Chapter 4

PSEUDORANDOM SEQUENCES

Alev Topuzoğlu and Arne Winterhof

1. Introduction

Sequences, which are generated by deterministic algorithms so as to simulate truly random sequences are said to be *pseudorandom* (PR). A pseudorandom sequence in the unit interval $[0, 1)$ is called a sequence of *pseudorandom numbers* (PRNs). In particular, for a prime p we represent the elements of the finite field $\mathbb{F}_p$ of p elements by the set $\{0, 1, ..., p-1\}$, and arrive at a sequence of PRNs, say (y_n), through a sequence (x_n) over $\mathbb{F}_p$ satisfying $y_n = x_n/p$. The sequence (x_n) in this case is usually called a *pseudorandom number generator*.

Our main aim here is to elucidate the motivation for constructing PR sequences with some specific properties that foster their use in *cryptography* and in *quasi-Monte Carlo methods*. Our exposition focuses on some particular measures of "randomness" with respect to which "good" sequences have been constructed recently by the use of geometric methods. Some of these constructions are given in Chapter 2 of this book.

We also illustrate some typical methods that are used in the classical analysis of randomness of PRNs and briefly describe some recent approaches in order to familiarise the reader with basic notions and problems in this area of research. An extensive list of references is provided for the interested reader.

Various quality measures for randomness of PR sequences are in use. One should note here that the hierarchy among them varies according to the type of problem where PR sequences are needed. For example, if one wishes to employ a quasi-Monte Carlo method to approximate π by choosing N pairs $(x_n, x_{n+1}) \in [0, 1)^2$, $n = 0, 1, \ldots, N-1$, of PRNs, counting the number K of

A. Garcia and H. Stichtenoth (eds.), Topics in Geometry, Coding Theory and Cryptography, 135–166.

pairs (x_n, x_{n+1}) in the unit circle and taking $\pi \approx 4K/N$, one should make sure that the PRNs in use are "distributed uniformly" in the unit square. On the other hand "unpredictability" is often the most desirable property for cryptographic applications, as it is described in Chapter 2, Section 3.

This chapter is structured as follows. We start with an outline of some basic facts regarding "linear complexity" and "linear complexity profile", which are potent measures of unpredictability (or, at least of predictability). Results on lower bounds for linear complexity and linear complexity profile for various PR sequences of wide interest are given in Section 2.1. We consider explicit and recursive nonlinear generators, in particular a new class of PR sequences, defined via Dickson polynomials and Rédei functions, and a generalisation of the well known inversive generator. Section 2.1 also deals with Legendre sequences and their variants, and the elliptic curve generators which have attracted considerable attention recently. In Section 2.2, we describe other measures related to linear complexity, with particular emphasis on the lattice test. In Sections 3 and 4 we turn our attention to measures of distribution; in particular we focus on autocorrelation and related concepts for binary sequences in Section 3. This may provide further background for Section 3 of Chapter 2. We conclude with Section 4 where we concentrate on discrepancy as a measure for uniform distribution of PRNs. Some recent results are presented which illustrate the well known relation of discrepancy to exponential sums. The significance of recent geometric constructions of low-discrepancy point sets is described. With the intention of keeping this chapter concise, we present primarily short or elementary proofs which are sufficiently indicative of some standard tools.

In the sequel we shall be concerned with PR sequences over a finite field $\mathbb{F}_q$ of $q = p^r$ elements with a positive integer r and a prime p. Note that a sequence (y_n) of PRNs in the unit interval can be obtained from a sequence (ξ_n) over $\mathbb{F}_q$ by $y_n = (k_r + k_{r-1}p + \ldots + k_1 p^{r-1})/q$ if $\xi_n = k_1\beta_1 + \ldots + k_r\beta_r$ for some fixed ordered basis $\{\beta_1, \ldots, \beta_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. A sequence over $\mathbb{F}_2$ is called a *bit sequence*. We shall restrict ourselves to (purely) periodic sequences, i.e., to those (ξ_n) satisfying $\xi_{n+t} = \xi_n$ for some positive integer t, for all $n \geq 0$.

We should note here that the term "pseudorandom number generator" is commonly used in the literature on pseudorandom sequences. In particular for sequences over $\mathbb{F}_p$ (identified with $\mathbb{Z}_p = \{0, 1, ..., p-1\}$) or the ring $\mathbb{Z}_m$, one refers to *congruential generators*. The "generator" here is sometimes used to mean the "(recurrence) relation" producing the sequence over $\mathbb{F}_p$ (or $\mathbb{Z}_m$), which in return gives rise to a PRN in the unit interval. In this Chapter we generally use the expression PR sequences. However the term congruential generator (or generator) will also appear when referring to some specific sequences over $\mathbb{F}_p$ (or $\mathbb{F}_q$), that are widely known as such.

2. Linear Complexity and Linear Complexity Profile

Linear complexity and linear complexity profile are defined in Chapter 2. We restate their definitions here for the convenience of the reader.

Let us first recall that a sequence $(s_n)_{n\geq 0}$ of elements of a ring R is called a *(homogeneous) linear recurring sequence of order* k if there exist elements $a_0, a_1, \ldots, a_{k-1}$ in R, satisfying the *linear recurrence of order* k *over* R;

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n,\ n = 0, 1, \ldots$$

Now let (s_n) be a sequence over a ring R. One can associate to it a non-decreasing sequence $L(s_n, N)$ of non-negative integers as follows:

The *linear complexity profile* of a sequence (s_n) over the ring R is the sequence $L(s_n, N)$, $N \geq 1$, where its Nth term is defined to be the smallest L such that a linear recurrence of order L over R can generate the first N terms of (s_n).

We use the convention that $L(s_n, N) = 0$ if the first N elements of (s_n) are all zero and $L(s_n, N) = N$ if the first $N - 1$ elements of (s_n) are zero and $s_{N-1} \neq 0$.

The value

$$L(s_n) = \sup_{N\geq 1} L(s_n, N)$$

is called the *linear complexity* of the sequence (s_n). For the linear complexity of any periodic sequence of period t one easily verifies that

$$L(s_n) = L(s_n, 2t) \leq t.$$

Linear complexity and linear complexity profile of a given sequence (as well as the linear recurrence defining it) can be determined by using the well known Berlekamp-Massey algorithm (see e.g. [35]). The algorithm is efficient for sequences with low linear complexity and hence such sequences can easily be predicted. One typical example is the so-called "linear generator"

$$s_{n+1} = as_n + b, \tag{2.1}$$

for $a, b \in \mathbb{F}_p, a \neq 0$, with $L(s_n) \leq 2$. Faster algorithms are known for sequences of particular periods [26, 78, 79]. PR sequences with low linear complexity are shown to be unsuitable also for some applications using quasi-Monte Carlo methods (see [53, 55, 59]).

The expected values of linear complexity and linear complexity profile show that a "random" sequence should have $L(s_n, N)$ to be close to $\min\{N/2, t\}$ for all $N \geq 1$, see Chapter 2.

Two types of problems concerning linear complexity and linear complexity profile are of interest. One would like to construct sequences with high linear

complexity (and possibly with other favourable properties). Chapter 2 illustrates such constructions. One would also like to find lower bounds for widely used PR sequences in order to judge whether it is reasonable to use them for cryptographic purposes. The present section focuses on this problem.

2.1 Lower Bounds for Linear Complexity and Linear Complexity Profile

Explicit Nonlinear Pseudorandom Sequences

It is possible to express linear complexity in connection with various invariants of the PR sequences at hand. The linear complexity profile of a sequence, for instance, can be determined utilising its generating function as described in Chapter 2.

In case of a q-periodic sequence (ξ_n) over $\mathbb{F}_q$, linear complexity is related to the degree of the polynomial $g \in \mathbb{F}_q[X]$ representing the sequence (ξ_n). We recall that the polynomial g can be uniquely determined as follows: Consider a fixed ordered basis $\{\beta_1, \ldots, \beta_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, and for $n = n_1 + n_2 p + \ldots + n_r p^{r-1}$ with $0 \leq n_k < p$, $1 \leq k \leq r$, order the elements of $\mathbb{F}_q$ as

$$\zeta_n = n_1\beta_1 + n_2\beta_2 + \ldots + n_r\beta_r.$$

Then g is the polynomial which satisfies $\deg g \leq q-1$ and

$$\xi_n = g(\zeta_n), \quad 0 \leq n \leq q-1. \tag{2.2}$$

When $\deg g \geq 2$, $q = p$ (and $\beta_1 = 1$) these sequences are called *explicit nonlinear congruential generators* and we have

$$L(\xi_n) = \deg g + 1 \tag{2.3}$$

(for a proof, see Blackburn *et al* [5, Theorem 8]). For a prime power q they are named *explicit nonlinear digital generators*. In general (2.3) is not valid for $r \geq 2$. Meidl and Winterhof [47] showed however that the following inequalities hold:

$$(\deg(g) + 1 + p - q)\frac{q}{p} \leq L(\xi_n) \leq (\deg(g) + 1)\frac{p}{q} + q - p.$$

For lower bounds on the linear complexity profile of (ξ_n) see Meidl and Winterhof [48].

A similar relation is valid for t-periodic sequences over $\mathbb{F}_q$ where t divides $q-1$. For a t-periodic sequence (ω_n) one considers the unique polynomial $f \in \mathbb{F}_q[x]$ of degree at most $t-1$, satisfying

$$\omega_n = f(\gamma^n), \quad n \geq 0,$$

for an element $\gamma \in \mathbb{F}_q$ of order t. In this case, $L(\omega_n)$ is equal to the number of nonzero coefficients of f (see [35]). Lower bounds for the linear complexity profile in some special cases are given by Meidl and Winterhof in [49]. For a general study of sequences with arbitrary periods see Massey and Serconek [42].

The following sequences exhibit a particularly nice behaviour with respect to the linear complexity profile. The *explicit inversive congruential generator* (z_n) was introduced by Eichenauer-Herrmann in [19]. The sequence (z_n) in this case is produced by the relation

$$z_n = (an+b)^{p-2}, \quad n = 0, \ldots, p-1, \quad z_{n+p} = z_n, \ n \geq 0, \tag{2.4}$$

with $a, b \in \mathbb{F}_p$, $a \neq 0$, and $p \geq 5$. It is shown in [48] that

$$L(z_n, N) \geq \begin{cases} (N-1)/3, & 1 \leq N \leq (3p-7)/2, \\ N-p+2, & (3p-5)/2 \leq N \leq 2p-3, \\ p-1, & N \geq 2p-2. \end{cases} \tag{2.5}$$

We provide the proof of a slightly weaker result.

Theorem 2.1. *Let* (z_n) *be as in* (2.4)*, then*

$$L(z_n, N) \geq \min\left\{\frac{N-1}{3}, \frac{p-1}{2}\right\}, \quad N \geq 1.$$

Proof. Suppose (z_n) satisfies a linear recurrence relation of length L,

$$z_{n+L} = c_{L-1}z_{n+L-1} + \ldots + c_0 z_n, \quad 0 \leq n \leq N-L-1, \tag{2.6}$$

with $c_0, \ldots, c_{L-1} \in \mathbb{F}_p$. We may assume $L \leq p-1$. Put

$$C_L(N) = \{n; 0 \leq n \leq \min\{N-L, p\} - 1, a(n+l)+b \neq 0, \ 0 \leq l \leq L\}$$

Note that $\#C_L(N) \geq \min\{p, N-L\} - (L+1)$.

For $n \in C_L(N)$ the recurrence (2.6) is equivalent to

$$(a(n+L)+b)^{-1} = c_{L-1}(a(n+L-1)+b)^{-1} + \ldots + c_0(an+b)^{-1}.$$

Multiplication with

$$\prod_{j=0}^{L}(a(n+j)+b)$$

yields

$$\prod_{j=0}^{L-1}(a(n+j)+b) = \sum_{l=0}^{L-1} c_l \prod_{\substack{j=0 \\ j\neq l}}^{L}(a(n+j)+b)$$

for all $n \in C_L(N)$. Hence the polynomial

$$F(X) = -\prod_{j=0}^{L-1}(a(X+j)+b) + \sum_{l=0}^{L-1} c_l \prod_{\substack{j=0 \\ j\neq l}}^{L}(a(X+j)+b)$$

is of degree at most L and has at least $\min\{p, N-L\} - (L+1)$ zeros. On the other hand

$$F(-a^{-1}b - L) = -a^L \prod_{j=0}^{L-1}(j-L) \neq 0,$$

hence $F(X)$ is not the zero polynomial and we get

$$L \geq \deg(F) \geq \min\{p, N-L\} - (L+1),$$

which implies the desired result. □

Analogues of (2.5) for *digital inversive generators*, i.e., for $r \geq 2$, are also given in [48]. For *t-periodic inversive generators*, where t is a divisor of $q-1$, see [49].

We mention one more explicit nonlinear generator, namely the *quadratic exponential generator*, introduced by Gutierrez *et al* [32]. Given an element $\vartheta \in \mathbb{F}_q^*$ we consider the sequence (q_n) where

$$q_n = \vartheta^{n^2}, \qquad n = 0, 1, \ldots .$$

The lower bound

$$L(q_n, N) \geq \frac{\min\{N, t\}}{2}, \quad N \geq 1,$$

is obtained in [32]. Here t is at least $\tau/2$ where τ is the multiplicative order of ϑ.

Recursive Nonlinear Pseudorandom Sequences

Given a polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \geq 2$, the *nonlinear congruential pseudorandom number generator* (u_n) is defined by the recurrence relation

$$u_{n+1} = f(u_n), \quad n \geq 0, \tag{2.7}$$

with some initial value $u_0 \in \mathbb{F}_p$. Obviously, the sequence (u_n) is eventually periodic with some period $t \leq p$. As usual, we assume it to be purely periodic.

The following lower bound on the linear complexity profile of a nonlinear congruential generator is given in [32].

Theorem 2.2. *Let* (u_n) *be as in* (2.7)*, where* $f(X) \in \mathbb{F}_p[X]$ *is of degree* $d \geq 2$*, then*

$$L(u_n, N) \geq \min\left\{\log_d(N - \lfloor \log_d N \rfloor), \log_d t\right\}, \quad N \geq 1.$$

Proof. Let us consider the following sequence of polynomials over $\mathbb{F}_p$:

$$F_0(X) = X, \qquad F_i(X) = F_{i-1}(f(X)), \qquad i = 1, 2, \ldots .$$

It is clear that $\deg(F_i) = d^i$ for every $i = 1, 2, \ldots$. Moreover $u_{n+j} = F_j(u_n)$ for any integers $n, j \geq 0$. Put $L = L(u_n, N)$ so that we have

$$u_{n+L} = \sum_{l=0}^{L-1} c_l u_{n+l}, \qquad 0 \leq n \leq N - L - 1,$$

for some $c_0, \ldots, c_{L-1} \in \mathbb{F}_p$. Therefore the polynomial

$$F(X) = -F_L(X) + \sum_{l=0}^{L-1} c_l F_l(X)$$

has degree d^L and at least $\min\{N - L, t\}$ zeros. Thus $d^L \geq \min\{N - L, t\}$. Since otherwise the result is trivial, we may suppose $L \leq \lfloor \log_d N \rfloor$ and get $d^L \geq \min\{N - \lfloor \log_d N \rfloor, t\}$, which yields the assertion. □

For some special classes of polynomials much better results are available, see [30, 32, 65]. For instance, in case of the largest possible period $t = p$ we have

$$L(u_n, N) \geq \min\{N - p + 1, p/d\}, \quad N \geq 1.$$

The *inversive (congruential) generator* (y_n) defined by

$$y_{n+1} = a y_n^{p-2} + b = \begin{cases} a y_n^{-1} + b & \text{if } y_n \neq 0, \\ b & \text{otherwise,} \end{cases} \qquad n \geq 0, \tag{2.8}$$

with $a, b, y_0 \in \mathbb{F}_p$, $a \neq 0$, has linear complexity profile

$$L(y_n, N) \geq \min\left\{\frac{N-1}{3}, \frac{t-1}{2}\right\}, \quad N \geq 1. \tag{2.9}$$

This sequence, introduced by Eichenauer and Lehn [18], has succeeded in drawing significant attention due to some of its enchanting properties. In terms of the linear complexity profile the lower bound (2.9) shows that the inversive generator is almost optimal. This aspect will be reconsidered in Section 2.2. The sequence (y_n) attains the largest possible period $t = p$ if, for instance, $X^2 - aX - b$ is a primitive polynomial over $\mathbb{F}_p$. See Flahive and Niederreiter [21] for a refinement of this result.

The *power generator* (p_n), defined as

$$p_{n+1} = p_n^e, \quad n \geq 0,$$

with some integer $e \geq 2$ and initial value $0 \neq p_0 \in \mathbb{F}_p$ satisfies

$$L(p_n, N) \geq \min\left\{\frac{N^2}{4(p-1)}, \frac{t^2}{p-1}\right\}, \quad N \geq 1.$$

Results about the period length of (p_n) can be found in Friedlander *et al* [23, 24].

The family of *Dickson polynomials* $D_e(X, a) \in \mathbb{F}_p[X]$ is defined by the recurrence relation

$$D_e(X, a) = XD_{e-1}(X, a) - aD_{e-2}(X, a), \quad e = 2, 3, \ldots,$$

with initial values $D_0(X, a) = 2$, $D_1(X, a) = X$, where $a \in \mathbb{F}_p$. Obviously, the degree of D_e is e. It is easy to see that $D_e(X, 0) = X^e$, $e \geq 2$, which corresponds to the case of the power generator. In the special case that $a = 1$ the lower bound

$$L(u_n, N) \geq \frac{\min\{N^2, 4t^2\}}{16(p+1)} - (p+1)^{1/2}, \quad N \geq 1,$$

for a new class of nonlinear congruential generators where $f(X) = D_e(X, 1)$ is proven by Aly and Winterhof [1]. Here t is a divisor of $p-1$ or $p+1$.

Another class of nonlinear congruential pseudorandom number generators, where $f(X)$ is a Rédei function, is analysed by Meidl and Winterhof [52]. Suppose that

$$r(X) = X^2 - \alpha X - \beta \in \mathbb{F}_p[X]$$

is an irreducible quadratic polynomial with the two different roots ξ and $\zeta = \xi^p$ in $\mathbb{F}_{p^2}$. We consider the polynomials $g_e(X)$ and $h_e(X) \in \mathbb{F}_p[X]$, which are uniquely defined by the equation

$$(X + \xi)^e = g_e(X) + h_e(X)\xi.$$

The *Rédei function* $f_e(X)$ of degree e is then given by

$$f_e(X) = \frac{g_e(X)}{h_e(X)}.$$

The function $f_e(X)$ is a permutation of $\mathbb{F}_p$ if and only if $\gcd(e, p+1) = 1$, see Nöbauer [63]. For further background on Rédei functions we refer to [41, 63]. We consider generators (r_n) defined by

$$r_{n+1} = f_e(r_n), \quad n \geq 0,$$

with a Rédei permutation $f_e(X)$ and some initial element $u_0 \in \mathbb{F}_p$. The sequence (r_n) is periodic with period t, where t is a divisor of $\varphi(p+1)$ and φ is the Euler φ-function. As any mapping over $\mathbb{F}_p$, the Rédei permutation can be uniquely represented by a polynomial of degree at most $p-1$ and therefore the sequence (r_n) belongs to the class of nonlinear congruential pseudorandom number generators (2.7). In [52] the following lower bound on the linear complexity profile of the sequence (r_n) is obtained:

$$L(r_n, N) \geq \frac{\min\{N^2, 4t^2\}}{20(p+1)^{3/2}}, \quad N \geq 2,$$

provided that $t \geq 2$.

The linear complexity profile of pseudorandom number generators over $\mathbb{F}_p$, defined by a recurrence relation of order $m \geq 1$ is studied in Topuzoğlu and Winterhof [71];

$$u_{n+1} = f(u_n, u_{n-1}, \ldots, u_{n-m+1}),\ n = m-1, m, \ldots. \tag{2.10}$$

Here initial values $u_0, \ldots, u_{m-1}$ are in $\mathbb{F}_p$ and $f \in \mathbb{F}_p(X_1, \ldots, X_m)$ is a rational function in m variables over $\mathbb{F}_p$. The sequence (2.10) eventually becomes periodic with least period $t \leq p^m$. The fact that t can actually attain the value p^m gains nonlinear generators of higher orders a particular interest. In case of a polynomial f, lower bounds for the linear complexity and linear complexity profile of higher order generators are given in [71].

A particular rational function f in (2.10) gives rise to a generalisation of the inversive generator (2.8), as described below. Let (x_n) be the sequence over $\mathbb{F}_p$, defined by the linear recurrence relation of order $m+1$;

$$x_{n+1} = a_0 x_n + a_1 x_{n-1} + \ldots + a_m x_{n-m}, \quad n \geq m,$$

with $a_0, a_1, \ldots, a_m \in \mathbb{F}_p$ and initial values $x_0, \ldots, x_m \in \mathbb{F}_p$. An increasing function $N(n)$ is defined by

$$N(0) = \min\{n \geq 0 : x_n \neq 0\},$$
$$N(n) = \min\{l \geq N(n-1) + 1 : x_l \neq 0\},$$

and the nonlinear generator (z_n) is produced by

$$z_n = x_{N(n)+1} x_{N(n)}^{-1}, \quad n \geq 0$$

(see Eichenauer et.al. [17]). It is easy to see that (z_n) satisfies

$$z_{n+1} = f(z_n, \ldots, z_{n-m+1}), \quad n \geq m-1,$$

whenever $z_n \cdots z_{n-m+1} \neq 0$ for the rational function

$$f(X_1, \ldots, X_m) = a_0 + a_1 X_1^{-1} + a_2 X_1^{-1} X_2^{-1} + \ldots + a_m X_1^{-1} X_2^{-1} \cdots X_m^{-1}.$$

A sufficient condition for (z_n) to attain the maximal period length p^m is given in [17]. It is shown in [71] that the linear complexity profile $L(z_n, N)$ of (z_n) with the least period p^m satisfies

$$L(z_n, N) \geq \min\left(\left\lceil \frac{p-m}{m+1} \right\rceil p^{m-1} + 1, N - p^m + 1\right), \quad N \geq 1.$$

This result is in accordance with (2.9), i.e., the case $m = 1$.

Legendre Sequence and Related Bit Sequences

Let $p > 2$ be a prime. The *Legendre-sequence* (l_n) is defined by

$$l_n = \begin{cases} 1, & \left(\frac{n}{p}\right) = -1, \\ 0, & \text{otherwise}, \end{cases} \qquad n \geq 0,$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre-symbol. Obviously, (l_n) is p-periodic. Results on the linear complexity of (l_n) can be found in [13, 73]. We give the proof here since the method is illustrative.

Theorem 2.3. *The linear complexity of the Legendre sequence is*

$$L(l_n) = \begin{cases} (p-1)/2, & p \equiv 1 \bmod 8, \\ p, & p \equiv 3 \bmod 8, \\ p-1, & p \equiv 5 \bmod 8, \\ (p+1)/2, & p \equiv 7 \bmod 8. \end{cases}$$

Proof. We start with the well known relation

$$L(l_n) = p - \deg(\gcd(S(X), X^p - 1))$$

where

$$S(X) = \sum_{n=0}^{p-1} l_n X^n,$$

(see for example [66, Lemma 8.2.1]), i.e., in order to determine the linear complexity it is sufficient to count the number of common zeros of $S(X)$ and $X^p - 1$ in the splitting field $\mathbb{F}$ of $X^p - 1$ over $\mathbb{F}_2$. Let $1 \neq \beta \in \mathbb{F}$ be a root of $X^p - 1$. For q with $\left(\frac{q}{p}\right) = 1$ we have

$$S(\beta^q) = \sum_{n=0}^{p-1} l_n \beta^{nq} = \sum_{\left(\frac{n}{p}\right)=-1} \beta^{nq} = \sum_{\left(\frac{n}{p}\right)=-1} \beta^n = S(\beta)$$

and for m with $\left(\frac{m}{p}\right) = -1$,

$$\begin{aligned} S(\beta^m) &= \sum_{\left(\frac{n}{p}\right)=-1} \beta^{nm} = \sum_{\left(\frac{n}{p}\right)=1} \beta^n \\ &= \sum_{n=1}^{p-1} (1+l_n)\beta^n = \frac{\beta^p - \beta}{\beta - 1} + S(\beta) = 1 + S(\beta). \end{aligned}$$

Moreover, we have $S(\beta) \in \mathbb{F}_2$ if and only if $S(\beta)^2 = S(\beta^2) = S(\beta)$, i.e., $\left(\frac{2}{p}\right) = 1$ which is equivalent to $p \equiv \pm 1 \bmod 8$. Next we have

$$S(1) = \sum_{\left(\frac{n}{p}\right)=-1} 1 = \frac{p-1}{2} = \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4, \\ 1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Let Q and N denote the sets of quadratic residues and nonresidues modulo p, respectively. If $p \equiv \pm 1 \bmod 8$ then we have one of the following two cases: Either $S(\beta^q) = S(\beta^m) + 1 = 0$ for all $q \in Q$ and $m \in N$, or $S(\beta^m) = S(\beta^q) + 1 = 0$ for all $q \in Q$ and $m \in N$. Now the assertion is clear since $|Q| = |N| = (p-1)/2$. □

The profile can be estimated by using bounds on incomplete sums of Legendre symbols. The proof below essentially follows that of [66, Theorem 9.2].

Theorem 2.4. *The linear complexity profile of the Legendre sequence satisfies*

$$L(l_n, N) > \frac{\min\{N, p\}}{1 + p^{1/2}(1 + \log p)} - 1, \quad N \geq 1.$$

Proof. Since $L(l_n, N) \geq L(l_n, p)$ for $N > p$ we may assume $N \leq p$. As usual, put $L = L(l_n, N)$ so that

$$l_{n+L} = c_{L-1} l_{n+L-1} + \ldots + c_0 l_n, \quad 0 \leq n \leq N - L - 1,$$

for some $c_0, \ldots, c_{L-1} \in \mathbb{F}_2$. Since $(-1)^{l_n} = \left(\frac{n}{p}\right)$, $1 \leq n \leq p-1$, with $c_L = 1$ we have

$$1 = (-1)^{\sum_{j=0}^{L} c_j l_{n+j}} = \left(\frac{\prod_{j=0}^{L} (n+j)^{c_j}}{p} \right), \ 1 \leq n \leq N - L - 1,$$

and thus

$$N - L - 1 = \sum_{n=1}^{N-L-1} \left(\frac{\prod_{j=0}^{L} (n+j)^{c_j}}{p} \right).$$

The following bound for the right hand side of this equation

$$\left|\sum_{n=1}^{N-L-1}\left(\frac{\prod_{j=0}^{L}(n+j)^{c_j}}{p}\right)\right| < (L+1)p^{1/2}(1+\log p) \tag{2.11}$$

yields

$$N-(L+1) < (L+1)p^{1/2}(1+\log p)$$

from which the assertion follows. The bound (2.11) can be proved as follows: For an integer $k \geq 2$ put $\mathrm{e}_k(x) = \exp(2\pi \mathrm{i} x/k)$. The relations below can be found in [74];

$$\sum_{a=0}^{k-1}\mathrm{e}_k(au) = \begin{cases} 0, & u \not\equiv 0 \bmod k, \\ k, & u \equiv 0 \bmod k, \end{cases} \tag{2.12}$$

$$\sum_{a=1}^{k-1}\left|\sum_{x=0}^{K-1}\mathrm{e}_k(ax)\right| \leq k\log k, \quad 1 \leq K \leq k. \tag{2.13}$$

The Weil bound, which we present in the following form (see [64, Theorems 2C and 2G]),

$$\left|\sum_{a=0}^{p-1}\chi(f(a))\mathrm{e}_p(ax)\right| \leq \begin{cases} p^{1/2}\deg f, & 1 \leq x < p, \\ p^{1/2}(\deg f - 1), & x = 0, \end{cases} \tag{2.14}$$

where χ denotes a nontrivial multiplicative character of $\mathbb{F}_p$ and $f \in \mathbb{F}_p[X]$, enables us to handle the complete hybrid character sum below. Application of Vinogradov's method (see [70]) with (2.12) and

$$f(X) = \prod_{j=0}^{L}(X+j)^{c_j}$$

gives

$$\begin{aligned}\left|\sum_{n=1}^{N-L-1}\left(\frac{f(n)}{p}\right)\right| &= \frac{1}{p}\left|\sum_{x\in\mathbb{F}_p}\sum_{m\in\mathbb{F}_p}\left(\frac{f(m)}{p}\right)\sum_{n=1}^{N-L-1}\mathrm{e}_p(x(n-m))\right| \\ &\leq \frac{1}{p}\sum_{x\in\mathbb{F}_p}\left|\sum_{m\in\mathbb{F}_p}\left(\frac{f(m)\mathrm{e}_p(-xm)}{p}\right)\right|\left|\sum_{n=1}^{N-L-1}\mathrm{e}_p(xn))\right| \\ &< (L+1)p^{1/2}(1+\log p),\end{aligned}$$

where we used that f is not a square (since $c_L = 1$) to apply (2.14) in the case $x = 0$. □

For similar sequences, that are defined by the use of the quadratic character of arbitrary finite fields and the study of their linear complexity profiles, see [39, 46, 76].

Let γ be a primitive element and η be the quadratic character of the finite field $\mathbb{F}_q$ of odd characteristic. The *Sidelnikov sequence* (σ_n) is defined by

$$\sigma_n = \begin{cases} 1, & \text{if } \eta(\gamma^n + 1) = -1, \\ 0, & \text{otherwise,} \end{cases} \qquad n \geq 0.$$

In many cases one is able to determine the linear complexity $L(\sigma_n)$ over $\mathbb{F}_2$ exactly, see Meidl and Winterhof [51]. For example, if $(q-1)/2$ is an odd prime such that 2 is a primitive root modulo $(q-1)/2$, then (s_n) attains the largest possible linear complexity $L(\sigma_n) = q-1$. Moreover we have the lower bound, see [51],

$$L(\sigma_n, N) = \Omega\left(\frac{\min\{N, q\}}{q^{1/2}\log q}\right), \quad N \geq 1.$$

The linear complexity over $\mathbb{F}_p$ of this sequence has been estimated in Garaev *et al* [27] by using bounds of character sums with middle binomial coefficients. For small values of p the linear complexity can be evaluated explicitly.

Let p and q be two distinct odd primes. Put

$$Q = \{q, 2q, \ldots, (p-1)q\},\ Q_0 = Q \cup \{0\},$$

and

$$P = \{p, 2p, \ldots, (q-1)p\}.$$

The pq-periodic sequence (t_n) over $\mathbb{F}_2$, defined by

$$t_n = \begin{cases} 0, & \text{if } (n \bmod pq) \in Q_0, \\ 1, & \text{if } (n \bmod pq) \in P, \\ \left(1 - \left(\frac{n}{p}\right)\left(\frac{n}{q}\right)\right)/2, & \text{otherwise} \end{cases}$$

is called the *two-prime generator* (or *generalised cyclotomic sequence of order* 2) (see [10], and [13, Chapter 8.2]). Under the restriction $\gcd(p-1, q-1) = 2$

it satisfies

$$L(t_n) = \begin{cases} pq-1, & p \equiv 1 \bmod 8 \text{ and } q \equiv 3 \bmod 8 \\ & \text{or } p \equiv 5 \bmod 8 \text{ and } q \equiv 7 \bmod 8, \\ (p-1)q, & p \equiv 7 \bmod 8 \text{ and } q \equiv 3 \bmod 8 \\ & \text{or } p \equiv 3 \bmod 8 \text{ and } q \equiv 7 \bmod 8, \\ pq-p-q+1, & p \equiv 7 \bmod 8 \text{ and } q \equiv 5 \bmod 8 \\ & \text{or } p \equiv 3 \bmod 8 \text{ and } q \equiv 1 \bmod 8, \\ (pq+p+q-3)/2, & p \equiv 1 \bmod 8 \text{ and } q \equiv 7 \bmod 8 \\ & \text{or } p \equiv 5 \bmod 8 \text{ and } q \equiv 3 \bmod 8, \\ (p-1)(q-1)/2, & p \equiv 7 \bmod 8 \text{ and } q \equiv 1 \bmod 8 \\ & \text{or } p \equiv 3 \bmod 8 \text{ and } q \equiv 5 \bmod 8, \\ (p-1)(q+1)/2, & p \equiv 7 \bmod 8 \text{ and } q \equiv 7 \bmod 8 \\ & \text{or } p \equiv 3 \bmod 8 \text{ and } q \equiv 3 \bmod 8. \end{cases}$$

In the most important case when $|p-q|$ is small we have a lower bound on the linear complexity profile of order of magnitude

$$O(N^{1/2}(pq)^{-1/4}\log^{-1/2}(pq))$$

for $2 \le N < pq$.

Elliptic Curve Generators

We recall some definitions and basic facts about elliptic curves (see [37] or Chapter 5).

Let $p > 3$ be a prime and E be an elliptic curve over $\mathbb{F}_p$ of the form

$$Y^2 = X^3 + aX + b$$

where the coefficients a, b are in $\mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$. The set $E(\mathbb{F}_p)$ of all $\mathbb{F}_p$ -rational points on E forms an abelian group where we denote addition by $\oplus$. The point O at infinity is the zero element of $E(\mathbb{F}_p)$. We recall the Hasse-Weil bound

$$|\#E(\mathbb{F}_p) - p - 1| \le 2p^{1/2},$$

where $\#E(\mathbb{F}_p)$ is the number of $\mathbb{F}_p$-rational points, including O. For a given initial value $W_0 \in E(\mathbb{F}_p)$, a fixed point $G \in E(\mathbb{F}_p)$ of order t and a rational function $f \in \mathbb{F}_p(E)$ the *elliptic curve congruential generator* (with respect to f) is defined by $w_n = f(W_n)$, $n \ge 0$, where

$$W_n = G \oplus W_{n-1} = nG \oplus W_0, \quad n \ge 1.$$

Obviously, (w_n) is t-periodic. See [3, 34] and references therein for results on the properties of elliptic curve generators. For example, choosing the function

$f(x,y)=x$, the work of Hess and Shparlinski [34] gives the following lower bound for the linear complexity profile:

$$L(w_n,N)\geq \min\{N/3,t/2\},\quad N\geq 2.$$

Here we present an elementary proof of a slightly weaker result. Let $x(Q)$ denote the first coordinate x of the point $Q=(x,y)\in E$.

Theorem 2.5. *Let (w_n) be the t-periodic sequence defined by*

$$w_n=x(nG),\quad 1\leq n\leq t-1, \tag{2.15}$$

with some $w_0\in\mathbb{F}_p$ and $G\in E$ of order t. Then we have

$$L(w_n,N)\geq \frac{\min\{N,t/2\}-3}{4},\quad N\geq 2.$$

Proof. We may assume $N\leq t/2$ and $L(w_n,N)<t/2$. Put $nG=(x_n,y_n)$, $1\leq n\leq t-1$. Note that $x_k=x_m$ if and only if $k=m$ or $k=t-m$, $1\leq k\leq t-1$, and $y_k=0$ if and only if t is even and $k=t/2$. Put $c_L=-1$ and assume that

$$\sum_{l=0}^{L}c_l w_{n+l}=0,\quad L+1\leq n\leq N-L-1,$$

or equivalently

$$\sum_{l=0}^{L}c_l w_{t-n-l}=0,\quad L+1\leq n\leq N-L-1.$$

Hence,

$$\sum_{l=0}^{L}c_l\frac{w_{n+l}+w_{t-n-l}}{2}=0,\quad L+1\leq n\leq N-L-1.$$

By the addition formulas for points on elliptic curves we have

$$\begin{aligned} x_{n+l} &= \left(\frac{y_n-y_l}{x_n-x_l}\right)^2-(x_n+x_l)\\ &= \frac{x_l x_n^2+(x_l^2+a)x_n+ax_l+2b-2y_l y_n}{(x_n-x_l)^2},\ l+1\leq n\leq t-l-1, \end{aligned}$$

where we used $y_n^2=x_n^3+ax_n+b$. Similarly we get

$$x_{t-n-l}=\frac{x_l x_n^2+(x_l^2+a)x_n+ax_l+2b+2y_l y_n}{(x_n-x_l)^2},\ l+1\leq n\leq t-l-1,$$

and hence

$$\frac{x_{n+l}+x_{t-n-l}}{2}=\frac{x_l x_n^2+(x_l^2+a)x_n+ax_l+2b}{(x_n-x_l)^2},\quad l+1\le n\le t-l-1.$$

So we get

$$\sum_{l=0}^{L} c_l\frac{x_l x_n^2+(x_l^2+a)x_n+ax_l+2b}{(x_n-x_l)^2}=0,\quad L+1\le n\le N-L-1.$$

Clearing denominators we get

$$\sum_{l=0}^{L} c_l(x_l x_n^2+(x_l^2+a)x_n+ax_l+2b)\prod_{\substack{j=0\\ j\ne l}}^{L}(x_n-x_j)^2=0,\ L+1\le n\le N-L-1.$$

So the polynomial

$$F(X)=\sum_{l=0}^{L} c_l(x_l X^2+(x_l^2+a)X+ax_l+2b)\prod_{\substack{j=0\\ j\ne l}}^{L}(X-x_j)^2$$

of degree at most $2(L+1)$ has at least $N-2L-1$ different zeros. Moreover, we have

$$F(x_L)=-2(x_L^3+ax_L+b)\prod_{j=0}^{L-1}(x_L-x_j)^2=-2y_L^2\prod_{j=0}^{L-1}(x_L-x_j)^2\ne 0.$$

Hence we get $2(L+1)\ge N-2L-1$ and the result follows. □

2.2 Related Measures

Lattice Test

In order to study the structural properties of a given periodic sequence (s_n) over $\mathbb{F}_q$, it is natural to consider the subspaces $\mathcal{L}(s_n,s)$ of $\mathbb{F}_q^s$ for $s\ge 1$, spanned by the vectors $\mathbf{s}_n-\mathbf{s}_0$, $n=1,2,\ldots$ where

$$\mathbf{s}_n=(s_n,s_{n+1},\ldots,s_{n+s-1}),\quad n=0,1,\ldots.$$

We recall that (s_n) is said to pass the *s-dimensional lattice test* for some integer $s\ge 1$, if $\mathcal{L}(s_n,s)=\mathbb{F}_q^s$. It is obvious for example that the linear generator (2.1) can pass the s-dimensional lattice test at most for $s=1$. On the other hand for $q=p$, the nonlinear generator (2.2) passes the test for all $s\le \deg g$ (see [53]). However this test is well known to be unreliable since

sequences, which pass the lattice test for large dimensions, yet having bad statistical properties are known [53].

Accordingly the notion of *lattice profile* is introduced by Dorfer and Winterhof [16]. For given $s \geq 1$ and $N \geq 2$ we say that (s_n) passes the *s-dimensional N-lattice test* if the subspace spanned by the vectors $\mathbf{s}_n - \mathbf{s}_0$, $1 \leq n \leq N - s$, is $\mathbb{F}_q^s$. The largest s for which (s_n) passes the s-dimensional N-lattice test is called the *lattice profile at N*, and is denoted by $S(s_n, N)$.

The lattice profile is closely related to the linear complexity profile, as the following result in [16] shows:

We have either

$$S(s_n, N) = \min\{L(s_n, N), N + 1 - L(s_n, N)\}$$

or

$$S(s_n, N) = \min\{L(s_n, N), N + 1 - L(s_n, N)\} - 1.$$

The results of Dorfer *et al* [15] on the expected value of the lattice profile show that a "random" sequence should have $S(s_n, N)$ to be close to $\min\{N/2, t\}$.

k-Error Linear Complexity

We have remarked that a cryptographically strong sequence necessarily has a high linear complexity. It is also clear that the linear complexity of such a sequence should not decrease significantly when a small number of its terms are altered. The error linear complexity is introduced in connection with this observation [14, 69].

Let (s_n) be a sequence over $\mathbb{F}_q$, with period t. The *k-error linear complexity* $L_k(s_n)$ of (s_n) is defined as

$$L_k(s_n) = \min_{(y_n)} L(y_n),$$

where the minimum is taken over all t-periodic sequences (y_n) over $\mathbb{F}_q$, for which the Hamming distance of the vectors $(s_0, \ldots, s_{t-1})$ and $(y_0, \ldots, y_{t-1})$ is at most k.

One problem of interest here is to determine the minimum value k, for which $L_k(s_n) < L(s_n)$. This problem is tackled by Meidl [44], in case (s_n) is a bit sequence with period length p^n, where p is an odd prime and 2 is a primitive root modulo p^2. Meidl [44] also describes an algorithm to determine the k-error linear complexity that is based on an algorithm of [79]. Stronger results for p^n-periodic sequences over $\mathbb{F}_p$ have been recently obtained in Meidl [45].

Here we give the proof of the following recent result on the k-error linear complexity over $\mathbb{F}_p$ of Legendre sequences, obtained by Aly and Winterhof in [2].

Theorem 2.6. *Let $L_k(l_n)$ denote the k-error linear complexity over $\mathbb{F}_p$ of the Legendre sequence (l_n). Then,*

$$L_k(l_n) = \begin{cases} p, & k = 0, \\ (p+1)/2, & 1 \le k \le (p-3)/2, \\ 0, & k \ge (p-1)/2. \end{cases}$$

Proof. Put

$$g_1(X) = \frac{1}{2}\left(X^{p-1} - X^{(p-1)/2}\right) \text{ and } g_2(X) = \frac{1}{2}\left(1 - X^{(p-1)/2}\right).$$

Since $l_n = g_1(n)$ for $n \ge 0$ we get that the Legendre sequence (l_n) over $\mathbb{F}_p$ has linear complexity $L(l_n) = p$ by (2.3).

Consider now the p-periodic sequence (l'_n) defined by $l'_n = g_2(n)$, $n \ge 0$. Note that

$$g_1(n) = g_2(n), \quad 1 \le n \le p-1,$$

and

$$L_k(l_n) \le L(l'_n) = \frac{p+1}{2}, \quad k \ge 1.$$

Assume now that $1 \le k \le (p-3)/2$. Let (s_n) be any sequence obtained from (l_n) by changing at most $(p-3)/2$ elements. Suppose that g is the polynomial in $\mathbb{F}_p[x]$ of degree at most $p-1$, which represents the sequence (s_n), i.e., $s_n = g(n)$, $n \ge 0$.

It is obvious that the sequences (s_n) and (l'_n) coincide for at least $p - 1 - k \ge (p+1)/2$ elements in a period. Hence, the polynomial $g(X) - g_2(X)$ has at least $(p+1)/2$ zeros, which implies that either $g(X) = g_2(X)$ or $\deg g \ge (p+1)/2$. Therefore $L_k(l_n) = L(l'_n) = (p+1)/2$.

Finally we remark that $L_k(l_n) = 0$ for $k \ge (p-1)/2$, since we have exactly $(p-1)/2$ nonzero elements in a period of (l_n) and the zero sequence of linear complexity 0 can be obtained by $(p-1)/2$ changes. □

Aly and Winterhof also give a lower bound for the k-error linear complexity over $\mathbb{F}_p$ of Sidelnikov sequences in the same paper ,

$$L_k(\sigma_n) \ge \min\left(\left(\frac{p+1}{2}\right)^r - 1, \frac{q-1}{k+1} - \left(\frac{p+1}{2}\right)^r + 1\right).$$

For $k \ge (q-1)/2$ we have $L_k(\sigma_n) = 0$. The 1-error linear complexity over $\mathbb{F}_p$ of Sidelnikov sequences has recently be determined by Eun *et al.* in [20] to be

$$L_1(\sigma_n) = \left(\frac{p+1}{2}\right)^r - 1, \quad q > 3.$$

Other Measures Related to Linear Complexity

The *Kolmogorov complexity* of a binary sequence is, roughly speaking, the length of the shortest computer program that generates the sequence. The relationship between linear complexity and Kolmogorov complexity was studied in [4, 75].

We recall that the *nonlinear complexity profile* $NL_m(s_n, N)$ of an infinite sequence (s_n) over $\mathbb{F}_q$ is the function, which is defined for every integer $N \geq 2$, as the smallest k such that a polynomial recurrence relation

$$s_{n+k} = \Psi(s_{n+k-1}, \ldots, s_n), \qquad 0 \leq n \leq N-k-1,$$

with a polynomial $\Psi(\lambda_1, \ldots, \lambda_k)$ over $\mathbb{F}_q$ of total degree at most m can generate the first N terms of (s_n). Note that generally speaking $NL_1(s_n, N) \neq L(s_n, N)$ because in the definition of $L(s_n, N)$ one can use only homogeneous linear polynomials. Obviously, we have

$$L(s_n, N) \geq NL_1(s_n, N) \geq NL_2(s_n, N) \geq \ldots.$$

See [32] for the presentation of results on the linear complexity profile of nonlinear, inversive and quadratic exponential generators in a more general form, namely in terms of lower bounds on the nonlinear complexity profile.

Linear Complexity and Predictability

It is clear that sequences with low linear complexity have to be avoided for cryptographic applications. One should note that sequences which show favourable behaviour with respect to linear complexity and related quality measures should also be used with care. Rigorous results, demonstrating this fact, have been recently obtained by Blackburn *et al* [6, 7], which we briefly describe below.

As we have remarked earlier, the inversive generator (2.8) stands out as a sequence with almost best possible linear complexity. Nevertheless it turns out that it is polynomial time predictable if sufficiently many bits of its consecutive terms are known, except for some very limited special cases.

Recall that the inversive generator (y_n) is defined as

$$y_{n+1} = ay_n^{p-2} + b = \begin{cases} ay_n^{-1} + b & \text{if } y_n \neq 0, \\ b & \text{otherwise,} \end{cases} \qquad n \geq 0,$$

with $a, b, y_0 \in \mathbb{F}_p$ (regarded as integers in $\{0, 1, \ldots, p-1\}$), $a \neq 0$.

The elements a, b and y_0 are assumed to be the secret key in the cryptographic setting. Since it is easy to recover the secret key in case several consecutive terms of the sequence are known, it is assumed that only the most significant bits of them are revealed. When approximations x_0, x_1, x_2, x_3 to $y_n, y_{n+1}, y_{n+2}, y_{n+3}$ are known for some n, [6] shows that $a, b, y_n, \ldots, y_{n+3}$ can be recovered in

polynomial (in $\log p$) time, if the approximations are sufficiently good and a small set of values of a, b is excluded.

It is shown in [7] that the knowledge of b, and approximations x_0, x_1, x_2 to y_n, y_{n+1}, y_{n+2} is sufficient to recover a and the consecutive terms y_n, y_{n+1}, y_{n+2}, in polynomial time, provided that the approximations are good enough and the initial value y_0 is not in a certain small set. Although the assumption that b is public is not realistic in the cryptographic setting, it is not unlikely that the result can be extended to the case when b is unknown (see [7]).

References to the earlier work on the predictability of linear congruential generators can also be found in [6, 7]. A weaker attack is discussed in Klapper [36], where the idea is to decrease the linear complexity of a given sequence by considering it over a ring which is different from the ring where the sequence is naturally defined (and its high linear complexity is guaranteed). The result in Shparlinski and Winterhof [67] shows that this approach has very limited chance to succeed.

3. Autocorrelation and Related Distribution Measures for Binary Sequences

3.1 Autocorrelation

One would expect that a periodic random sequence and a shift of it would have a low correlation. Autocorrelation measures the similarity between a sequence (s_n) of period t and its shifts by k positions, for $1 \le k \le t-1$.

The *(periodic) autocorrelation* of a t-periodic binary sequence (s_n) is the function defined by

$$\mathrm{A}(s_n, k) = \sum_{n=0}^{t-1} (-1)^{s_{n+k}+s_n}, \quad 1 \le k \le t-1.$$

Note that Section 3 of Chapter 2 is concerned with the *correlation* of two sequences (s_n) and (t_n).

Obviously a low autocorrelation is a desirable feature for pseudorandom sequences that are used in cryptographic systems. Local randomness of periodic sequences is also of importance cryptographically, since only small parts of the period are used for the generation of stream ciphers.

The *aperiodic autocorrelation* reflects local randomness and is defined by

$$\mathrm{AA}(s_n, k, u, v) = \sum_{n=u}^{v} (-1)^{s_{n+k}+s_n}, \quad 1 \le k \le t-1,\ 0 \le u < v \le p-1.$$

For the Legendre sequences, for example, $\mathrm{A}(l_n, k)$ can be immediately derived from the well-known formula, see e.g. [35],

$$\sum_{n=0}^{p-1} \left(\frac{n}{p}\right)\left(\frac{n+k}{p}\right) = -1, \quad 1 \le k \le p-1,$$

and the following bound on the aperiodic autocorrelation of Legendre sequences follows immediately from (2.11).

Theorem 3.1. *The (aperiodic) autocorrelation of the Legendre sequence satisfies*

$$\mathrm{A}(l_n, k) = \left(\frac{k}{p}\right)\left(1 + (-1)^{(p-1)/2}\right) - 1, \quad 1 \le k \le p-1,$$

$$|\mathrm{AA}(l_n, k, u, v)| \le 2p^{1/2}(1+\log p) + 2,\ 1 \le k \le p-1,\ 0 \le u \le v \le p-1.$$

For bounds on the aperiodic autocorrelation of extended Legendre sequences see [50]. For the aperiodic autocorrelation of Sidelnikov sequences and two-prime generators see [68] and [10], respectively.

3.2 Related Distribution Measures

Higher Order Correlation

In Mauduit and Sárközy [43] the *correlation measure of order* k of a binary sequence (s_n) is introduced as

$$C_k(s_n) = \max_{M,D} \left| \sum_{n=1}^{M} (-1)^{s_{n+d_1}} \cdots (-1)^{s_{n+d_k}} \right|, \quad k \ge 1,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_k)$ with non-negative integers $d_1 < d_2 < \ldots < d_k$ and M such that $M - 1 + d_k \le T - 1$. $C_2(s_n)$ is obviously bounded by the maximal absolute value of the aperiodic autocorrelation of (s_n). It is also shown in [43] that the Legendre sequence has small correlation measure up to rather high orders.

The following family of pseudorandom binary sequences is introduced in Gyarmati [33]: Let p be an odd prime and g be a primitive root modulo p. Denote by $\mathrm{ind}\, n$ the *discrete logarithm* of n to the base g, i.e., $\mathrm{ind}\, n = j$ if $n = g^j$ with $1 \le j \le p-1$. Let $f(X)$ be a polynomial of degree k modulo p. Then the finite sequence (e_n) is defined by

$$e_n = \begin{cases} 1 & \text{if } 1 \le \mathrm{ind}\, f(n) \le (p-1)/2, \\ -1 & \text{if } (p+1)/2 \le \mathrm{ind}\, f(n) \le p-1 \text{ or } p \mid f(n), \end{cases} \quad 1 \le n \le p-1.$$

The correlation measure of the sequence (e_n) is also analysed in [33].

The sequence (k_n) of signs of Kloosterman sums is defined as follows;

$$k_n = \begin{cases} 1 & \text{if } \sum_{j=1}^{p-1} \exp(2\pi i(j+nj^{-1})/p) > 0, \\ -1 & \text{if } \sum_{j=1}^{p-1} \exp(2\pi i(j+nj^{-1})/p) < 0, \end{cases} \quad 1 \le n \le p-1,$$

where j^{-1} is the inverse of j modulo p. Bounds on the correlation measure of order k of (k_n) are given in Fouvry *et al* [22].

Recently Brandstätter and Winterhof [12] have shown that the linear complexity profile of a given t-periodic sequence can be estimated in terms of its correlation measure;

$$L(s_n, N) \ge N - \max_{1 \le k \le L(s_n,N)+1} C_k(s_n), \quad 2 \le N \le t-1.$$

Hence, a lower bound on $L(s_n, N)$ can be obtained whenever an appropriate bound on $\max C_k(s_n)$ is known. The proof is similar to that of Theorem 2.4.

Nonlinearity

Each binary sequence (s_n) of period t over the field $\mathbb{F}_2$ can naturally be associated with a Boolean function B. More precisely, we define an integer m by $2^m \le t < 2^{m+1}$ and denote by $\mathcal{B}_m$ the set of m-bit integers

$$\mathcal{B}_m = \{n \in \mathbb{Z} : 0 \le n \le 2^m - 1\}.$$

We do not distinguish between m-bit integers $n \in \mathcal{B}_m$ and their binary expansion. So $\mathcal{B}_m$ can be considered as the m-dimensional Boolean cube $\mathcal{B}_m = \{0,1\}^m$. The Boolean function $B : \mathcal{B}_m \to \mathbb{F}_2$ associated to the sequence (s_n) is given by

$$B(n) = s_n, \quad n \in \mathcal{B}_m. \tag{3.1}$$

For $n, r \in \mathcal{B}_m$, $\langle n, r \rangle$ denotes the inner product of n and r considered as binary vectors. That is

$$\langle n, r \rangle = n_1 r_1 + \ldots + n_m r_m,$$

where $n = (n_1, \ldots, n_m)$ and $r = (r_1, \ldots, r_m)$ are the binary representations of n and r.

The *Fourier coefficients* of a Boolean function $B : \mathcal{B}_m \to \{0,1\}$ are defined as

$$\hat{B}(r) = 2^{-m} \sum_{n \in \mathcal{B}_m} (-1)^{B(n)+\langle n,r \rangle}, \quad r \in \mathcal{B}_m,$$

and the *nonlinearity* $\mathcal{NL}(B)$ is defined as

$$\mathcal{NL}(B) = 2^{m-1} - 2^{m-1} \max_{r \in \mathcal{B}_m} \left| \hat{B}(r) \right|.$$

The nonlinearity corresponds to the smallest possible Hamming distance between the vector of values of B and the vector of values of a linear function in m variables over $\mathbb{F}_2$. For the cryptographic significance of this notion see [11] and references therein. In particular, a high nonlinearity is necessary for achieving confusion and avoiding differential attacks.

In Brandstätter and Winterhof [11] the nonlinearity of the Boolean function B, defined by (3.1) is estimated in terms of the correlation measure of order 2 of the sequence (s_n). It is shown that

$$\mathcal{NL}(B) > 2^{m-1}(1 - 8^{1/4}2^{-m/4}C_2(s_n)^{1/4}).$$

This result can be applied to any binary sequence for which a bound on the correlation measure of order 2 or the aperiodic autocorrelation is known. For example, consider the Boolean function

$$B(n) = \begin{cases} 0 & \text{if } \left(\frac{n}{p}\right) = 1 \text{ or } n = 0, \\ 1 & \text{if } \left(\frac{n}{p}\right) = -1, \end{cases} \qquad 0 \le n \le 2^m - 1,$$

corresponding to the Legendre sequence, where $2^m \le p < 2^{m+1}$. The bound

$$\mathcal{NL}(B) = 2^{m-1}(1 + O(2^{-m/8}m^{1/4}))$$

follows immediately from [66, Theorem 10.1] or [43].

Note that the Legendre sequence describes the least significant bit of the discrete logarithm. An analogue result on the nonlinearity of the Boolean function corresponding to the sequence of least significant bits of the discrete logarithm in the finite field $\mathbb{F}_{2^r}$ is given in Brandstätter *et al.* [9].

4. Discrepancy and Uniform Distribution

A quantitative measure of uniformity of distribution of a sequence, the so-called discrepancy has a long history. Originated from a classical problem in Diophantine approximations, namely distribution of fractional parts of integer multiples of an irrational in the unit interval, this concept has found applications in various areas like combinatorics, probability theory, mathematical finance, to name a few. It is apparent that it can be used in the analysis of PR sequences; it also emerges as a valuable tool in quasi-Monte Carlo methods where the so-called quasi-random sequences are often utilised.

Let P be a point set (finite sequence) $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1} \in [0,1)^s$ with $s \ge 1$. The *discrepancy* $D_N^{(s)}$ of P is defined as

$$D_N^{(s)}(P) = D_N^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}) = \sup_J \left| \frac{A_N(J)}{N} - V(J) \right|,$$

where the supremum is taken over all subboxes $J \subseteq [0,1)^s$, $A_N(J)$ is the number of points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ in J and $V(J)$ is the volume of J. We put $D_N(P) = D_N^{(1)}(P)$. For an infinite sequence $(\mathbf{s}_n) \in [0,1)^s$, the discrepancy of $(\mathbf{s}_n)$ is defined as

$$D_N^{(s)}(\mathbf{s}_n) = D_N^{(s)}(\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{N-1}).$$

It is evident from the well-known Erdős-Turán inequality, (4.1) below, that the main tool in estimating discrepancy is the use of bounds on exponential sums. Let P be a point set $x_0, x_1, \ldots, x_{N-1}$ in $[0,1)$. There exists an absolute constant C such that for any integer $H \geq 1$,

$$D_N(P) < C\left(\frac{1}{H} + \frac{1}{N}\sum_{h=1}^{H}\frac{1}{h}|S_N(h)|\right), \tag{4.1}$$

where $S_N(h) = \sum_{n=0}^{N-1} \exp(2\pi i h x_n)$.

For the case $s \geq 2$ the generalised version of (4.1), namely the Erdős-Turán-Koksma inequality is used.

The law of the iterated logarithm asserts that the order of magnitude of discrepancy of N points in $[0,1)^s$ should be around $N^{-1/2}(\log\log N)^{1/2}$. Accordingly, as a measure of randomness of a PRN sequence, one investigates the discrepancy of s-tuples of consecutive terms.

Consider, for example, the inversive congruential PRNs, produced by (2.5), with least period p. For a fixed dimension $s \geq 1$, put

$$\mathbf{x}_n = (y_n/p, y_{n+1}/p, \ldots, y_{n+s-1}/p) \in [0,1)^s, \quad n = 0, \ldots, p-1.$$

Depending on the parameters $a, b \in \mathbb{F}_p$, and in particular on the average, $D_p^{(s)}(\mathbf{x}_0, \ldots, \mathbf{x}_{p-1})$ has an order of magnitude between $p^{-1/2}$ and $p^{-1/2}(\log p)^s$ for every $s \geq 2$. Similar favourable results are available, for instance, for nonlinear, quadratic exponential and elliptic curve generators.

As we have remarked earlier, only parts of the period of a PR sequence are used in applications. Therefore bounds on the discrepancy of sequences in parts of the period are of great interest.

The following theorem of Niederreiter and Shparlinski [57] gives an upper bound for the discrepancy of nonlinear congruential PRNs for parts of the period. We present a slightly imroved version.

Theorem 4.1. *Let (u_n) be a nonlinear congruential generator (2.7) with period t. For any positive integer r we have*

$$D_N(u_n/p) = O(N^{-1/(2r)}p^{1/(2r)}(\log p)^{-1/2}\log\log p), \quad 1 \leq N \leq t,$$

where the implied constant depends on r and the degree of f.

Proof. First we prove that, for $\gcd(h,p)=1$,

$$S_N(h) = O(N^{1-1/(2r)}p^{1/(2r)}(\log p)^{-1/2}), \quad 1 \le N \le t. \tag{4.2}$$

Select any $h \in \mathbb{Z}$ with $\gcd(h,p)=1$. It is obvious that for any integer $k \ge 0$ we have

$$\left| S_N(h) - \sum_{n=0}^{N-1} \mathrm{e}_p(u_{n+k}) \right| \le 2k.$$

Therefore, for any integer $K \ge 1$,

$$K|S_N(H)| \le W + K(K-1),$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathrm{e}_p(u_{n+k}) \right|.$$

We consider again the sequence of polynomials $F_k(X)$ defined in the proof of Theorem 2.2. By the Hölder inequality and using $u_{n+k} = F_k(u_n)$ we obtain

$$\begin{aligned} W^{2r} &\le N^{2r-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathrm{e}_p(F_k(u_n)) \right|^{2r} \\ &\le N^{2r-1} \sum_{x \in \mathbb{F}_p} \left| \sum_{k=0}^{K-1} \mathrm{e}_p(F_k(x)) \right|^{2r} \\ &\le N^{2r-1} \sum_{k_1,\ldots,k_{2r}}^{K-1} \left| \sum_{x \in \mathbb{F}_p} \mathrm{e}_p(F(x)) \right|, \end{aligned}$$

where $F(X) = F_{k_1}(X) + \ldots + F_{k_r}(X) - F_{k_{r+1}}(X) - \ldots - F_{k_{2r}}(X)$. If $\{k_1,\ldots,k_r\} = \{k_{r+1},\ldots,k_{2r}\}$, then $F(X)$ is constant and the inner sum is trivially equal to p. There are at most $r!K^r$ such sums. Otherwise we can apply Weil's bound to the inner sum using $\deg F \le d^{K-1}$, to get the upper bound $d^{K-1}p^{1/2}$ for at most K^{2r} sums. Hence,

$$W^{2r} \le r!K^r N^{2r-1}p + d^{K-1}K^{2r}N^{2r-1}p^{1/2}.$$

Choose

$$K = \left\lceil 0.4 \frac{\log p}{\log d} \right\rceil.$$

Then it is easy to see that the first term dominates the second one and we get (4.2) after simple calculations. Choosing

$$H = \left\lceil N^{1/(2r)}p^{-1/(2r)}(\log p)^{1/2} \right\rceil$$

in (4.1), we obtain the discrepancy bound. □

Note that the known upper bounds obtained for full period are often the best possible, as the corresponding lower bounds demonstrate (see [53]). However for parts of the period, the bound in Theorem 4.1 is rather weak and improvements are sought for. One should note on the other hand that the method used in [57] for estimating $S_N(h)$, is the first to give nontrivial bounds for parts of the period. This method also applies in case $s \geq 2$.

As to bounds on discrepancy of some special nonlinear generators for parts of the period, much better results can be obtained. For the inversive congruential generators (y_n) of period t, Niederreiter and Shparlinski showed in [58] that

$$D_N(y_n/p) = O(N^{-1/2}p^{1/4}\log p), \quad 1 \leq N \leq t.$$

For an average discrepancy bound over all initial values of a fixed inversive congruential generator see Niederreiter and Shparlinski [60].

Results about the distribution of the power generator follow from the bounds of exponential sums in Friedlander and Shparlinski [25] and in Bourgain [8]. Exponential sums of nonlinear generators with Dickson polynomials have been estimated in Gomez-Perez *et al* [28]. Discrepancy bounds for nonlinear congruential generators of higher order can be found in [29, 31, 72].

For the distribution of explicit nonlinear generators see the series of papers [61, 62, 77]. In particular for the explicit inversive generator (2.4) we have the discrepancy bound

$$D_N(z_n/p) = O(\min\{N^{-1/2}p^{1/4}\log p, N^{-1}p^{1/2}(\log p)^2\}), \quad 1 \leq N \leq p.$$

The order of magnitude of discrepancy of the PRNs produced by the elliptic curve generator of period t with $f(x,y) = x$ or $f(x,y) = y$ is $t^{-1}p^{1/2}\log p$, by Hess and Shparlinski [34]. This result can be easily extended to parts of the period. We present the proof of the following special version.

Theorem 4.2. *The sequence* (w_n) *defined by* (2.15)*, having period* t *satisfies*

$$D_N(w_n/p) = O(t^{-1}p^{1/2}\log p \log t), \quad 1 \leq N < t.$$

Proof. First we estimate the exponential sums

$$S_N = \sum_{n=1}^{N-1} \mathrm{e}_p(w_n) = \sum_{n=1}^{N-1} \mathrm{e}_p(x(nG)), \quad 1 \leq N < t.$$

Using the Vinogradov method again we get by (2.12)

$$|S_N| \leq \frac{1}{t}\sum_{a=0}^{t-1}\left|\sum_{n=1}^{t-1}\mathrm{e}_p(x(nG))\mathrm{e}_t(an)\right|\left|\sum_{m=0}^{N-1}\mathrm{e}_t(am)\right| = O(p^{1/2}\log t)$$

by (2.13) and [38, Corollary 1]. The discrepancy bound follows from (4.1). □

The distribution of an elliptic curve analogue of the power generator has been analysed in Lange and Shparlinski [40].

We should remark that the linear congruential generator, unlike other generators we mentioned above, is distributed too evenly. In case a in (2.1) is a primitive root mod p, $b = 0$ and $s_0 \neq 0$, the sequence has period length $p - 1$, and for most choices of a,

$$D_{p-1}^{(s)}(s_n/p) = O(p^{-1}(\log p)^s(\log\log(p+1))).$$

Although such low-discrepancy sequences need to be avoided as PR sequences, they are needed for use in quasi-Monte Carlo methods (see [53]). The study of *irregularities of distribution* suggests that for any N-element point set P and any sequence (s_n) in $[0,1)^s$, $s \geq 1$, the least order of magnitude of $D_N^{(s)}(P)$ and $D_N^{(s)}(s_n)$ can be $N^{-1}(\log n)^{s-1}$ and $N^{-1}(\log n)^s$, respectively.

The construction of point sets and sequences with these least possible bounds has been a challenging problem; both for theoretical interest and for applications. Recent results of Xing, Niederreiter and Özbudak show that geometric methods are particularly fruitful for such constructions. We refer the reader to the surveys by Niederreiter [54, 56] for an extensive description of this study, illustrating yet another application of global function fields.

References

[1] H. Aly and A. Winterhof, "On the linear complexity profile of nonlinear congruential pseudorandom number generators with Dickson polynomials", Des. Codes Cryptogr., to appear.

[2] H. Aly and A. Winterhof, "On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov sequences", preprint 2005.

[3] P. Beelen and J.M. Doumen, "Pseudorandom sequences from elliptic curves", *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, Springer, Berlin, 37–52 (2002).

[4] T. Beth and Z.D. Dai, "On the complexity of pseudo-random sequences—or: If you can describe a sequence it can't be random", *Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989)*, Lecture Notes in Comput. Sci., Vol. 434, 533–543 (1990).

[5] S.R. Blackburn, T. Etzion and K.G. Paterson, "Permutation polynomials, de Bruijn sequences, and linear complexity", J. Combin. Theory Ser. A, Vol. 76, 55–82 (1996).

[6] S.R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. Shparlinski, "Predicting the inversive generator", Lecture Notes in Comput. Sci., Vol. 2898, 264–275 (2003).

[7] S.R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. Shparlinski, "Predicting nonlinear pseudorandom number generators", Math. Comp., Vol. 74, 1471–1494 (2005).

[8] J. Bourgain, "Mordell's exponential sum estimate revisited", J. Amer. Math. Soc., Vol. 18, 477-499 (2005).

[9] N. Brandstätter, T. Lange and A. Winterhof, "On the non-linearity and sparsity of Boolean functions related to the discrete logarithm", preprint 2005.

[10] N. Brandstätter and A. Winterhof, "Some notes on the two-prime generator", IEEE Trans. Inform. Theory, Vol. 51, 3654–3657 (2005).

[11] N. Brandstätter and A. Winterhof, "Nonlinearity of binary sequences with small autocorrelation", *Proceedings of the Second International Workshop on Sequence Design and its Applications in Communications (IWSDA'05)*, to appear.

[12] N. Brandstätter and A. Winterhof, "Linear complexity profile of binary sequences with small correlation measure", preprint 2005.

[13] T.W. Cusick, C. Ding and A. Renvall, *Stream ciphers and number theory*, Revised edition. North-Holland Mathematical Library, 66. Elsevier Science B.V., Amsterdam, 2004.

[14] C. Ding, G. Xiao and W. Shan, *The stability theory of stream ciphers*, Lecture Notes in Computer Science, Vol. 561, Springer-Verlag, Berlin 1991.

[15] G. Dorfer, W. Meidl and A. Winterhof, "Counting functions and expected values for the lattice profile at n", Finite Fields Appl., Vol. 10, 636–652 (2004).

[16] G. Dorfer and A. Winterhof, "Lattice structure and linear complexity profile of nonlinear pseudorandom number generators", Appl. Algebra Engrg. Comm. Comput., Vol. 13, 499–508 (2003).

[17] J. Eichenauer, H. Grothe, J. Lehn and A. Topuzoğlu, "A multiple recursive nonlinear congruential pseudo random number generator", Manuscripta Math., Vol. 59, 331–346 (1987).

[18] J. Eichenauer and J. Lehn, "A nonlinear congruential pseudorandom number generator", Statist. Hefte, Vol. 27, 315–326 (1986).

[19] J. Eichenauer-Herrmann, "Statistical independence of a new class of inversive congruential pseudorandom numbers", Math. Comp., Vol. 60, 375–384 (1993).

[20] Y.-C. Eun, H.-Y. Song and M.G. Kyureghyan, "One-error linear complexity over $\mathbb{F}_p$ of Sidelnikov sequences", *Sequences and Their Applications SETA 2004*, Lecture Notes in Comput. Sci., Vol. 3486, 154–165 (2005).

[21] M. Flahive and H. Niederreiter, "On inversive congruential generators for pseudorandom numbers", *Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991)*, Lecture Notes in Pure and Appl. Math., Vol. 141, 75–80 (1993).

[22] É. Fouvry, P. Michel, J. Rivat and A. Sárközy, "On the pseudorandomness of the signs of Kloosterman sums", J. Aust. Math. Soc., Vol. 77, 425–436 (2004).

[23] J.B. Friedlander, C. Pomerance and I. Shparlinski, "Period of the power generator and small values of Carmichael's function", Math. Comp., Vol. 70, 1591–1605 (2001).

[24] J.B. Friedlander, C. Pomerance and I. Shparlinski, "Corrigendum to: Period of the power generator and small values of Carmichael's function", Math. Comp., Vol. 71, 1803–1806 (2002).

[25] J.B. Friedlander and I. Shparlinski, "On the distribution of the power generator", Math. Comp., Vol. 70, 1575–1589 (2001).

[26] R.A. Games and A.H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n", IEEE Trans. Inform. Theory, Vol. 29, 144–146 (1983).

[27] M.Z. Garaev, F. Luca, I. Shparlinski and A. Winterhof, "On the lower bound of the linear complexity over $\mathbb{F}_p$ of Sidelnikov sequences", preprint 2005.

[28] D. Gomez-Perez, J. Gutierrez and I. Shparlinski, "Exponential sums with Dickson polynomials", Finite Fields Appl., Vol. 12, 16-25 (2006).

[29] F. Griffin, H. Niederreiter and I. Shparlinski, "On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders", *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, Lecture Notes in Comput. Sci., Vol. 1719, 87–93 (1999).

[30] F. Griffin and I. Shparlinski,"On the linear complexity profile of the power generator", IEEE Trans. Inform. Theory, Vol. 46, 2159–2162 (2000).

[31] J. Gutierrez and D. Gomez-Perez, "Iterations of multivariate polynomials and discrepancy of pseudorandom numbers", *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, Lecture Notes in Comput. Sci., Vol. 2227, 192–199 (2001).

[32] J. Gutierrez, I. Shparlinski and A. Winterhof, "On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators", IEEE Trans. Inform. Theory, Vol. 49, 60–64 (2003).

[33] K. Gyarmati, "On a family of pseudorandom binary sequences", Period. Math. Hungar., Vol. 49, 45–63 (2004).

[34] F. Hess and I. Shparlinski, "On the linear complexity and multidimensional distribution of congruential generators over elliptic curves", Des. Codes and Cryptogr., Vol. 35, 111–117 (2005).

[35] D. Jungnickel, *Finite fields. Structure and arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[36] A. Klapper, "The vulnerability of geometric sequences based on fields of odd characteristic", J. Cryptology, Vol. 7, 33–51 (1994).

[37] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, Berlin Heidelberg, 1998.

[38] D.R. Kohel and I. Shparlinski, "On exponential sums and group generators for elliptic curves over finite fields", *Algorithmic number theory (Leiden, 2000)*, Lecture Notes in Comput. Sci., Vol. 1838, 395–404 (2000).

[39] S. Konyagin, T. Lange and I. Shparlinski, "Linear complexity of the discrete logarithm", Des. Codes Cryptogr., Vol. 28, 135–146 (2003).

[40] T. Lange and I. Shparlinski, "Certain exponential sums and random walks on elliptic curves", Canad. J. Math., Vol. 57, 338–350 (2005).

[41] R. Lidl, G.L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, 65. Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[42] J.L. Massey and S. Serconek, "Linear complexity of periodic sequences: a general theory", *Advances in cryptology—CRYPTO '96 (Santa Barbara, CA)*, Lecture Notes in Comput. Sci., Vol. 1109, 358–371 1996.

[43] C. Mauduit and A. Sárközy, "On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol", Acta Arith., Vol. 82, 365–377 (1997).

[44] W. Meidl, "How many bits have to be changed to decrease the linear complexity?", Des. Codes Cryptogr., Vol. 33, 109–122 (2004).

[45] W. Meidl, "Linear complexity and k-error linear complexity for p^n-periodic sequences", *Coding, cryptography and combinatorics*, Progr. Comput. Sci. Appl. Logic, Vol. 23, 227–235 (2004).

[46] W. Meidl and A. Winterhof, "Lower bounds on the linear complexity of the discrete logarithm in finite fields", IEEE Trans. Inform. Theory, Vol. 47, 2807–2811 (2001).

[47] W. Meidl and A. Winterhof, "Linear complexity and polynomial degree of a function over a finite field", *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, Springer, Berlin, 229–238 (2002).

[48] W. Meidl and A. Winterhof, "On the linear complexity profile of explicit nonlinear pseudorandom numbers", Inform. Process. Lett., Vol. 85, 13–18 (2003).

[49] W. Meidl and A. Winterhof, "On the linear complexity profile of some new explicit inversive pseudorandom numbers", J. Complexity, Vol. 20, 350–355 (2004).

[50] W. Meidl and A. Winterhof, "On the autocorrelation of cyclotomic generators", *Finite fields and applications*, Lecture Notes in Comput. Sci., Vol. 2948, 1–11 (2004).

[51] W. Meidl and A. Winterhof, "Some notes on the linear complexity of Sidelnikov-Lempel-Cohn-Eastman sequences", Designs, Codes and Cryptography, to appear.

[52] W. Meidl and A. Winterhof, "On the linear complexity profile of nonlinear pseudorandom number generators with Rédei functions", Finite Fields Appl., to appear.

[53] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, CBMS-NSF Regional Conference Series in Applied Mathematics, Vol. 63. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[54] H. Niederreiter, "Constructions of (t, m, s)-nets", *Monte Carlo and quasi-Monte Carlo methods 1998 (Claremont, CA)*, Springer, Berlin, 70–85 (2000).

[55] H. Niederreiter, "Linear complexity and related complexity measures for sequences", *Progress in cryptology—INDOCRYPT 2003*, Lecture Notes in Comput. Sci., Vol. 2904, 1–17 (2003).

[56] H. Niederreiter, "Constructions of (t, m, s)-nets and (t, s)-sequences", Finite Fields Appl., Vol. 11, 578–600 (2005).

[57] H. Niederreiter and I. Shparlinski, "On the distribution and lattice structure of nonlinear congruential pseudorandom numbers", Finite Fields Appl., Vol. 5, 246–253 (1999).

[58] H. Niederreiter and I. Shparlinski, "On the distribution of inversive congruential pseudorandom numbers in parts of the period", Math. Comp., Vol. 70, 1569–1574 (2001).

[59] H. Niederreiter and I. Shparlinski, "Recent advances in the theory of nonlinear pseudorandom number generators", *Monte Carlo and quasi-Monte Carlo methods, 2000 (Hong Kong)*, Springer, Berlin, 86–102 (2002).

[60] H. Niederreiter and I. Shparlinski, "On the average distribution of inversive pseudorandom numbers", Finite Fields Appl., Vol. 8, 491–503 (2002).

[61] H. Niederreiter and A. Winterhof, "Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators", Acta Arith., Vol. 93, 387–399 (2000).

[62] H. Niederreiter and A. Winterhof, "On the distribution of some new explicit nonlinear congruential pseudorandom numbers", *Sequences and Their Applications SETA 2004*, Lecture Notes in Comput. Sci., Vol. 3486, 266–274, (2005).

[63] R. Nöbauer, "Rédei-Permutationen endlicher Körper", *Contributions to general algebra, 5 (Salzburg, 1986)*, Hölder-Pichler-Tempsky, Vienna, 235–246 (1987).

[64] W.M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, 1976.

[65] I. Shparlinski, "On the linear complexity of the power generator", Des. Codes Cryptogr., Vol. 23, 5–10 (2001).

[66] I. Shparlinski, *Cryptographic applications of analytic number theory. Complexity lower bounds and pseudorandomness*, Progress in Computer Science and Applied Logic, 22. Birkhäuser Verlag, Basel, 2003.

[67] I. Shparlinski and A. Winterhof, "On the linear complexity of bounded integer sequences over different moduli", Inform. Process. Lett., Vol. 96, 175-177 (2005).

[68] V.M. Sidel'nikov, "Some k-valued pseudo-random sequences and nearly equidistant codes", Problems of Information Transmission, Vol. 5, 12–16 (1969); translated from Problemy Peredači Informacii, Vol. 5, 16–22 (1969), (Russian).

[69] M. Stamp and C.F. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n", IEEE Trans. Inform. Theory, Vol. 39, 1398–1401 (1993).

[70] A. Tietäväinen, "Vinogradov's method and some applications", *Number theory and its applications (Ankara, 1996)*, Lecture Notes in Pure and Appl. Math., Vol. 204, 261–282 (1999).

[71] A. Topuzoğlu and A. Winterhof, "On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders", Appl. Algebra Engrg. Comm. Comput., Vol. 16, 219–228 (2005).

[72] A. Topuzoğlu and A. Winterhof, "On the distribution of inversive congruential pseudorandom number generators of higher orders with largest possible period", preprint 2006.

[73] R.J. Turyn, "The linear generation of Legendre sequence", J. Soc. Indust. Appl. Math., Vol. 12, 115–116 (1964).

[74] I.M. Vinogradov, *Elements of number theory*, Dover Publications, Inc., New York, 1954.

[75] Y. Wang, "Linear complexity versus pseudorandomness: on Beth and Dai's result", *Advances in cryptology—ASIACRYPT'99 (Singapore)*, Lecture Notes in Comput. Sci., Vol. 1716, 288–298 (1999).

[76] A. Winterhof, "A note on the linear complexity profile of the discrete logarithm in finite fields", *Coding, cryptography and combinatorics*, Progr. Comput. Sci. Appl. Logic, Vol. 23, 359–367 (2004).

[77] A. Winterhof, "On the distribution of some new explicit inversive pseudorandom numbers and vectors", *Proceedings MC2QMC 2004*, to appear.

[78] G. Xiao and S. Wei, "Fast algorithms for determining the linear complexity of period sequences", *Progress in cryptology - INDOCRYPT 2002. Third international conference on cryptology in India, Hyderabad, India, December 16-18, 2002*, Lect. Notes in Comput. Sci., Vol. 2551, 12-21, (2002).

[79] G. Xiao, S. Wei, K.Y. Lam and K. Imamura, "A fast algorithm for determining the linear complexity of a sequence with period p^n over $\mathrm{GF}(q)$", IEEE Trans. Inform. Theory, Vol. 46, 2203–2206 (2000).