f(\boldsymbol{x}) = \sum_{k=1}^{m-1} h_k(\boldsymbol{x_{k-1}}, \boldsymbol{x_k}) + l(\boldsymbol{x}), \tag{31}$$

where $h_k(\cdot,\cdot) \in \delta_Q(q,p^n)(1 \le k \le m-1)$ and $l(\boldsymbol{x}) \in \delta_L(q,p^n)$.

The set of δ-linear terms is a free $\mathbb{Z}_q$-module. To obtain all the functions with form (31), we only need to calculate those δ-quadratic terms $\sum_{k=1}^{m-1} h_k(\boldsymbol{x_{k-1}}, \boldsymbol{x_k})$, which are the coset representatives with respect to $\delta_L(q,p^n)$. These coset representatives can be associated with a directed and weighted Hamilton path on m vertices, as shown in Fig. 7, which resembles the standard Golay sequences!

Theorem 5 [71, Theorem 5] Let $f(\boldsymbol{x})$ be a function (or array) with the form (31) and $h_0(\cdot,\cdot), h_m(\cdot,\cdot) \in \delta_Q(q,p^n)$. Then the entries of the function matrix of the generalized seed PU matrix with form (28) can be represented by

$$f_{u,v}(\boldsymbol{x}) = f(\boldsymbol{x}) + h_0(\boldsymbol{u}, \boldsymbol{x_0}) + h_m(\boldsymbol{x_{m-1}}, \boldsymbol{v}),\ u, v \in \mathbb{Z}_{p^n},$$

where $\boldsymbol{u}$ and $\boldsymbol{v}$ are the p-ary expansion of u and v respectively.

We will show parameterized constructions of CAS and CCA of sizes 2, 3, 4 [71] by Theorems 4 and 5 as follows.

Constructions of *q*-ary Golay array pairs We set $N = p = 2$ and q even in Theorems 4 and 5. Up to equivalence, there is only one BH matrix of order 2:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

namely, the WHT matrix of order 2, with phase matrix $h(u, v) = \frac{q}{2}uv$ from $\mathbb{Z}_2^2$ to $\mathbb{Z}_q$.

Then the sets of δ-linear terms and δ-quadratic terms can be easily determined by

$$\begin{aligned} \delta_L(q,2) &= \left\{ \sum_{k=0}^{m-1} c_k x_k + c' \middle| c_k, c' \in \mathbb{Z}_q \right\}, \\ \delta_Q(q,2) &= \left\{ \tfrac{q}{2} x_0 x_1 \right\}. \end{aligned}$$

From Theorems 4 and 5, we obtain the function

$$f(\boldsymbol{x}) = \frac{q}{2} \sum_{k=1}^{m-1} x_{k-1}x_k + \sum_{k=0}^{m-1} c_k x_k + c', \text{ for } c_k, c' \in \mathbb{Z}_q, \tag{32}$$

and the corresponding function matrix $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ (or CCA)

$$\widetilde{\boldsymbol{M}}(\boldsymbol{x}) = f(\boldsymbol{x}) \cdot \boldsymbol{J}_2 + \frac{q}{2} \cdot \begin{bmatrix} 0 & x_{m-1} \\ x_0 & x_0 + x_{m-1} \end{bmatrix}.$$

The construction, given above is identical to the construction of the standard Golay sequences given by Davis and Jedwab in their milestone work [12].

Constructions of ternary complementary array triads We set $N = p = q = 3$ in Theorems 4 and 5. Up to equivalence, there exists only one BH matrix of order 3:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 \\ 1 & \omega^2 & \omega^1 \end{bmatrix},$$

where $\omega = \omega_3$. This is the DFT matrix of order 3 with phase matrix $h(u,v) = uv$ from $\mathbb{Z}_3^2$ to $\mathbb{Z}_3$. The sets of δ-linear terms and δ-quadratic terms are determined by

$$\begin{aligned} \delta_L(3,3) &= \left\{ \sum_{k=0}^{m-1} c_{k,2} x_k^2 + \sum_{k=0}^{m-1} c_{k,1} x_k + c' \middle| c_{k,1}, c_{k,2}, c' \in \mathbb{Z}_3 \right\}. \\ \delta_Q(3,3) &= \left\{ x_0 x_1, 2x_0 x_1 \right\}. \end{aligned}$$

From Theorem 4, we obtain the function

$$f(\boldsymbol{x}) = \sum_{k=1}^{m-1} d_k x_{k-1} x_k + \sum_{k=0}^{m-1} c_{k,2} x_k^2 + \sum_{k=0}^{m-1} c_{k,1} x_k + c', \tag{33}$$

for $d_k \in \mathbb{Z}_3^*$ and $c_{k,1}, c_{k,2}, c' \in \mathbb{Z}_3$. Moreover, from Theorem 5, the corresponding function matrix $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ (or CCA) is given by

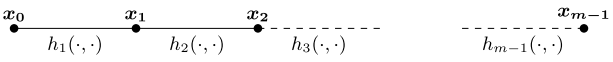


Fig. 7 The graph of coset representatives

$$\widetilde{\boldsymbol{M}}(\boldsymbol{x}) = f \cdot \boldsymbol{J}_3 + \begin{bmatrix} 0 & x_{m-1} & 2x_{m-1} \\ x_0 & x_0 + x_{m-1} & x_0 + 2x_{m-1} \\ 2x_0 & 2x_0 + x_{m-1} & 2x_0 + 2x_{m-1} \end{bmatrix}.$$

This construction was first found in [71] using the methodology of the desired PU matrices.

Constructions of quaternary complementary arrays of size 4 We set $p = n = 2$, $N = q = 4$ in Theorems 4 and 5. The δ-linear terms is determined by

$$\delta_L(4,4) = \left\{ \sum_{k=0}^{m-1} d_k x_{2k} x_{2k+1} + \sum_{k=0}^{2m-1} c_k x_k + c' \middle| \forall d_k, c_k, c' \in \mathbb{Z}_4 \right\}.$$

Up to equivalence, there are only two quaternary BH matrices of order 4, one is the WHT matrix and the other, the DFT matrix of order 4, as shown in Example 14.

The WHT matrix of order 4 determines 6 δ-quadratic terms:

$$h(\boldsymbol{x_0}, \boldsymbol{x_1}) = \begin{cases} 2(x_1x_3 + x_0x_3 + x_1x_2), \\ 2(x_0x_2 + x_0x_3 + x_1x_2), \\ 2(x_1x_3 + x_0x_2), \\ 2(x_0x_3 + x_1x_2), \\ 2(x_0x_2 + x_1x_3 + x_1x_2), \\ 2(x_0x_2 + x_0x_3 + x_1x_3), \end{cases}$$

where $\boldsymbol{x_0} = (x_0, x_1)$ and $\boldsymbol{x_1} = (x_2, x_3)$. And the DFT matrix of order 4 determines 18 δ-quadratic terms:

$$h(\boldsymbol{x_0}, \boldsymbol{x_1}) = dg(\boldsymbol{x_0})g'(\boldsymbol{x_1}) \text{ for } g, g' \in \{g_1, g_2, g_3\}, d = 1, 3,$$

where

$$\begin{cases} g_1(\boldsymbol{x_0}) = x_0 + 2x_1, \\ g_2(\boldsymbol{x_0}) = 2x_0 + x_1, \\ g_3(\boldsymbol{x_0}) = 2x_0x_1 + x_0 + 3x_1. \end{cases}$$

Those 24 δ-quadratic terms form $\delta_Q(4,4)$. From Theorem 4, we obtain the function

$$f(\boldsymbol{x}) = \sum_{k=1}^{m-1} h_k(\boldsymbol{x_{k-1}}, \boldsymbol{x_k}) + l(\boldsymbol{x}),$$

for $h_k(\cdot,\cdot) \in \delta_Q(4,4)$ and $l(\boldsymbol{x}) \in \delta_L(4,4)$.

Moreover, from Theorem 5, the corresponding function matrix is given by

$$\widetilde{\boldsymbol{M}}(\boldsymbol{x}) = f(\boldsymbol{x}) \cdot \boldsymbol{J}_4 + A(\boldsymbol{x_0}) \cdot \boldsymbol{J}_4 + \boldsymbol{J}_4 \cdot B(\boldsymbol{x_{m-1}}),$$

where the diagonal matrices $A(\boldsymbol{x_0})$,$B(\boldsymbol{x_0})$ are arbitrarily chosen from the following set:

$$diag(0, 2x_0, 2x_1, 2x_0 + 2x_1),$$
$$diag(0, 2x_0 + x_1, 2x_1, 2x_0 + 3x_1),$$
$$diag(0, x_0 + 3x_1 + 2x_0x_1, 2x_0 + 2x_1, 3x_0 + x_1 + 2x_0x_1).$$

Since every row (or column) of $\widetilde{\boldsymbol{M}}(\boldsymbol{x})$ forms a CAS, the arrays in the following any set

$$\begin{cases} f(\boldsymbol{x}), \\ f(\boldsymbol{x}) + 2x_0, \\ f(\boldsymbol{x}) + 2x_1, \\ f(\boldsymbol{x}) + 2x_0 + 2x_1, \end{cases} \begin{cases} f(\boldsymbol{x}), \\ f(\boldsymbol{x}) + 2x_0 + x_1, \\ f(\boldsymbol{x}) + 2x_1, \\ f(\boldsymbol{x}) + 2x_0 + 3x_1, \end{cases} \text{or} \begin{cases} f(\boldsymbol{x}), \\ f(\boldsymbol{x}) + 3x_0 + x_1 + 2x_0x_1, \\ f(\boldsymbol{x}) + 2x_0 + 2x_1, \\ f(\boldsymbol{x}) + x_0 + 3x_1 + 2x_0x_1, \end{cases}$$

form a CAS of size 4.

The constructions of complementary arrays of size 4 have been studied for long time along the direction of determining aperiodic correlation of the generalized Boolean functions. Using that method, the recursive formulae for quaternary complementary arrays of size 4 are all generalized from those for binary complementary arrays of size 4. However, for the binary case, there is only one BH matrix, namely, the WHT matrix. In fact, the constructions of the quaternary complementary arrays involving by δ-quadratic terms determined by the DFT matrices have not been reported before the use of the desired PU matrices proposed in [71].

5.4 Other recursive constructions

The recursive construction in Theorem 2 constructs desired PU matrices from lower dimensions to higher dimensions, which can be generalized in the following form.

Theorem 6 Let $\boldsymbol{V}(z_1)$ and $\boldsymbol{U}^{\{\beta\}}(\boldsymbol{z_2})$ $(0 \le \beta < p^{n'})$ be desired PU matrices of order $p^{n+n'}$ and p^n, respectively. Then

$$\boldsymbol{M}(\boldsymbol{z_0}, \boldsymbol{z_1}, \boldsymbol{z_2}) = \boldsymbol{V}(z_1) \cdot \begin{bmatrix} \boldsymbol{D}(z_0) & 0 & \cdots & 0 \\ 0 & \boldsymbol{D}(z_0) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{D}(z_0) \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{U}^{\{0\}}(\boldsymbol{z_2}) & 0 & \cdots & 0 \\ 0 & \boldsymbol{U}^{\{1\}}(\boldsymbol{z_2}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{U}^{\{2^{n'}-1\}}(\boldsymbol{z_2}) \end{bmatrix}$$

is a desired PU matrix. Moreover, the function matrix of $\boldsymbol{M}(\boldsymbol{z_0}, \boldsymbol{z_1}, \boldsymbol{z_2})$ is given by

$$\begin{aligned} \widetilde{\boldsymbol{M}}(\boldsymbol{x_0}, \boldsymbol{x_1}, \boldsymbol{x_2}) = {} & \widetilde{\boldsymbol{V}}(\boldsymbol{x}_1) \cdot \begin{bmatrix} \boldsymbol{\Delta}(\boldsymbol{x}_0) & 0 & \cdots & 0 \\ 0 & \boldsymbol{\Delta}(\boldsymbol{x}_0) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{\Delta}(\boldsymbol{x}_0) \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{J} & 0 & \cdots & 0 \\ 0 & \boldsymbol{J} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{J} \end{bmatrix} \\ & + \boldsymbol{J}_{p^{n+n'}} \cdot \begin{bmatrix} \boldsymbol{\Delta}(\boldsymbol{x}_0) & 0 & \cdots & 0 \\ 0 & \boldsymbol{\Delta}(\boldsymbol{x}_0) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{\Delta}(\boldsymbol{x}_0) \end{bmatrix} \cdot \begin{bmatrix} \widetilde{\boldsymbol{U}}^{\{0\}}(\boldsymbol{x}_2) & 0 & \cdots & 0 \\ 0 & \widetilde{\boldsymbol{U}}^{\{1\}}(\boldsymbol{x}_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \widetilde{\boldsymbol{U}}^{\{2^{n'}-1\}}(\boldsymbol{x}_2) \end{bmatrix} \end{aligned}$$

Proof For the case $p=2$, it has been shown in [71, Theorem 11] that $\boldsymbol{M}(z_0,z_1,z_2)$ is a desired PU matrix. It is straightforward to show that this result is valid for arbitrary integer p.

In addition, It is not difficult to verify that the matrix form of $\widetilde{\boldsymbol{M}}(\boldsymbol{x_0},\boldsymbol{x_1},\boldsymbol{x_2})$ here is equivalent to the function from of entries in $\widetilde{\boldsymbol{M}}(\boldsymbol{x_0},\boldsymbol{x_1},\boldsymbol{x_2})$ in [71, Theorem 11]. □

Furthermore, we can construct desired PU matrices from lower dimensions and smaller orders to higher dimensions and larger orders as follows.

Theorem 7 Let $\boldsymbol{U}^{\{j\}}(z_0)$ $(0\le j<p^n)$ and $\boldsymbol{V}^{\{\alpha\}}(z_1)$ $(0\le\alpha<p^{n'})$ be desired PU matrices of order $p^{n'}$ and p^n, respectively. And suppose that $\boldsymbol{P}$ is a permutation matrix of order $p^{n+n'}$ with each entry $P_{u,v}=1$ if and only if $v\equiv p^{n'}u \pmod{p^{n+n'}-1}$, $\boldsymbol{U}^{\{j\}}(z_0)$ $(0\le j<p^n)$. Then

$$\boldsymbol{G}(z_0,z_1)=\begin{bmatrix}\boldsymbol{V}^{\{0\}}(z_1) & 0 & \cdots & 0\\ 0 & \boldsymbol{V}^{\{1\}}(z_1) & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \boldsymbol{V}^{\{2^{n'}-1\}}(z_1)\end{bmatrix}\boldsymbol{P}\begin{bmatrix}\boldsymbol{U}^{\{0\}}(z_0) & 0 & \cdots & 0\\ 0 & \boldsymbol{U}^{\{1\}}(z_0) & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \boldsymbol{U}^{\{2^{n}-1\}}(z_0)\end{bmatrix}\boldsymbol{P}^T.$$

is a desired PU matrix of order $p^{n+n'}$. Moreover, the function matrix of $\boldsymbol{G}(z_0,z_1)$ is given by

$$\begin{aligned}\boldsymbol{G}(\boldsymbol{x_0},\boldsymbol{x_1})=&\begin{bmatrix}\widetilde{\boldsymbol{V}}^{\{0\}}(\boldsymbol{x_1}) & 0 & \cdots & 0\\ 0 & \widetilde{\boldsymbol{V}}^{\{1\}}(\boldsymbol{x_1}) & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \widetilde{\boldsymbol{V}}^{\{2^{n'}-1\}}(\boldsymbol{x_1})\end{bmatrix}\boldsymbol{P}\begin{bmatrix}\boldsymbol{J} & 0 & \cdots & 0\\ 0 & \boldsymbol{J} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \boldsymbol{J}\end{bmatrix}\boldsymbol{P}^T\\ &+\begin{bmatrix}\boldsymbol{J} & 0 & \cdots & 0\\ 0 & \boldsymbol{J} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \boldsymbol{J}\end{bmatrix}\boldsymbol{P}\begin{bmatrix}\widetilde{\boldsymbol{U}}^{\{0\}}(\boldsymbol{x_0}) & 0 & \cdots & 0\\ 0 & \widetilde{\boldsymbol{U}}^{\{1\}}(\boldsymbol{x_0}) & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \widetilde{\boldsymbol{U}}^{\{2^{n}-1\}}(\boldsymbol{x_0})\end{bmatrix}\boldsymbol{P}^T\end{aligned}$$

Proof For the case $p=2$, it has been shown in [71, Theorem 10] that $\boldsymbol{G}(z_0,z_1)$ is a desired PU matrix. We can extend it to arbitrary integer p straightforwardly. Thus the equivalence of the matrix form $\boldsymbol{G}(\boldsymbol{x_0},\boldsymbol{x_1})$ and the function form of the entries in $\boldsymbol{G}(\boldsymbol{x_0},\boldsymbol{x_1})$ in [71, Theorem 10] follows immediately.

□

It has been shown in [71], the CSSs, constructed in [50, 56], and CCCs, constructed in [52] can be obtained by the above recursive formulae only involving the delay matrices and WHT matrices of order 2. Furthermore, the work in [71] has shown that all the known constructions of CSSs and CCCs [10, 11, 50, 52, 56, 73] (except non-standard Golay pair) can be obtained by these desired PU matrices involving only the delay matrices and WHT matrices of order 2 as well.

5.5 Discussions

Up to equivalence, for the binary case [30], there is a unique Hadamard matrix of orders 1,2,4,8, and 12. There are 5 inequivalent matrices of order 16, 3 of order 20, 60 of order

24, and 487 of order 28. Millions of inequivalent matrices are known for orders 32,36, and 40. And for quaternary case [63], there are 15 inequivalent BH matrices in $H(4,8)$, and 319 inequivalent BH matrices in $H(4,12)$. Combining with the results that inequivalent BH matrices yield inequivalent δ-quadratic terms with respect to the δ-linear terms, this makes it very interesting that the functions derived from desired PU matrices involving higher order ($N > 2$) BH matrices. This may significantly increase the number of the sequences with low PMEPR.

A recent process in [69] showed the CCAs and CASs extracted from the PU matrices with form (28) involving in DFT matrices, WHT matrices, BH matrices constructed from 2-level autocorrelation sequences, and BH matrices constructed from bent functions. This connects the research of CCAs and CASs with other separate objects in the literature, such as 2-level autocorrelation sequences, perfect sequences, bent functions and permutation polynomials over finite fields. From Proposition 2 in Section 2, we know that the value of the periodic correlation at shift τ can be determined by the sum of the aperiodic correlation at shifts τ and $\tau - L$ where L is the sequence length. It is surprising that the CCCs and CSSs defined by aperiodic correlation can be constructed by 2-level autocorrelation sequences or perfect sequences, which are defined by periodic correlation.

From the discussions in [71] and this section, the method to construct CSSs and CCCs by desired PU matrices explains all the known results in this area, except for the sporadic cases and produce tremendously many new constructions as well, which presents a very compelling tool.

If a desired PU matrix cannot be obtained by another desired PU matrix of higher dimension, we call it a *primitive* desired PU matrix. Currently, we only know two types of primitive desired PU matrices: one is of BH matrices and the other is of PU matrices constructed by non-standard Golay complementary pairs. We can easily show that all the known Golay complementary pairs can be constructed by these two types of primitive desired PU matrices and the recursive formula shown in Theorem 2.

It is natural to ask the following questions. Are there any other primitive desired PU matrices of order 2 or any higher order? Are there any other recursive formulae of desired PU matrices for producing new CASs?

6 Concluding remarks and open problems

In this survey, we have presented the current status of 2-level autocorrelation sequences, the sequence sets with low ambiguity and CSSs and CCCs. We have exhibited several unsolved problems or some inspiring remarks throughout the context. In the following, we summarize those problems as follows.

1. Sequences with 2-level autocorrelation:

   (a) Can we classify all sequences with 2-level autocorrelation? Can we confirm that any 2-level autocorrelation sequence is (multiplexing) Hadamard equivalent to an m-sequence? At least, for binary sequences, can we classify for $n = 12$?
   (b) Prove the observation of Gong-Helleseth on the linear span of Ludkovski-Gong conjectured ternary sequences of type D (or with some modification, since the experiments were done only up to $n = 15$).

(c) Find new primary constructions (i.e., not composited constructions) for 2-level autocorrelation sequences.
(d) Determine some 2-level autocorrelation sequences with good aperiodic autocorrelation, say the values of aperiodic autocorrelation are bounded by the square root of the period with some constant multiplier.

2. Sequence sets with low ambiguity:

(a) Construct more time-phase shift distinct sequence sets with the same ambiguity and DFT bounds in Constructions 1-4, but with larger sizes, say the sizes are in the cubic order of the period in Constructions 1-3 and quadratic-order of the period in Construction 4. If we extend the elements of a sequence to complex values, can the sizes of sequence sets be increased greater than cubic order of the period? If so, find constructions.
(b) Can we have the functions associated with additive characters with higher degrees than those in Constructions 1-3, but the bounds on ambiguity and DFT remain unchanged, also with good aperiodic correlation?
(c) Open problems proposed by Gong presented in Sections 7.2 and 7.3 in [23], which are simplified and rephrased as follows according to the definitions in Sections 4.1 and 4.2.

Problem 1. Find sequences constructed from multiplicative characters over $\mathbb{F}_{p^n}$ which have the same autocorrelation as the power residue sequences or Sidel'nikov sequences (i.e., analogue to 2-level autocorrelation sequences), and constructions for sequence sets based on those sequences with good ambiguity and large sizes.

Problem 2. Note that the elements of a sequence in Sections 3 and 4 are ordered in terms of the multiplicative group of $\mathbb{F}_{p^n}$ whenever an additive character or a multiplicative character is used, while the elements of a complementary sequence in Section 5 are ordered in terms of the additive group of $\mathbb{F}_{p^n}$. So the open question would be to find aperiodic autocorrelation of a sequence $\psi(f(t)), t = 0,1,\cdots,p^n-1$ where $\psi(f(\alpha^t))$ gives a 2-level autocorrelation, and reversely, find periodic autocorrelation of a sequence $f(\alpha^t)$ where $f(t)$ gives a complementary sequence. Find the constructions of sequence sets based on those sequences with good ambiguity and large sizes.

3. PU matrices based constructions on CSSs and CCCs:

(a) Find new primitive desired PU matrices.
(b) Explore other recursive formulae for desired PU matrices for producing new CASs.

Appendix A: List of Acronyms

- almost perfect nonlinear (APN)
- authenticated encryption (AE)
- Butson-type Hadamard (BH)

- code-division multiple access (CDMA)
- complementary array set (CAS)
- complementary sequence set (CSS)
- complete complementary arrays (CCA)
- complete complementary codes (CCC)
- complete mutually orthogonal complementary sets (CMOCS)
- decimation-Hadamard transform (DHT)
- discrete Fourier transform (DFT)
- generalized Boolean function (GBF)
- generalized Reed-Muller (GRM)
- Globe Position System (GPS)
- Golay array pair (GAP)
- inverse DFT (IDFT)
- linear feedback shift register (LFSR)
- millimeter-wave (mm-wave)
- multi-input multi-output (MIMO)
- orthogonal frequency division multiplexing (OFDM)
- orthogonal time frequency space (OTFS)
- parameter unitary (PU)
- peak-to-average power ratio (PAPR)
- peak-to-mean envelope power ratio (PMEPR)
- quadrature amplitude modulation (QAM)
- Walsh Hadamard Transform (WHT)
- Welch-Gong (WG)

References

1. Aagaard, M., AlTawy, R., Gong, G., Mandal, K., Rohit, R., Zidaric, N.: WAGE: An authenticated cipher NIST lightweight cryptography standardization project Round 2 Candidate (2019)
2. Altawy, R., Gong, G., Mandal, K., Rohit, R.: Wage: An authenticated encryption with a twist. IACR Trans. Symmetric-key Crypt. Spec. Issue 1 **2020**, 132–159 (2020)
3. Arasu, K.T., Dillon, J.F., Player, K.J.: Character sum factorizations yield sequences with ideal two-level autocorrelation. IEEE Trans. Inf. Theory **61**(6), 3276–3304 (2015)
4. Baumert, L.: Cyclic Difference Sets, vol. 182. Springer-Verlag, New York (1971)
5. Boehmer, A.M.: Binary pulse compression codes. IEEE Trans. Inf. Theory **13**(2), 156–167 (1967)
6. Budišin, S.Z., Spasojević, P.: Filter bank representation of complementary sequence pairs. In: Fiftieth Annual Allerton Conference on Communication, Control, and Computing, pp 716–723, Monticello, IL, USA (2012)
7. Budišin, S.Z., Spasojević, P.: Paraunitary-based Boolean generator for QAM sequences of length 2^K. IEEE Trans. Inf. Theory **64**(8), 5938–5956 (2018)
8. Butson, A.T.: Generalized Hadamard matrices. Proc. Amer. Math. Soc. **13**(6), 894–898 (1962)
9. Carlet, C.: Componentwise APNness, Walsh uniformity of APN functions, and cyclic-additive difference sets. Finite Fields Appl. **53**, 226–253 (2018)
10. Chen, C., Wang, C., Chao, C.: Complementary sets and Reed-Muller codes for peak-to-average power ratio reduction in OFDM. In: Fossorier, M., et al. (eds.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp 317–327. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
11. Chen, C., Wang, C., Chao, C.: Complete complementary codes and generalized reed-muller codes. IEEE Commun. Lett. **12**(11), 849–851 (2008)
12. Davis, J., Jedwab, J.: Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. IEEE Trans. Inf. Theory **45**(7), 2397–2417 (1999)

13. Dillon, J.F., Dobbertin, H.: New cyclic difference sets with singer parameters. Finite Fields Appl. **10**(3), 342–389 (2004)
14. Ding, C., Feng, K., Feng, R., Xiong, M., Zhang, A.: Unit time-phase signal sets: bounds and constructions. Cryptogr. Commun. **5**(3), 209–227 (2013)
15. Ding, C., Helleseth, T., Lam, K.Y.: Several classes of binary sequences with three-level autocorrelation. IEEE Trans. Inf. Theory **45**, 2606–2612 (1999)
16. Fiedler, F., Jedwab, J., Wiebe, A.: A new source of seed pairs for Golay sequences of length 2^m. J. Combin. Theory (Series A) **117**, 589–597 (2010)
17. Golay, M.: Static multisplit spectrometry its application to the panoramic display of infrared spectra. J. Opt. Soc. Am. **117**, 468–472 (1951)
18. Golay, M.: Complementary series. IRE Trans. Inf. Theory **7**(2), 82–87 (1961)
19. Golomb, S., Gong, G.: Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar Applications. Cambridge University Press, Cambridge (2005)
20. Golomb, S.W.: On the classification of Boolean functions. IEEE Trans. Inf. Theory **5**(4), 176–186 (1959)
21. Golomb, S.W.: Shift Register Sequences. Holden-Day, Inc., San Francisco, 1967, 2nd revised edition, Aegean Park Press, Laguna Hills, CA (1981), 3rd revised edition World Scientific (2017)
22. Golomb, S.W.: Mathematics forty years after Sputnik. Am. Sch. **67**(2), 89–100 (1998)
23. Gong, G.: Character sums and polyphase sequence families with low correlation, discrete fourier transform (DFT), and ambiguity. In: A. W., et al. (eds.) Finite Fields, and Their Applications, pp 1–42. De Gruyter, Germany (2013)
24. Gong, G., Golomb, S.: The decimation-hadamard transform of two-level autocorrelation sequences. IEEE Trans. Inf. Theory **48**(4), 853–865 (2002)
25. Gong, G., Golomb, S., Song, H.: A note on low-correlation zone signal sets. IEEE Trans. Inf. Theory **53**(7), 2575–2581 (2007)
26. Gong, G., Helleseth, T.: Linear span of ternary 2-level autocorrelation sequences from the second-order DHT. Unpublished manuscript (2004)
27. Gong, G., Helleseth, T., Kumar, V., Solomon, W.: Golomb – mathematician, engineer, and pioneer. IEEE Trans. Inf. Theory - Spec. Issue Shift-Register Sequences, Codes Cryptogr. Mem. Solomon W. Golomb **64**(4), 2844–2857 (2018)
28. Gurevich, S., Hadani, R., Sochen, N.: The finite harmonic oscillator and its applications to sequences, communication and radar. IEEE Trans. Inf. Theory **54**(9), 4239–4253 (2008)
29. Hadani, R., Rakib, S., Tsatsanis, M., Monk, A., Goldsmith, A.J., Molisch, A.F., Calderbank, R.: Orthogonal time frequency space modulation. In: 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp 1–6 (2017)
30. Hedayat, A.S., Sloane, N.J.A., Stufken, J.: Orthogonal arrays: theory and applications. Springer Science & Business Media, New York (1999)
31. Helleseth, T., Gong, G.: New nonbinary sequences with ideal two-level autocorrelation. IEEE Trans. Inf. Theory **48**(11), 2868–2872 (2002)
32. Helleseth, T., Kumar, P.V.: Sequences with low correlation. In: Handbook of Coding Theory, vol. 2, pp 1765–1853. Elsevier, Amsterdam, The Netherlands (1998)
33. Helleseth, T., Li, C.: Pseudo-noise sequences. In: Cary Huffman, P.S.W., Kim, J.-L. (eds.) Concise Encyclopedia of Coding Theory, chapter 25, pp 613–644. Chapman and Hall/CRC Press, North-Holland, Amsterdam (2021)
34. Howard, S., Calderbank, A., Moran, W.: The finite Heisenberg-Weyl groups in radar and communications. EURASIP J. Appl. Sig. Process., 1–12 (2006)
35. Hu, H., Shao, S., Gong, G., Helleseth, T.: The proof of lin's conjecture via the decimation-hadamard transform. IEEE Trans. Inf. Theory **60**(8), 5054–5064 (2014)
36. Katz, D.J.: Sequences with low correlation. In: Budaghyan, L., Rodríguez-Henríquez, F. (eds.) Arithmetic of Finite Fields, pp 149–172. Springer International Publishing, Cham (2018)
37. Kim, Y., Song, H.: Cross correlation of Sidelnikov sequences and their constant multiples. IEEE Trans. Inf. Theory **53**(3), 1220–1224 (2007)
38. Kim, Y., Song, H., Gong, G., Chung, H.: Crosscorrelation of q-ary power residue sequences of period p. In: IEEE International Symposium on Information Theory 2006, pp 311–315. IEEE (2006)
39. Lempel, A., Cohn, M., Eastman, W.: A class of balanced binary sequences with optimal autocorrelation properties. IEEE Trans. Inf. Theory **23**(1), 38–42 (1977)
40. Li, W.: Number Theory with Applications - Series on University Mathematics, vol. 7. Springer-Verlag, New York (1995)
41. Li, Y., Chu, W.B.: More Golay sequences. IEEE Trans. Inf. Theory **51**(3), 1141–1145 (2005)

42. Ludkovski, M., Gong, G.: New families of ideal 2-level autocorrelation ternary sequences from second order DHT. In: The proceedings of the Second International Workshop in Coding and Cryptography, pp 345–354 (2001)
43. Lüke, H.: Sets of one and higher dimensional codes and complementary codes. IEEE Trans. Aerosp. Electron. Syst. **21**(2), 170–179 (1985)
44. Lüke, H., Schotten, H., Hadinejad-Mahram, H.: Binary and quadriphase sequences with optimal autocorrelation properties: a survey. IEEE Trans. Inf. Theory **49**(12), 3271–3282 (2003)
45. Malling, L., Golomb, S.W.: Radar measurements of the planet venus. Journal Brit.I.R.E., pp. 297–300 (1961)
46. Nawaz, Y., Gong, G.: The WG Stream Cipher. Technical report, eSTREAM, ECRYPT Stream Cipher Project (2005)
47. No, J.: p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation property. IEEE Trans. Inf. Theory **48**(9), 2540–2546 (2002)
48. Park, K., Song, H., Kim, D.S., Golomb, S.W.: Optimal families of perfect polyphase sequences from the array structure of fermat-quotient sequences. IEEE Trans. Inf. Theory **62**(2), 1076–1086 (2016)
49. Parker, M.G., Riera, C.: Generalised complementary arrays. In: Lecture Notes in Computer Science, vol. 7089, pp 41–60 (2011)
50. Paterson, K.: Generalized Reed-Muller codes and power control in OFDM modulation. IEEE Trans. Inf. Theory **46**(1), 104–120 (2000)
51. Paterson, K.: Sequences for OFDM and multi-code CDMA: Two problems in algebraic coding theory. In: Helleseth, T., Kumar, P., Yang, K. (eds.) Sequences and their Applications, pp 46–71. Springer London, London (2002)
52. Rathinakumar, A., Chaturvedi, A.K.: A new framework for constructing mutually orthogonal complementary sets and ZCZ sequences. IEEE Trans. Inf. Theory **52**(8), 3817–3826 (2006)
53. Rößing, C., Tarokh, V.: A construction of OFDM 16-QAM sequences having low peak powers. IEEE Trans. Inf. Theory **47**(7), 2091–2094 (2001)
54. Sarwate, D.: Comments on A class of balanced binary sequences with optimal autocorrelation properties by Lempel et al. IEEE Trans. Inf. Theory **24** (1), 128–129 (1978)
55. Schmidt, K.: On cosets of the generalized first-order Reed-Muller code with low PMEPR. IEEE Trans. Inf. Theory **52**(7), 3220–3232 (2006)
56. Schmidt, K.: Complementary sets, generalized Reed-Muller codes, and power control for OFDM. IEEE Trans. Inf. Theory **53**(2), 808–814 (2007)
57. Schmidt, K.: Sequence families with low correlation derived from multiplicative and additive characters. IEEE Trans. Inf. Theory **57**(4), 2291–2294 (2011)
58. Sidel'nikov, V.: Some k-valued pseudo-random sequences and nearly equidistant codes. Probl. Peredachi Informatii (Problems on Information Transmission) **5**(1), 16–22 (1969)
59. Sivaswamy, R.: Multiphase complementary codes. IEEE Trans. Inf. Theory **24**(5), 546–552 (1978)
60. Song, M.K., Song, H.-Y.: A construction of odd length generators for optimal families of perfect sequences. IEEE Trans. Inf. Theory **64**(4), 2901–2909 (2018)
61. Song, M.K., Song, H.-Y.: New framework for sequences with perfect autocorrelation and optimal crosscorrelation. IEEE Trans. Inf. Theory **67**(11), 7490–7500 (2021)
62. Suehiro, N.: A signal design without co-channel interference for approximately synchronized cdma systems. IEEE J. Sel. Areas Commun. **12**(5), 837–841 (1994)
63. Szöllősi, F.: On quaternary complex hadamard matrices of small orders. Adv. Math. Commun. **5**(2), 309 (2011)
64. Tang, X., Fan, P., Lindner, J.: Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets. IEEE Trans. Inf. Theory **56**, 4038–4045 (2010)
65. Tang, X., Mow, W.: A new systematic construction of zero correlation zone sequences based on interleaved perfect sequences. IEEE Trans. Inf. Theory **54**, 5729–5734 (2008)
66. Tseng, C., Liu, C.: Complementary sets of sequences. IEEE Trans. Inf. Theory **18**(5), 644–652 (1972)
67. Turyn, R.: Ambiguity functions of complementary sequences. IEEE Trans. Inf. Theory **9**(1), 46–47 (1963)
68. Wang, Z., Gong, G.: New sequences design fromWeil representation with low two-dimensional correlation in both time and phase shifts. IEEE Trans. Inf. Theory **57**(7), 4600–4611 (2011)
69. Wang, Z., Gong, G.: Constructions of complementary sequence sets and complete complementary codes by ideal two-level autocorrelation sequences and permutation polynomials. arXiv:2005.05825, submitted to IEEE Transactions on Information Theory, under revision (2020)
70. Wang, Z., Gong, G., Yu, N.Y.: Polyphase sequence families with low correlation from the bounds of character sums. IEEE Trans. Inf. Theory **59**(6), 3990–3998 (2013)

71. Wang, Z., Ma, D., Gong, G., Xue, E.: New construction of complementary sequence (or array) sets and complete complementary codes. IEEE Trans. Inf. Theory **67**(7), 4902–4928 (2021)
72. Wang, Z., Wu, G., Ma, D.: A new method to construct golay complementary set by paraunitary matrices and Hadamard matrices. In: Proc. Sequences and Their Appl., pp 252–263, Chengdu (2016)
73. Wu, G., Zhang, Y., Liu, X.: New complementary sets of length 2^m and size 4. Adv. Math. Commun. **10**(4), 825–845 (2016)
74. Yu, N.Y., Gong, G.: Realizations from decimation hadamard transform for special classes of binary sequences with two-level autocorrelation. In: Coding and Cryptography - Lecture Notes in Computer Science, pp 371–385 (2006)