

# Chapter 1

## LINEAR COMPLEXITY AND RELATED COMPLEXITY MEASURES

ARNE WINTERHOF

*Johann Radon Institute for Computational and Applied Mathematics,  
Austrian Academy of Sciences,  
Altenbergerstr. 69, 4040 Linz, Austria  
arne.winterhof@oeaw.ac.at*

The linear complexity of a sequence is not only a measure for the unpredictability and thus suitability for cryptography but also of interest in information theory because of its close relation to the Kolmogorov complexity. However, in contrast to the Kolmogorov complexity the linear complexity is computable and so of practical significance.

It is also linked to coding theory. On the one hand, the linear complexity of a sequence can be estimated in terms of its correlation and there are strong ties between low correlation sequence design and the theory of error-correcting codes. On the other hand, the linear complexity can be calculated with the Berlekamp–Massey algorithm which was initially introduced for decoding BCH-codes.

This chapter surveys several mainly number theoretic methods for the theoretical analysis of the linear complexity and related complexity measures and describes several classes of particularly interesting sequences with high linear complexity.

### 1.1. Introduction

A sequence  $(s_n)$  of elements of the finite field  $\mathbb{F}_q$  of  $q$  elements is called a (*homogeneous*) *linear recurring sequence of order  $k$*  if there exist  $c_0, c_1, \dots, c_{k-1}$  in  $\mathbb{F}_q$ , satisfying the *linear recurrence of order  $k$  over  $\mathbb{F}_q$* ;

$$s_{n+k} = c_{k-1}s_{n+k-1} + c_{k-2}s_{n+k-2} + \dots + c_0s_n, \quad n = 0, 1, \dots \quad (1.1)$$

Now let  $(s_n)$  be a sequence over  $\mathbb{F}_q$ . 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  $\mathbb{F}_q$  is the sequence  $L(s_n, N)$ ,

$N \geq 1$ , where its  $N$ th term is defined to be the smallest  $L$  such that a linear recurrence of order  $L$  over  $\mathbb{F}_q$  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 over  $\mathbb{F}_q$*  of the sequence  $(s_n)$ . For the linear complexity of any periodic sequence of period  $t$  one can easily verify 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 Sec. 1.3. 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”

$$s_{n+1} = as_n + b, \tag{1.2}$$

for  $a, b \in \mathbb{F}_q$ ,  $a \neq 0$ , and some initial value  $s_0 \in \mathbb{F}_q$ , which satisfies  $L(s_n) \leq 2$ .

The expected values of linear complexity and linear complexity profile show that a “random” sequence should have  $L(s_n, N)$  close to  $\min\{N/2, t\}$  for all  $N \geq 1$ , see Sec. 1.4.

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 favorable properties). We illustrate such constructions. One would also like to find lower bounds for widely used sequences in order to judge whether it is reasonable to use them for cryptographic purposes. We present lower bounds and exact values of the linear complexity (profile) of many interesting sequences in Sec. 1.5.

Several other quality measures for sequences in view of different applications are closely related to linear complexity including the  $k$ -error linear complexity and the correlation measure of order  $k$ . We give an overview on these measures and their relations to linear complexity in Sec. 1.6.

## 1.2. Background

The *Kolmogorov complexity* is the central topic in *algorithmic information theory*. 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 [5, 69]. Kolmogorov complexity and linear complexity are the same for almost all sequences over  $\mathbb{F}_2$  of sufficiently (but only moderately) large length. In contrast to the linear complexity, the Kolmogorov complexity is in general not computable and so of no practical significance. The linear complexity (profile) is not only of theoretical interest, but can also be obtained algorithmically with the Berlekamp–Massey algorithm, see Sec. 1.3, which was initially introduced for decoding BCH-codes.

Mainly, the linear complexity (profile) is an important cryptographic characteristic of sequences (see the monographs and survey [9, 49, 50, 52, 56, 66]). A low linear complexity profile has turned out to be undesirable for cryptographical applications as stream ciphers.

**Example 1.1 (Stream Cipher).** We consider a message  $m_0, m_1, \dots$  represented as a sequence over  $\mathbb{F}_q$ . In a stream cipher each message symbol  $m_j$  is enciphered with an element  $x_j$  of another sequence  $x_0, x_1, \dots$  over  $\mathbb{F}_q$ , the key stream, by

$$c_j = m_j + x_j.$$

The cipher text  $c_0, c_1, \dots$  can be deciphered by subtracting the key stream

$$m_j = c_j - x_j.$$

The security of such a stream cipher depends on the unpredictability of the key stream. Since a sequence of small linear complexity is highly predictable, a high linear complexity of the sequence  $(x_n)$  is necessary (but not sufficient).

Sequences with low linear complexity are shown to be unsuitable for some applications using quasi-Monte Carlo methods as well (see [51–53, 66]). The following example describes a typical quasi-Monte-Carlo application.

**Example 1.2 (Quasi-Monte-Carlo Calculation of  $\pi$ ).**

(1) Choose  $N$  pairs of a sequence  $(x_n)$  in  $[0, 1)$

$$(x_n, x_{n+1}) \in [0, 1)^2, \quad n = 0, \dots, N - 1.$$

- (2) Count the number  $K$  of pairs  $(x_n, x_{n+1})$  in the unit circle.
- (3) Approximate  $\pi$  by  $\frac{4K}{N}$ .

Note that sequences in  $[0, 1)$  can easily be derived from sequences over  $\mathbb{F}_q$ , see Sec. 1.7.

In [8] the linear complexity profile of a given binary sequence is estimated in terms of its *correlation measure of order  $k$*  which was introduced by Mauduit and Sárközy [38] and is closely related to its *autocorrelation*, see Sec. 1.6.4. There are strong ties between low correlation sequence design and the theory of error-correcting codes, see [27]. Good error-correcting codes very often correspond to a sequence with low correlation (and large linear complexity).

### 1.3. The Berlekamp–Massey Algorithm

The proof of the following Theorem contains the Berlekamp–Massey algorithm (see [4, 35] and also e.g. [30]).

**Theorem 1.1.** *If  $L(s_n, N) > N/2$ , then we have*

$$L(s_n, N + 1) = L(s_n, N).$$

*If  $L(s_n, N) \leq N/2$ , then we have either*

$$L(s_n, N + 1) = L(s_n, N),$$

*or*

$$L(s_n, N + 1) = N + 1 - L(s_n, N).$$

**Proof.** Put  $L := L(s_n, N)$ . Then there are  $c_0, \dots, c_{L-1} \in \mathbb{F}_q$  with

$$s_{n+L} = c_{L-1}s_{n+L-1} + \dots + c_0s_n, \quad 0 \leq n \leq N - L - 1.$$

If the same recurrence holds for  $n = N - L$  as well then we have  $L(s_n, N + 1) = L(s_n, N)$ . Otherwise put

$$\lambda := s_N - c_{L-1}s_{N-1} - \dots - c_0s_{N-L} \neq 0.$$

Put  $a_n := s_n$  for  $n = 0, \dots, N - 1$  and  $a_N := s_N - \lambda$ , so we have

$$\begin{aligned} N + 1 &= L(s_n - a_n, N + 1) \leq L(s_n, N + 1) + L(-a_n, N + 1) \\ &= L(s_n, N + 1) + L(a_n, N + 1) = L(s_n, N + 1) + L(s_n, N). \end{aligned}$$

Hence we have

$$L(s_n, N + 1) \geq \max(L(s_n, N), N + 1 - L(s_n, N)).$$

The equality is proven by induction. For  $N = 1$ , the equality is obvious and we assume  $N > 1$ .

If  $L(s_n, N) = L(s_n, N - 1) = \dots = L(s_n, 1) = 0$ , then we have  $s_n = 0$  for  $0 \leq n \leq N - 1$ . Since  $s_N \neq 0$  we get  $L(s_n, N + 1) = N + 1$ .

If  $L(s_n, N) = L(s_n, N - 1) = \dots = L(s_n, 1) = 1$ , then is  $s_{n+N} = s_N s_0^{-1} s_n$  the desired linear recurrence.

We may assume that there is  $1 \leq M \leq N - 1$  with

$$L(s_n, N) = L(s_n, N - 1) = \dots = L(s_n, M + 1) > L(s_n, M).$$

By induction we have  $L(s_n, M) = M + 1 - L$ . Let

$$s_{n+M+1-L} = d_{M-L}s_{n+M-L} + \dots + d_0s_n, \quad 0 \leq n \leq L - 2,$$

and put

$$\mu := s_M - d_{M-L}s_{M-1} - \dots - d_0s_{L-1} \neq 0.$$

If  $L > N/2$  then

$$\begin{aligned} s_{n+L} &= c_{L-1}s_{n+L-1} + \dots + c_0s_n \\ &+ \lambda\mu^{-1}(s_{n+M-N+L} - d_{M-L}s_{n+M-N+L-1} - \dots - d_0s_{n-N+2L-1}), \end{aligned} \quad 0 \leq n \leq N - L,$$

is a linear recurrence of order  $L$ , and if  $L \leq N/2$  then

$$\begin{aligned} s_{n+N+1-L} &= c_{L-1}s_{n+N-L} + \dots + c_0s_{n+N-2L+1} \\ &+ \lambda\mu^{-1}(s_{n+M-L+1} - d_{M-L}s_{n+M-L} - \dots - d_0s_n), \end{aligned} \quad 0 \leq n \leq L - 1,$$

is a linear recurrence of length  $N + 1 - L$  for the first  $N + 1$  sequence elements. □

The proof is constructive and provides an algorithm for the calculation of the linear complexity profile including the corresponding linear recurrences.

**Example 1.3.** Consider the finite sequence  $(s_0, \dots, s_9) = (1101011101)$  over  $\mathbb{F}_2$ . Then we have

$N$	$L(s_n, N)$	
1	1	---
2	1	$s_{n+1} = s_n$
3	2	$s_{n+2} = s_{n+1} + s_n$ or $s_{n+2} = 0$
4	2	$s_{n+2} = s_{n+1} + s_n$
5	3	$s_{n+3} = s_{n+1}$ or $s_{n+3} = s_{n+2} + s_n$
6	3	$s_{n+3} = s_{n+1}$
7	4	$s_{n+4} = s_{n+1} + s_n$ or $s_{n+4} = s_{n+3} + s_n$
8	4	$s_{n+4} = s_{n+1} + s_n$
9	5	$s_{n+5} = s_{n+4} + s_{n+3} + s_{n+2} + s_{n+1} + s_n$ or $s_{n+5} = s_{n+3} + s_{n+2}$
10	5	$s_{n+5} = s_{n+4} + s_{n+3} + s_{n+2} + s_{n+1} + s_n$ .

### 1.4. The Expected Value of the Linear Complexity Profile

In this section, we show that for a “random” sequence  $(s_n)$  the value  $L(s_n, N)$  is close to  $N/2$ .

**Lemma 1.1.** *If  $L(s_n, N) \leq N/2$  then there is a unique linear recurrence of shortest length for the first  $N$  sequence elements of  $(s_n)$ , i.e. for  $L := L(s_n, N)$  the coefficients  $c_0, \dots, c_{L-1} \in \mathbb{F}_q$  in (1.1) are uniquely defined.*

**Proof.** Assume we had two different linear recurrences of the form (1.1) for the first  $N$  sequence elements of  $(s_n)$  with coefficients  $c_0, \dots, c_{L-1}$ , respectively,  $d_0, \dots, d_{L-1}$ . Put

$$k := \max\{j \mid c_j \neq d_j\},$$

such that  $0 \leq k \leq L - 1$ . Comparing the right hand sides in (1.1) yields

$$(c_0 - d_0)s_n + \dots + (c_k - d_k)s_{n+k} = 0, \quad 0 \leq n \leq N - L - 1.$$

Since  $c_k - d_k \neq 0$  this is a linear recurrence of order  $k$  for the first  $N - (L - k)$  sequence elements of  $(s_n)$  and thus

$$L(s_n, N - (L - k)) \leq k. \tag{1.3}$$

Hence,  $L(s_n, N - (L - k)) < L(s_n, N)$  and there exists a smallest positive index  $j \leq L - k$  with  $L(s_n, N - (L - k) + j) > L(s_n, N - (L - k))$ . Applying

the second part of Theorem 1.1 gives

$$L(s_n, N - (L - k) + j) = N - (L - k) + j - L(s_n, N - (L - k)).$$

From (1.3) and  $L \leq N/2$  we get

$$L(s_n, N - (L - k) + j) \geq N - L + j \geq \frac{N}{2} + j.$$

Since  $N - (L - k) + j \leq N$  we have  $L(s_n, N) = L \geq N/2 + j$  in contradiction to  $L \leq N/2$ .  $\square$

Let  $A(N, L)$  be the number of finite sequences  $s_0, \dots, s_{N-1} \in \mathbb{F}_q$  of length  $N$  with  $L(s_n, N) = L$ .

**Lemma 1.2.** *We have*

$$A(N, 0) = 1$$

and

$$A(N, L) = (q - 1)q^{\min(2L-1, 2N-2L)}$$

for  $1 \leq L \leq N$ .

**Proof.** We prove the result by induction. It is trivial for  $N = 1$ . We assume the assertion for  $N$  and derive the formula for  $N + 1$ .

First we consider the case  $L := L(s_n, N + 1) \leq (N + 1)/2$ .

By Theorem 1.1, we can have  $L(s_n, N + 1) \leq (N + 1)/2$  only if  $L(s_n, N + 1) = L(s_n, N)$ . By Lemma 1.1, we have a unique linear recurrence to the sequence  $(s_0, \dots, s_{N-1})$  with  $L(s_n, N) = L$  which can be extended for exactly one choice of  $s_N \in \mathbb{F}_q$ . Hence we have

$$A(N + 1, L) = A(N, L),$$

and get the result by induction.

If  $L > (N + 1)/2$  then we have by Theorem 1.1

$$L = L(s_n, N + 1) = L(s_n, N) = \dots = L(s_n, L + j) = L + j - L(s_n, L + j - 1),$$

and thus  $L(s_n, L + j - 1) = j$  with some  $0 \leq j \leq N + 1 - L$ . Each sequence  $(s_n)$  with  $L(s_n, L + j - 1) = j$  corresponds to  $(q - 1)q^{N-L+1-j}$  sequences

with  $L(s_n, N + 1) = L$ . Summation over  $j$  and induction provide

$$\begin{aligned} A(N + 1, L) &= (q - 1) \sum_{j=0}^{N+1-L} q^{N-L+1-j} A(L + j - 1, j) \\ &= (q - 1)q^{N-L+1} + \sum_{j=1}^{N+1-L} (q - 1)^2 q^{N-L+1-j} q^{2j-1}, \end{aligned}$$

and thus the assertion. □

This Lemma was first proven by Gustavson [24]. The main result of this section can be found in [55, Proposition 4.2] for  $q = 2$  and for arbitrary  $q$  in the unpublished work [62] of Smeets.

**Theorem 1.2.** *The expected value for  $L(s_n, N)$  is*

$$\frac{1}{q^N} \sum_{L=0}^N A(N, L)L = \begin{cases} \frac{N}{2} + \frac{q}{(q+1)^2} - q^{-N} \frac{N(q+1)+q}{(q+1)^2} & \text{for even } N, \\ \frac{N}{2} + \frac{q^2+1}{2(q+1)^2} - q^{-N} \frac{N(q+1)+q}{(q+1)^2} & \text{for odd } N. \end{cases}$$

**Proof.** By the previous Lemma, we have

$$\begin{aligned} &\sum_{L=1}^N A(N, L)L \\ &= (q - 1) \sum_{L=1}^N q^{\min(2L-1, 2N-2L)} L \\ &= (q - 1) \left( \sum_{L=1}^{\lfloor N/2 \rfloor} q^{2L-1} L + \sum_{L=\lfloor N/2 \rfloor + 1}^N q^{2N-2L} L \right) \\ &= (q - 1) \left( \sum_{L=1}^{\lfloor N/2 \rfloor} q^{2L-1} \sum_{k=1}^L 1 + \sum_{L=\lfloor N/2 \rfloor + 1}^N q^{2N-2L} \right. \\ &\quad \left. \times \left( \lfloor N/2 \rfloor + \sum_{k=\lfloor N/2 \rfloor + 1}^L 1 \right) \right) \end{aligned}$$

$$\begin{aligned}
 &= (q - 1) \left( \sum_{k=1}^{\lfloor N/2 \rfloor} \sum_{L=k}^{\lfloor N/2 \rfloor} q^{2L-1} + \left\lfloor \frac{N}{2} \right\rfloor \sum_{L=\lfloor N/2 \rfloor+1}^N q^{2N-2L} \right. \\
 &\quad \left. + \sum_{k=\lfloor N/2 \rfloor+1}^N \sum_{L=k}^N q^{2N-2L} \right) \\
 &= \sum_{k=1}^{\lfloor N/2 \rfloor} \frac{q^{2\lfloor N/2 \rfloor+2} - q^{2k}}{q^2 + q} + \left\lfloor \frac{N}{2} \right\rfloor \frac{q^{2(N-\lfloor N/2 \rfloor)} - 1}{q + 1} \\
 &\quad + \sum_{k=\lfloor N/2 \rfloor+1}^N \frac{q^{2(N-k+1)} - 1}{q + 1} \\
 &= \left\lfloor \frac{N}{2} \right\rfloor \frac{q}{q + 1} q^{2\lfloor N/2 \rfloor} - \frac{q}{q + 1} \frac{q^{2\lfloor N/2 \rfloor} - 1}{q^2 - 1} + \left\lfloor \frac{N}{2} \right\rfloor \frac{q^{2(N-\lfloor N/2 \rfloor)} - 1}{q + 1} \\
 &\quad + \frac{q^{2(N-\lfloor N/2 \rfloor+1)} - q^2}{(q + 1)(q^2 - 1)} - \frac{N - \lfloor N/2 \rfloor}{q + 1},
 \end{aligned}$$

which implies the assertion. □

For results on the expected value of periodic sequences see [41].

### 1.5. Lower Bounds for Linear Complexity and Linear Complexity Profile

In this section, we describe some methods for determining or estimating the linear complexity (profile) and present results for several interesting classes of sequences.

#### 1.5.1. Explicit Non-linear Pseudorandom Numbers

It is possible to express linear complexity in connection with various invariants of the sequences at hand.

In case of a  $q$ -periodic sequence  $(\xi_n)$  over  $\mathbb{F}_q$ , linear complexity is related to the degree of the polynomial  $g(X) \in \mathbb{F}_q[X]$  representing the sequence  $(\xi_n)$ . We recall that the polynomial  $g(X)$  can be uniquely determined as follows: Consider a fixed ordered basis  $\{\beta_1, \dots, \beta_r\}$  of  $\mathbb{F}_q$  over  $\mathbb{F}_p$ , and for  $n = n_1 + n_2p + \dots + n_r p^{r-1}$  with  $0 \leq n_k < p, 1 \leq k \leq r$ , order the elements of  $\mathbb{F}_q$  as

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

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

$$\xi_n = g(\zeta_n), \quad 0 \leq n \leq q - 1. \quad (1.4)$$

When  $q = p$  (and  $\beta_1 = 1$ ) these sequences are called *explicit non-linear congruential generators* and we have

$$L(\xi_n) = \deg g + 1 \quad (1.5)$$

(for a proof, see [6, Theorem 8]). For a prime power  $q$  they are named *explicit non-linear digital generators*. In general (1.5) is not valid for  $r \geq 2$ . Meidl and Winterhof [43] 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  $(\xi_n)$  see Meidl and Winterhof [44].

A similar relation is valid for  $t$ -periodic sequences over  $\mathbb{F}_q$  where  $t$  divides  $q - 1$ . For a  $t$ -periodic sequence  $(\omega_n)$  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 non-zero coefficients of  $f$  (see [30]). Lower bounds for the linear complexity profile in some special cases are given by Meidl and Winterhof in [45]. For a general study of sequences with arbitrary periods see Massey and Serconek [36].

The following sequences exhibit a particularly nice behavior with respect to the linear complexity profile. The *explicit inversive congruential generator*  $(z_n)$  was introduced by Eichenauer-Herrmann in [15]. The sequence  $(z_n)$  in this case is produced by the relation

$$z_n = (an + b)^{p-2}, \quad n = 0, \dots, p - 1, \quad z_{n+p} = z_n, \quad n \geq 0, \quad (1.6)$$

with  $a, b \in \mathbb{F}_p$ ,  $a \neq 0$ , and  $p \geq 5$ . (The name stems from the fact that  $n^{p-2} = n^{-1}$ ,  $0 \neq n \in \mathbb{F}_p$ .) It is shown in [44] that

$$L(z_n, N) \geq \begin{cases} (N - 1)/3, & 1 \leq N \leq (3p - 7)/2, \\ N - p + 2, & (3p - 5)/2 \leq N \leq 2p - 3, \\ p - 1, & N \geq 2p - 2. \end{cases} \quad (1.7)$$

We provide the proof of a slightly weaker result.

**Theorem 1.3.** Let  $(z_n)$  be as in (1.6), 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  $L$ ,

$$z_{n+L} = c_{L-1}z_{n+L-1} + \dots + c_0z_n, \quad 0 \leq n \leq N - L - 1, \quad (1.8)$$

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

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

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

For  $n \in C_L(N)$ , the recurrence (1.8) is equivalent to

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

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. □

Analogs of (1.7) for *digital inversive generators*, i.e. for  $r \geq 2$ , are also given in [44]. For *t-periodic inversive generators*, where  $t$  is a divisor of  $q-1$ , see [45].

We mention one more explicit non-linear generator, namely the *quadratic exponential generator*, introduced by Gutierrez *et al.* [25]. Given an element  $\vartheta \in \mathbb{F}_q^*$  we consider the sequence  $(q_n)$  where

$$q_n = \vartheta^{n^2}, \quad n = 0, 1, \dots$$

The lower bound

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

is obtained in [25]. Here the period  $t$  is at least  $\tau/2$  where  $\tau$  is the multiplicative order of  $\vartheta$ .

### 1.5.2. Recursive Non-linear Pseudorandom Numbers

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

$$u_{n+1} = f(u_n), \quad n \geq 0, \tag{1.9}$$

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

The following lower bound on the linear complexity profile of a non-linear congruential generator is given in [25].

**Theorem 1.4.** *Let  $(u_n)$  be as in (1.9), where  $f(X) \in \mathbb{F}_p[X]$  is of degree  $d \geq 2$ , then*

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

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

$$F_0(X) = X, \quad F_i(X) = F_{i-1}(f(X)), \quad i = 1, 2, \dots$$

It is clear that  $\deg(F_i) = d^i$  for every  $i = 1, 2, \dots$ . 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

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

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

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

is of degree  $d^L$  and has 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.  $\square$

For some special classes of polynomials much better results are available, see [23, 25, 58]. 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

$$y_{n+1} = ay_n^{p-2} + b = \begin{cases} ay_n^{-1} + b & \text{if } y_n \neq 0, \\ b & \text{otherwise,} \end{cases} \quad n \geq 0, \tag{1.10}$$

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

$$L(y_n, N) \geq \min \left\{ \frac{N - 1}{3}, \frac{t - 1}{2} \right\}, \quad N \geq 1. \tag{1.11}$$

This sequence, introduced by Eichenauer and Lehn [14], has succeeded in drawing significant attention due to some of its enchanting properties. In terms of the linear complexity profile, the lower bound (1.11) shows that the inversive generator is almost optimal. 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 [17] 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.* [19, 20].

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

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

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 non-linear congruential generators where  $f(X) = D_e(X, 1)$  is proven by Aly and Winterhof [1]. Here the period  $t$  is a divisor of  $p-1$  or  $p+1$ .

Another class of non-linear congruential pseudorandom number generators, where  $f(X)$  is a Rédei function, is analyzed by Meidl and Winterhof [48]. Suppose that

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

is an irreducible quadratic polynomial with the two different roots  $\xi$  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 Rédei function  $f_e(X)$  is a permutation of  $\mathbb{F}_p$  if and only if  $\gcd(e, p+1) = 1$ , see Nöbauer [54]. For further background on Rédei functions we refer to [34, 54]. 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  $\varphi(p+1)$ . 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 non-linear congruential pseudorandom number

generators (1.9). In [48] 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 [65];

$$u_{n+1} = f(u_n, u_{n-1}, \dots, u_{n-m+1}), \quad n = m - 1, m, \dots \quad (1.12)$$

Here initial values  $u_0, \dots, u_{m-1}$  are in  $\mathbb{F}_p$  and  $f \in \mathbb{F}_p(X_1, \dots, X_m)$  is a rational function in  $m$  variables over  $\mathbb{F}_p$ . The sequence (1.12) eventually becomes periodic with least period  $t \leq p^m$ . The fact that  $t$  can actually attain the value  $p^m$  gains non-linear 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 [65].

A particular rational function  $f$  in (1.12) gives rise to a generalization of the inversive generator (1.10), as described below. Let  $(x_n)$  be the sequence over  $\mathbb{F}_p$ , defined by the linear recurring sequence of order  $m + 1$ ;

$$x_{n+1} = a_0x_n + a_1x_{n-1} + \dots + a_mx_{n-m}, \quad n \geq m,$$

with  $a_0, a_1, \dots, a_m \in \mathbb{F}_p$  and initial values  $x_0, \dots, x_m \in \mathbb{F}_p$ . 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 non-linear generator  $(z_n)$  is produced by

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

(see Eichenauer *et al.* [13]). It is easy to see that  $(z_n)$  satisfies

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

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

$$f(X_1, \dots, X_m) = a_0 + a_1X_1^{-1} + \dots + a_mX_1^{-1}X_2^{-1} \cdots X_m^{-1}.$$

A sufficient condition for  $(z_n)$  to attain the maximal period length  $p^m$  is given in [13]. It is shown in [65] 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 (1.11), i.e. the case  $m = 1$ .

**1.5.3. Legendre Sequence and Related Bit Sequences**

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

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

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 [9, 67]. We give the proof here since the method is illustrative.

**Theorem 1.5.** *The linear complexity of the Legendre sequence is*

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

**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, [59, 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  $p \equiv \pm 1 \pmod 8$ . Next we have

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

Let  $Q$  and  $N$  denote the sets of quadratic residues and non-residues modulo  $p$ , respectively. If  $p \equiv \pm 1 \pmod 8$ , 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 using bounds on incomplete sums of Legendre symbols (cf. [59, Theorem 9.2]).

**Theorem 1.6.** *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

$$l_{n+L} = c_{L-1}l_{n+L-1} + \dots + c_0l_n, \quad 0 \leq n \leq N - L - 1,$$

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

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

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

$$\left| \sum_{n=1}^{N-L-1} \left( \frac{\prod_{j=0}^L (n+j)^{c_j}}{p} \right) \right| < (L+1)p^{1/2}(1+\log p), \tag{1.13}$$

yields

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

from which the assertion follows. The bound (1.13) can be proved as follows: For an integer  $k \geq 2$  put  $e_k(x) = \exp(2\pi i x/k)$ . The relations below can be found in [68];

$$\sum_{a=0}^{k-1} e_k(au) = \begin{cases} 0, & u \not\equiv 0 \pmod k, \\ k, & u \equiv 0 \pmod k, \end{cases} \tag{1.14}$$

$$\sum_{a=1}^{k-1} \left| \sum_{x=0}^{K-1} e_k(ax) \right| \leq k \log k, \quad 1 \leq K \leq k. \tag{1.15}$$

The Weil bound, which we present in the following form (see [57, Theorems 2C and 2G]),

$$\left| \sum_{a=0}^{p-1} \chi(f(a))e_p(ax) \right| \leq \begin{cases} p^{1/2} \deg f, & 1 \leq x < p, \\ p^{1/2}(\deg f - 1), & x = 0, \end{cases} \tag{1.16}$$

where  $\chi$  denotes a non-trivial 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 [64]) with (1.14) and

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

gives

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

where we used that  $f$  is not a square (since  $c_L = 1$ ) to apply (1.16) 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 [33, 42, 70].

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

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

In many cases one is able to determine the linear complexity  $L(\sigma_n)$  over  $\mathbb{F}_2$  exactly, see Meidl and Winterhof [47]. 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 [47],

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

where  $f(n) = \Omega(g(n))$  means that  $f(n) \geq cg(n)$  for all sufficiently large  $n$  and some constant  $c > 0$ . The linear complexity over  $\mathbb{F}_p$  of this sequence has been estimated in Garaev *et al.* [22] 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

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

and

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

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 *generalized cyclotomic sequence of order 2*) (see [7, 9]; Chapter 8.2). Under the restriction  $\gcd(p - 1, q - 1) = 2$  it satisfies

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

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  $2 \leq N < pq$ , where  $f(n) = O(g(n))$  is equivalent to  $f(n) \leq cg(n)$  for all sufficiently large  $n$  and some constant  $c > 0$ .

### 1.5.4. Elliptic Curve Generators

We recall some definitions and basic facts about elliptic curves (see [32] or Chapter 5).

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

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

with coefficients  $a, b \in \mathbb{F}_p$  such that  $4a^3 + 27b^2 \neq 0$ . 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

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

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  $w_n = f(W_n)$ ,  $n \geq 0$ , where

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

Obviously,  $(w_n)$  is  $t$ -periodic. See [3, 28] 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 [28] 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, see [66]. Let  $x(Q)$  denote the first coordinate  $x$  of the point  $Q = (x, y) \in E$ .

**Theorem 1.7.** *Let  $(w_n)$  be the  $t$ -periodic sequence defined by*

$$w_n = x(nG), \quad 1 \leq n \leq t - 1, \tag{1.17}$$

*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

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

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

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

and hence

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

So we get

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

Clearing denominators we get

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

$$L + 1 \leq n \leq N - L - 1.$$

So the polynomial

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

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

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

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

## 1.6. Related Measures

### 1.6.1. 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  $s \geq 1$ , spanned by the vectors  $\mathbf{s}_n - \mathbf{s}_0$ ,  $n = 1, 2, \dots$ , where

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

We recall that  $(s_n)$  is said to pass the *s-dimensional lattice test* for some  $s \geq 1$ , if  $\mathcal{L}(s_n, s) = \mathbb{F}_q^s$ . It is obvious for example that the linear generator (1.2) can pass the *s-dimensional lattice test* at most for  $s = 1$ . On the other hand for  $q = p$ , the non-linear generator (1.4) passes the test for all  $s \leq \deg g$  (see [51]). 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 [51].

Accordingly the notion of *lattice profile at N* is introduced by Dorfer and Winterhof [12]. 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 [12] shows:

We have either

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

or

$$(1.18)$$

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

The results of Dorfer *et al.* [11] on the expected value of the lattice profile show that a “random” sequence should have  $S(s_n, N)$  close to  $\min\{N/2, t\}$ .

### 1.6.2. *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 [10, 63].

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  $(s_0, s_1, \dots, s_{t-1})$  and  $(y_0, y_1, \dots, y_{t-1})$  is at most  $k$ .

One problem of interest here is to determine the minimum value  $k$ , for which  $L_k(s_n) \leq L(s_n)$ . This problem is tackled by Meidl [39], 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 [39] also describes an algorithm to determine the *k*-error linear complexity that is based on an algorithm of [72]. Stronger results for  $p^n$ -periodic sequences over  $\mathbb{F}_p$  have been recently obtained in Meidl [40].

In Klapper [31] an attack is discussed, where the idea is to decrease the linear complexity of a given sequence by considering it over a field which is different from the field where the sequence is naturally defined (and its high linear complexity is guaranteed). Although the result in Shparlinski and Winterhof [60] shows that this approach has very limited chance to succeed it is still important to analyze the (*k*-error) linear complexity of a sequence over different fields. Since Legendre sequences are constructed using properties of  $\mathbb{F}_p$  it is somewhat natural to consider them not only over  $\mathbb{F}_2$  but also over  $\mathbb{F}_p$ .

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

**Theorem 1.8.** Let  $L_k(l_n)$  denote the  $k$ -error linear complexity over  $\mathbb{F}_p$  of the Legendre sequence  $(l_n)$ . Then,

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

**Proof.** Put

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

Since  $l_n = g_1(n)$  for  $n \geq 0$  we get that the Legendre sequence  $(l_n)$  over  $\mathbb{F}_p$  has linear complexity  $L(l_n) = p$  by (1.5).

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

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

and

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

Assume now that  $1 \leq k \leq (p - 3)/2$ . 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.  $s_n = g(n)$ ,  $n \geq 0$ .

It is obvious that the sequences  $(s_n)$  and  $(l'_n)$  coincide for at least  $p - 1 - k \geq (p + 1)/2$  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  $\deg g \geq (p + 1)/2$ . Therefore,  $L_k(l_n) = L(l'_n) = (p + 1)/2$ .

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

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,

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

For  $k \geq (q - 1)/2$  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 [16] to

be

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

### 1.6.3. *Non-linear Complexity Profile*

We recall that the *non-linear 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

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

with a polynomial  $\Psi(\lambda_1, \dots, \lambda_k)$  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

$$L(s_n, N) \geq NL_1(s_n, N) \geq NL_2(s_n, N) \geq \dots$$

See [25] for the presentation of results on the linear complexity profile of non-linear, inversive, and quadratic exponential generators in a more general form, namely in terms of lower bounds on the non-linear complexity profile.

### 1.6.4. *Autocorrelation and Related Distribution Measures for Binary Sequences*

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  $1 \leq k \leq t - 1$ .

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

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

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

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

For the Legendre sequences, for example,  $A(l_n, k)$  can be immediately derived from the well-known formula, see e.g. [30]

$$\sum_{n=0}^{p-1} \binom{n}{p} \binom{n+k}{p} = -1, \quad 1 \leq k \leq p - 1,$$

and the following bound on the aperiodic autocorrelation of Legendre sequences follows immediately from (1.13).

**Theorem 1.9.** *The (aperiodic) autocorrelation of the Legendre sequence satisfies*

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

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

For bounds on the aperiodic autocorrelation of extended Legendre sequences see [46]. For the aperiodic autocorrelation of Sidelnikov sequences see [61] and of the two-prime generator see [7].

In Mauduit and Sárközy [38] the *correlation measure of order k* of a binary sequence  $(s_n)$  is introduced as

$$C_k(s_n) = \max_{M,D} \left| \sum_{n=0}^{M-1} (-1)^{s_{n+d_1}} \dots (-1)^{s_{n+d_k}} \right|, \quad k \geq 1,$$

where the maximum is taken over all  $D = (d_1, d_2, \dots, d_k)$  with non-negative integers  $d_1 < d_2 < \dots < d_k$  and  $M$  such that  $M - 1 + d_k \leq T - 1$ .  $C_2(s_n)$  is obviously bounded by the maximal absolute value of the aperiodic autocorrelation of  $(s_n)$ . (We remark that some of our references deal actually with the corresponding sequences  $s'_h = (-1)^{s_h}$  over  $\{-1, 1\}$  with the adequate definition of the correlation measure.)

It is also shown in [38] that the Legendre sequence has small correlation measure up to rather high orders.

The following family of pseudorandom binary sequences is introduced in Gyarmati [26]. Let  $p$  be an odd prime and  $g$  be a primitive root modulo  $p$ .

Denote by  $\text{ind } n$ , the *discrete logarithm* of  $n$  to the base  $g$ , i.e.  $\text{ind } n = j$  if  $n = g^j$  with  $1 \leq j \leq p-1$ . Let  $f(X)$  be a polynomial of degree  $k$  modulo  $p$ . Then the finite sequence  $(e'_n)$  is defined by

$$e'_n = \begin{cases} 1 & \text{if } 1 \leq \text{ind } f(n) \leq (p-1)/2, \\ -1 & \text{if } (p+1)/2 \leq \text{ind } f(n) \leq p-1 \text{ or } p \mid f(n), \end{cases} \quad 1 \leq n \leq p-1.$$

The correlation measure of the sequence  $(e_n)$  defined by  $e'_n = (-1)^{e_n}$  is also analyzed in [26].

The sequence  $(k'_n)$  of signs of Kloosterman sums is defined as follows;

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

where  $j^{-1}$  is the inverse of  $j$  modulo  $p$ . Bounds on the correlation measure of order  $k$  of  $(k_n)$  defined by  $k'_n = (-1)^{k_n}$  are given in Fouvry *et al.* [18].

Recently Brandstätter and Winterhof [8] have shown that the linear complexity profile of a given  $t$ -periodic sequence can be estimated in terms of its correlation measure;

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

Hence, a lower bound on  $L(s_n, N)$  can be obtained whenever an appropriate bound on  $\max C_k(s_n)$  is known.

### 1.6.5. Discrepancy

Let  $(x_n)$  be a sequence in the unit interval  $[0, 1)$ . For  $0 \leq d_1 < \dots < d_k < N$  we put

$$\mathbf{x}_n = \mathbf{x}_n(d_1, \dots, d_k) = (x_{n+d_1}, \dots, x_{n+d_k}), \quad 1 \leq n \leq N - d_k.$$

The *discrepancy* of the vectors  $\mathbf{x}_1(d_1, \dots, d_k), \dots, \mathbf{x}_{N-d_k}(d_1, \dots, d_k)$  is defined as

$$\sup_I \left| \frac{A(I, \mathbf{x}_1, \dots, \mathbf{x}_{N-d_k})}{N - d_k} - V(I) \right|,$$

where the supremum is taken over all subintervals of  $[0, 1]^k$ ,  $V(I)$  is the volume of  $I$  and  $A(I, \mathbf{x}_1, \dots, \mathbf{x}_{N-d_k})$  is the number of points  $\mathbf{x}_n$ ,  $n = 1, \dots, N - d_k$ , in the interval  $I$ .

We can derive a binary sequence  $(e_n)$  from  $(x_n)$  by  $e_n = 1$  if  $0 \leq x_n < 1/2$  and  $e_n = 0$  otherwise.

In [37, Theorem 1] the correlation measure of order  $k$  of  $(e_n)$  is estimated in terms of the above discrepancy of vectors derived from the sequence  $(x_n)$ . Hence, using the relation between linear complexity profile and correlation measure of  $(e_n)$  we can obtain (weak) linear complexity profile lower bounds for  $(e_n)$  from discrepancy upper bounds for  $(x_n)$ .

### 1.7. Thoughts for Practitioners

Faster algorithms than the Berlekamp–Massey algorithm are known for sequences of particular periods [21, 71, 72].

The Legendre symbol needed for the generation of several sequences in Sec. 1.5.3 can be efficiently evaluated using the quadratic reciprocity law and its supplement.

Inversion is the most expensive operation in the generation of inversive generators. For fields  $\mathbb{F}_p$  of prime order we can use the Euclidean algorithm. For fields  $\mathbb{F}_{2^r}$  of characteristic 2 we recommend to use the Itoh-Tsujii algorithm [29] and an optimal normal basis representation [30].

For many practical applications, for example for quasi-Monte Carlo methods, we need sequences in the unit interval  $[0, 1)$  (or any other interval) instead of sequences over finite fields. However, we can derive a sequence  $(x_n)$  over  $[0, 1)$  from a sequence  $(\xi_n)$  over the finite field  $\mathbb{F}_q$  in the following way. We fix a basis  $\{\beta_1, \dots, \beta_r\}$  of  $\mathbb{F}_q$  over its prime field  $\mathbb{F}_p$ , i.e.  $q = p^r$ , and identify  $\mathbb{F}_p$  with the integers  $\{0, 1, \dots, p - 1\}$ . Then we derive from the element

$$\xi_n = c_1\beta_1 + \dots + c_r\beta_r, \quad c_1, \dots, c_r \in \mathbb{F}_p,$$

an integer

$$y_n = c_r + c_{r-1}p + \dots + c_0p^{r-1} \in \{0, 1, \dots, q - 1\}.$$

The sequence  $(x_n)$  over  $[0, 1)$  is obtained by

$$x_n = y_n/q.$$

### 1.8. Directions for Future Research

- (1) Find more recursive non-linear generators for which substantial better lower bounds on the linear complexity profile can be proven.
- (2) Find more classes of sequences over  $[0, 1)$  for which the discrepancy with arbitrary lags  $0 \leq d_1 < \dots < d_k$  and thus the linear complexity of the corresponding binary sequence can be estimated.
- (3) Extend the linear complexity profile lower bounds on the inversive generators of higher orders to arbitrary period.
- (4) Analyze finer lattice tests with arbitrary lags.
- (5) Find other quality measures which are related to linear complexity, e.g. the non-linearity of a Boolean function corresponding to a binary sequence.
- (6) Prove results on other quality measures for the Sidelnikov sequence where analog results for the Legendre sequence are known, e.g. for the merit factor.

### 1.9. Conclusions

In this survey, we pointed to the strong ties between the cryptographic quality measure linear complexity and information theory and coding theory. We presented several lower bounds and exact values on the linear complexity (profile) of particular interesting sequences over a finite field using several illustrative methods. Finally, we mentioned other quality measures for sequences and their relations to linear complexity.

### 1.10. Questions

- (1) Calculate the linear complexity profile of the finite sequence  $(s_0, \dots, s_9) = (1101011101)$  over  $\mathbb{F}_2$  using the Berlekamp–Massey algorithm.
- (2) Prove the following result which shows that lower bounds on the linear complexity profile provide upper bounds, as well.

Let  $(l_N)$  be a sequence with  $l_1 \leq 0$  and  $l_N \leq l_{N-1} + 1$  for  $N \geq 2$ . If

$$L(s_n, N) \geq l_N \quad \text{for } N \geq 2$$

then we have

$$L(s_n, N) \leq N - l_{N-1} \quad \text{for } N \geq 2.$$

Apply this result to get an upper bound on the linear complexity profile of the explicit inversive congruential generator of period  $p$ .

- (3) Let  $g$  be an element of  $\mathbb{F}_q$  of order  $t$  and  $a, b \in \mathbb{F}_q \setminus \{0\}$ . Prove a lower bound on the linear complexity profile of the sequence  $z_n = (ag^n + b)^{q-2}$ . Find conditions on  $a, b$  such that the bound is stronger than in the general case.
- (4) Prove the formula for the exact value of the linear complexity of the two prime generator.
- (5) Prove a lower bound on the linear complexity profile of the two-prime generator.
- (6) Prove the relation between linear complexity profile and correlation measure of order  $k$ .
- (7) Prove an upper bound on the correlation of order  $k$  of the Sidelnikov sequence and derive a lower bound on its linear complexity profile.
- (8) Use the lower bound on the explicit inversive congruential generator of period  $p$  to derive an upper bound on the lattice profile  $S(z_n, N)$ .
- (9) Find a sequence with large linear complexity but small 1-error linear complexity.
- (10) Find an integer sequence with large linear complexity over  $\mathbb{F}_p, p \geq 3$ , but with small linear complexity over  $\mathbb{F}_2$ .

Solutions:

(1)

$N$	$L(s_n, N)$	
1	1	---
2	1	$s_{n+1} = s_n$
3	2	$s_{n+2} = s_{n+1} + s_n$ or $s_{n+2} = 0$
4	2	$s_{n+2} = s_{n+1} + s_n$
5	3	$s_{n+3} = s_{n+1}$ or $s_{n+3} = s_{n+2} + s_n$
6	3	$s_{n+3} = s_{n+1}$
7	4	$s_{n+4} = s_{n+1} + s_n$ or $s_{n+4} = s_{n+3} + s_n$
8	4	$s_{n+4} = s_{n+1} + s_n$
9	5	$s_{n+5} = s_{n+4} + s_{n+3} + s_{n+2} + s_{n+1} + s_n$ or $s_{n+5} = s_{n+3} + s_{n+2}$
10	5	$s_{n+5} = s_{n+4} + s_{n+3} + s_{n+2} + s_{n+1} + s_n.$

- (2) For  $N = 2$  we trivially have  $L(s_n, N) \leq 2 \leq N - l_1$ . For  $N \geq 2$  by Theorem 1.1 we have either  $L(s_n, N + 1) = L(s_n, N) \leq N - l_{N-1} \leq N + 1 - l_N$  by induction, where we used the condition  $l_N \leq l_{N-1} + 1$ , or  $L(s_n, N + 1) = N + 1 - L(s_n, N) \leq N + 1 - l_N$ . For the inversive generator  $(z_n)$  we have  $l_N = \min\{(N-1)/3, (p-1)/2\}$  by Theorem 1.3 and get  $L(z_n, N) \leq N - \min\{(N-4)/3, (p-3)/2\}$ .

- (3) As in Theorem 1.3, we can prove  $L(z_n, N) \geq \min\{(N-1)/3, (t-1)/2\}$ . We get the stronger bound  $L(z_n, N) \geq \min\{N/2, t\}$  if  $-a^{-1}b$  is not in the subgroup of  $\mathbb{F}_q^*$  generated by  $g$ .
- (4) See [9, Theorem 8.2.9].
- (5) See [7].
- (6) See [8].
- (7) See [8].
- (8) Use Exercise 2 and (1.18).
- (9) A  $t$ -periodic sequence with exactly one non-zero entry has linear complexity  $t$  but 1-error linear complexity 0.
- (10) A  $t$ -periodic sequence with one entry 2 and all other entries 0 has linear complexity  $t$  over  $\mathbb{F}_p$ ,  $p \geq 3$ , but linear complexity 0 over  $\mathbb{F}_2$ .

### 1.11. Keywords

#### *Linear complexity (profile)*

For  $N \geq 1$  the *linear complexity profile*  $L(s_n, N)$  of a sequence  $(s_n)$  over  $\mathbb{F}_q$  is the shortest length  $L$  of a linear recurrence relation

$$s_{n+L} = c_{L-1}s_{n+L-1} + \cdots + c_0s_n, \quad 0 \leq n \leq N - L - 1,$$

over  $\mathbb{F}_q$  satisfied by the first  $N$  sequence elements. The *linear complexity*  $L(s_n)$  is defined by

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

#### *k-error linear complexity*

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  $(s_0, s_1, \dots, s_{t-1})$  and  $(y_0, y_1, \dots, y_{t-1})$  is at most  $k$ .

#### *Explicit non-linear congruential generator*

For a prime  $p$  and a polynomial  $f(X) \in \mathbb{F}_p[X]$  with  $2 \leq \deg(f) \leq p-1$  the *explicit non-linear congruential generator* is the  $p$ -periodic sequence  $(x_n)$

over  $\mathbb{F}_p$  defined by

$$x_n = f(n), \quad n \geq 0.$$

**Explicit inversive congruential generator**

For  $a, b \in \mathbb{F}_p$  with  $a \neq 0$  the *explicit inversive congruential generator* ( $z_n$ ) is defined by

$$z_n = (an + b)^{p-2}, \quad n \geq 0.$$

**Recursive non-linear congruential generator**

The *recursive non-linear congruential generator* ( $x_n$ ) is defined by

$$x_{n+1} = f(x_n), \quad n \geq 0,$$

with some initial value  $x_0 \in \mathbb{F}_p$  and a polynomial  $f(X) \in \mathbb{F}_p[X]$  with  $2 \leq \deg(f) \leq p - 1$ .

**Recursive inversive generator**

For  $a, b \in \mathbb{F}_p$  with  $a \neq 0$  the *recursive inversive congruential generator* ( $z_n$ ) is defined by

$$z_{n+1} = az_n^{p-2} + b, \quad n \geq 0,$$

with some initial value  $z_0$ .

**Legendre sequence**

The *Legendre sequence* ( $l_n$ ) of period  $p$  is the sequence over  $\mathbb{F}_2$  defined by  $l_n = 1$  if  $\left(\frac{n}{p}\right) = -1$ , i.e.  $n$  is a quadratic non-residue modulo  $p$  and  $l_n = 0$  otherwise.

**Sidelnikov sequence**

Let  $g$  be a primitive root modulo  $p$ . Then the *Sidelnikov sequence* ( $s_n$ ) is the the  $p - 1$  periodic sequence over  $\mathbb{F}_2$  defined by  $s_n = 1$  if  $g^n + 1$  is a quadratic non-residue modulo  $p$  and  $s_n = 0$  otherwise.

**Two-prime generator**

Let  $p$  and  $q$  be two distinct odd primes. Put

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

and

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

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*.

### Correlation measure of order $k$

The *correlation measure of order  $k$*  of a binary sequence  $(s_n)$  is introduced as

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

where the maximum is taken over all  $D = (d_1, d_2, \dots, d_k)$  with non-negative integers  $d_1 < d_2 < \dots < d_k$  and  $M$  such that  $M - 1 + d_k \leq T - 1$ .

### References

1. H. Aly and A. Winterhof, On the linear complexity profile of nonlinear congruential pseudorandom number generators with Dickson polynomials, *Des. Codes Cryptogr.* **39**, 2 (2006), 155–162.
2. H. Aly and A. Winterhof, On the  $k$ -error linear complexity over  $\mathbb{F}_p$  of Legendre and Sidelnikov sequences, *Des. Codes Cryptogr.* **40**, 3 (2006), 369–374.
3. P. H. T. 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, 2002), pp. 37–52.
4. E. R. Berlekamp, *Algebraic Coding Theory* (McGraw-Hill Book Co., New York-Toronto, Ont.-London, 1968).
5. 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 Computer Science (Springer, Berlin, 1990), Vol. 434, pp. 533–543.
6. S. R. Blackburn, T. Etzion and K. G. Paterson, Permutation polynomials, de Bruijn sequences, and linear complexity, *J. Combin. Theory Ser. A* **76**, 1 (1996), 55–82.
7. N. Brandstätter and A. Winterhof, Some notes on the two-prime generator, *IEEE Trans. Inform. Theory* **51** (2005), 3645–3647.

8. N. Brandstätter and A. Winterhof, Linear complexity profile of binary sequences with small correlation measure, *Period. Math. Hungar.* **52**, 2 (2006), 1–8.
9. T. W. Cusick, C. Ding and A. Renvall, *Stream Ciphers and Number Theory*, revised ed., North-Holland Mathematical Library, 66 (Elsevier Science B.V., Amsterdam, 2004).
10. C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science, (Springer-Verlag, Berlin, 1991), Vol. 561.
11. G. Dorfer, W. Meidl and A. Winterhof, Counting functions and expected values for the lattice profile at  $n$ , *Finite Fields Appl.* **10**, 4 (2004), 636–652.
12. G. Dorfer and A. Winterhof, Lattice structure and linear complexity profile of nonlinear pseudorandom number generators, *Appl. Algebra Engrg. Comm. Comput.* **13**, 6 (2003), 499–508.
13. J. Eichenauer, H. Grothe, J. Lehn and A. Topuzoğlu, A multiple recursive nonlinear congruential pseudo random number generator, *Manuscripta Math.* **59**, 3 (1987), 331–346.
14. J. Eichenauer and J. Lehn, A nonlinear congruential pseudorandom number generator, *Statist. Hefte* 4 (1986), 315–326.
15. J. Eichenauer-Herrmann, Statistical independence of a new class of inversive congruential pseudorandom numbers, *Math. Comp.* **60**, 201 (1993), 375–384.
16. Y.-C. Eun, H.-Y. Song and G. M. Kyureghyan, One-error linear complexity over  $\mathbb{F}_p$  of Sidelnikov sequences, *Sequences and Their Applications SETA 2004*, Lecture Notes in Computer Science (Springer, Berlin, 2005), Vol. 3486, pp. 154–165.
17. 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 Applied Mathematics (Dekker, New York, 1993), Vol. 141, pp. 75–80.
18. É. Fouvry, P. Michel, J. Rivat and A. Sárközy, On the pseudorandomness of the signs of Kloosterman sums, *J. Aust. Math. Soc.* **77**, 3 (2004), 425–436.
19. J. B. Friedlander, C. Pomerance and I. E. Shparlinski, Period of the power generator and small values of Carmichael’s function, *Math. Comp.* **70**, 236 (2001), 1591–1605.
20. J. B. Friedlander, C. Pomerance and I. E. Shparlinski, Corrigendum to: Period of the power generator and small values of Carmichael’s function, *Math. Comp.* **71**, 240 (2002), 1803–1806.
21. 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* **29**, 1 (1983), 144–146.
22. M. Z. Garaev, F. Luca, I. E. Shparlinski and A. Winterhof, On the lower bound of the linear complexity over  $\mathbb{F}_p$  of Sidelnikov sequences, *IEEE Trans. Inform. Theory* **52**, 7 (2006), 3299–3304.
23. F. Griffin and I. E. Shparlinski, On the linear complexity profile of the power generator, *IEEE Trans. Inform. Theory* **46**, 6 (2000), 2159–2162.

24. F. G. Gustavson, Analysis of the Berlekamp–Massey linear feedback shift-register synthesis algorithm, *IBM J. Res. Develop.* **20**, 3 (1976), 204–212.
25. J. Gutierrez, I. E. Shparlinski and A. Winterhof, On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators, *IEEE Trans. Inform. Theory* **49**, 1 (2003), 60–64.
26. K. Gyarmati, On a family of pseudorandom binary sequences, *Period. Math. Hungar.* **49**, 2 (2004), 45–63.
27. T. Helleseth and P. V. Kumar, Sequences with low correlation, *Handbook of Coding Theory* (North-Holland, Amsterdam, 1998) Vol. I, II, pp. 1765–1853.
28. F. Hess and I. E. Shparlinski, On the linear complexity and multidimensional distribution of congruential generators over elliptic curves, *Des. Codes and Cryptogr.* **35**, 1 (2005), 111–117.
29. T. Itoh and S. Tsujii, A fast algorithm for computing multiplicative inverses in  $\text{GF}(2^m)$  using normal bases, *Inform. and Comput.* **78**, 3 (1988), 171–177.
30. D. Jungnickel, Finite fields. Structure and arithmetics. Bibliographisches Institut, Mannheim, (1993).
31. A. Klapper, The vulnerability of geometric sequences based on fields of odd characteristic, *J. Cryptology* **7**, 1 (1994), 33–51.
32. N. Koblitz, *Algebraic Aspects of Cryptography*. (Springer-Verlag, Berlin Heidelberg, 1998).
33. S. Konyagin, T. Lange and I. Shparlinski, Linear complexity of the discrete logarithm, *Des. Codes Cryptogr.* **28**, 2 (2003), 135–146.
34. R. Lidl, G. L. Mullen and G. Turnwald, Dickson polynomials, *Pitman Monographs and Surveys in Pure and Applied Mathematics* (Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.), Vol. 65.
35. J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inform. Theory* **IT-15** (1969) 122–127.
36. 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 Computer Science (Springer, Berlin, 1996), Vol. 1109, pp. 358–371.
37. C. Mauduit, H. Niederreiter and A. Sárközy, On pseudorandom  $[0, 1)$  and binary sequences, *Publ. Math. Debrecen* **71**, 3–4 (2007), 305–324.
38. C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol, *Acta Arith.* **82**, 4 (1997), 365–377.
39. W. Meidl, How many bits have to be changed to decrease the linear complexity? *Des. Codes Cryptogr.* **33**, 2 (2004), 109–122.
40. W. Meidl, Linear complexity and  $k$ -error linear complexity for  $p^n$ -periodic sequences, *Coding, Cryptography and Combinatorics*, Progr. Comput. Sci. Appl. Logic (Birkhäuser, Basel, 2004.), Vol. 23, pp. 227–235.
41. W. Meidl and H. Niederreiter, On the expected value of the linear complexity and the  $k$ -error linear complexity of periodic sequences, *IEEE Trans. Inform. Theory* **48**, 11 (2002), 2817–2825.

42. W. Meidl and A. Winterhof, Lower bounds on the linear complexity of the discrete logarithm in finite fields, *IEEE Trans. Inform. Theory* **47**, 7 (2001), 2807–2811.
43. 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, 2002), pp. 229–238.
44. W. Meidl and A. Winterhof, On the linear complexity profile of explicit nonlinear pseudorandom numbers, *Inform. Process. Lett.* **85**, 1 (2003), 13–18.
45. W. Meidl and A. Winterhof, On the linear complexity profile of some new explicit inversive pseudorandom numbers, *J. Complexity* **20**, 2–3 (2004), 350–355.
46. W. Meidl and A. Winterhof, On the autocorrelation of cyclotomic generators, *Finite Fields and Applications*, Lecture Notes in Computer Science (Springer, Berlin, 2004), Vol. 2948, 1–11.
47. W. Meidl and A. Winterhof, Some notes on the linear complexity of Sidelnikov-Lempel-Cohn-Eastman sequences, *Des. Codes Cryptogr.* **38**, 2 (2006), 159–178.
48. W. Meidl and A. Winterhof, On the linear complexity profile of nonlinear congruential pseudorandom number generators with Rdei functions, *Finite Fields Appl.* **13**, 3 (2007), 628–634.
49. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, With a foreword by R. L. Rivest. CRC Press Series on Discrete Mathematics and its Applications (CRC Press, Boca Raton, FL, 1997).
50. H. Niederreiter, Some computable complexity measures for binary sequences, *Sequences and their Applications*, Singapore, 1998, Springer Ser. Discrete Math. Theor. Comput. Sci. (Springer, London, 1999), pp. 67–78.
51. H. Niederreiter, Random number generation and quasi-Monte Carlo methods, *CBMS-NSF Regional Conference Series in Applied Mathematics*, 63, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, (1992).
52. H. Niederreiter, Linear complexity and related complexity measures for sequences, *Progress in Cryptology — INDOCRYPT 2003*, Lecture Notes in Computer Science (Springer, Berlin, 2003), Vol. 2904, pp. 1–17,
53. H. Niederreiter and I. E. Shparlinski, Recent advances in the theory of nonlinear pseudorandom number generators, *Monte Carlo and Quasi-Monte Carlo Methods*, 2000, Hong Kong, (Springer, Berlin, 2002), pp. 86–102.
54. R. Nöbauer, Rédei-Permutationen endlicher Körper, *Contributions to General Algebra*, Salzburg, 1986 (Hölder-Pichler-Tempsky, Vienna, 1987), Vol. 5, pp. 235–246.
55. R. A. Rueppel, in *Analysis and Design of Stream Ciphers*, With a foreword by J. L. Massey. Communications and Control Engineering Series (Springer-Verlag, Berlin, 1986).
56. R. A. Rueppel, Stream ciphers, *Contemporary Cryptology* (IEEE, New York, 1992), pp. 65–134.

57. W. M. Schmidt, Equations over finite fields, *An Elementary Approach*, Lecture Notes in Mathematics (Springer-Verlag, Berlin-New York, 1976), Vol. 536.
58. I. Shparlinski, On the linear complexity of the power generator, *Des. Codes Cryptogr.* **23**, 1 (2001), 5–10.
59. I. Shparlinski, Cryptographic applications of analytic number theory, *Complexity Lower Bounds and Pseudorandomness*, Progress in Computer Science and Applied Logic (Birkhäuser Verlag, Basel, 2003), Vol. 22.
60. I. E. Shparlinski and A. Winterhof, On the linear complexity of bounded integer sequences over different moduli, *Inform. Process. Lett.* **96**, 5 (2005), 175–177.
61. V. M. Sidel'nikov, Some  $k$ -valued pseudo-random sequences and nearly equidistant codes, *Prob. Inform. Transmission* **5**, 1 (1969), 12–16.; translated from *Problemy Peredači Informacii*, **5**, 1 (1969), 16–22 (Russian).
62. B. Smeets, The linear complexity profile and experimental results on a randomness test of sequences over the field  $\mathbb{F}_q$ , Preprint (1988).
63. 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* **39**, 4 (1993), 1398–1401.
64. A. Tietäväinen, Vinogradov's method and some applications, *Number Theory and Its Applications*, Ankara, 1996, Lecture Notes in Pure and Applied Mathematics (Dekker, New York, 1999), Vol. 204, pp. 261–282.
65. A. Topuzoğlu and A. Winterhof, On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders, *Appl. Algebra Engrg. Comm. Comput.* **16**, 4 (2005), 219–228.
66. A. Topuzoğlu and A. Winterhof, Pseudorandom sequences, *Topics in Geometry, Coding Theory and Cryptography*, Algebr. Appl. (Springer, Dordrecht, 2007), Vol. 6, pp. 135–166.
67. R. J. Turyn, The linear generation of Legendre sequence, *J. Soc. Indust. Appl. Math.* **12** (1964) 115–116.
68. I. M. Vinogradov, *Elements of Number Theory*, Translated by S. Kravetz (Dover Publications, Inc., New York, 1954).
69. Y. Wang, Linear complexity versus pseudorandomness: on Beth and Dai's result, *Advances in Cryptology — ASIACRYPT'99* (Singapore), Lecture Notes in Computer Science (Springer, Berlin, 1999), Vol. 1716, pp. 288–298.
70. 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 (Birkhäuser, Basel, 2004), Vol. 23, pp. 359–367.
71. G. Xiao and S. Wei, in Fast algorithms for determining the linear complexity of period sequences, ed., A. Menezes *et al.*, *Progress in Cryptology — INDOCRYPT 2002. Third International Conference on Cryptology in India*, Hyderabad, India (December 16–18, 2002), Proceedings. Berlin: Springer. Lecture Notes Computer Science 2551, pp. 12–21.
72. 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  $\text{GF}(q)$ , *IEEE Trans. Inform. Theory* **46**, 6 (2000), 2203–2206.