On lattice profile of the elliptic curve linear congruential generators

Zhixiong Chen
Department of Mathematics, Putian University,
Putian, Fujian 351100, China
ptczx@126.com

Domingo Gomez
University of Cantabria
Avd. Los Castros, s/n, Santander, Spain
domingo.gomez@unican.es

Gottlieb Pirsic
Johannes Kepler University
Altenbergerstr. 69, 4040 Linz, Austria
gpirsic@gmail.com

Abstract

Lattice tests are quality measures for assessing the intrinsic structure of pseudorandom number generators. Recently a new lattice test has been introduced by Niederreiter and Winterhof. In this paper, we present a general inequality that is satisfied by any periodic sequence. Then, we analyze the behavior of the linear congruential generators on elliptic curves (abbr. EC-LCG) under this new lattice test and prove that the EC-LCG passes it up to very high dimensions. We also use a result of Brandstätter and Winterhof on the linear complexity profile related to the correlation measure of order k to present lower bounds on the linear complexity profile of some binary sequences derived from the EC-LCG.

Keywords. Lattice test; Linear complexity profile; Linear congruential generator; Elliptic curve; Finite field

Mathematics subject classification number: 11K45.

1 Introduction

1.1 Lattice tests

Lattice tests are quality measures for assessing the intrinsic structure of pseudorandom generators. The following lattice test was introduced in [8, 9] and further analyzed in [6, 7, 8, 19]. Let $(\eta_n), n = 0, 1, \ldots$, be a sequence over the finite field $\mathbb{F}_q$ of q elements of period T. The characteristic of the field $\mathbb{F}_q$ will be p, so $q = p^m$, for some positive integer m.

For given integers $s \geq 1$ and $N \geq 2$, (η_n) passes the *s-dimensional N-lattice test* if the vectors $\{\underline{\eta_n} - \underline{\eta_0} \ : \ 1 \leq n \leq N-1\}$ span $\mathbb{F}_q^s$, where

$$\underline{\eta_n} = (\eta_n, \eta_{n+1}, \ldots, \eta_{n+s-1}), \text{ for } 0 \leq n \leq N-1.$$

The largest dimension s such that (η_n) satisfies the s-dimensional N-lattice test is called *lattice profile at N*, denoted by $S(\eta_n, N)$. Moreover, let

$$S(\eta_n) = \sup_{N \geq 2} S(\eta_n, N).$$

One can verify that

$$S(\eta_n) = S(\eta_n, T)$$

for any periodic sequence T of period $T > 1$. And clearly $S(\eta_n) = 1$ if the period $T = 1$.

If additionally $\mathbb{F}_q$ is a finite prime field, i. e. $q = p$, this special lattice test for $N = T$ is the one which was proposed by Marsaglia in [16].

A stronger lattice test was introduced in [20] by Niederreiter and Winterhof for inversive pseudorandom number generators, and further investigated in [21] by the third author and Winterhof for digital explicit nonlinear and inversive pseudorandom number generators. Let (η_n) be a T-periodic sequence over the finite field $\mathbb{F}_q$. For given integers $s \geq 1$, $0 < d_1 < d_2 < \cdots < d_{s-1} < T$, and $N \geq 2$, we say that (η_n) passes the *s-dimensional N-lattice test with lags* $d_1, \ldots, d_{s-1}$ if the vectors $\{\underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0} \ : \ 1 \leq n \leq N-1\}$ span $\mathbb{F}_q^s$, where

$$\underline{\eta_{n,\mathbf{d}}} = (\eta_n, \eta_{n+d_1}, \ldots, \eta_{n+d_{s-1}}), \quad 0 \leq n \leq N-1.$$

The largest dimension s such that (η_n) satisfies the s-dimensional N-lattice test for all lags $d_1, \ldots, d_{s-1}$ is denoted by $\mathbb{S}(\eta_n, N)$, i.e.,

$$\mathbb{S}(\eta_n, N) = \max\left\{ s : \forall 0 < d_1 < \cdots < d_{s-1} < T, \langle \underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0}, \ 0 \leq n \leq N-1 \rangle = \mathbb{F}_q^s \right\}.$$

It is easy to see $\mathbb{S}(\eta_n, N) \leq S(\eta_n, N)$. On the other hand, $\mathbb{S}(\eta_n, T)$ is bounded below by an expression depending only on $S(\eta_n)$, if T is a prime. We prove the following Lemma,which comes from [15, Lemma 1]. The residue classes modulo T are identified with integers in the range $\{0, \ldots, T-1\}$ and vice versa.

Lemma 1. *Let $s \geq 2$, T a prime and $0 < d_1 < \cdots < d_{s-1} < T$, then there exists an integer $r \in \mathbb{Z}$ with $\gcd(r, T) = 1$ such that,*

$$d_i \equiv r h_i \pmod{T},\ i = 1, \ldots, s-1$$

with $|h_i| \leq (4sT)^{(s-2)/(s-1)}$.

Proof. We start with the case $d_1 = 1$ and, at the end of the proof, we reduce the general case to this particular case.

First of all, let $\vec{e}_i$ be the ith $(s-2)$-dimensional unit vector. We consider the set

$$\mathcal{S} = \{\vec{e}_1, \ldots, \vec{e}_{s-2}, T\vec{e}_1, \ldots, T\vec{e}_{s-2}, (d_2, \ldots, d_{s-1})\}. \tag{1}$$

Applying [15, Lemma 1], there exist

$$h_2, \ldots, h_{s-1}, j_2, \ldots, j_{s-1}, r' \leq (4sT)^{(s-2)/(s-1)} \text{ such that}$$
$$h_2\vec{e}_1 + \ldots + h_{s-1}\vec{e}_{s-2} + j_2 T\vec{e}_1 + \ldots + j_{s-1}T\vec{e}_{s-2} + r'(d_2, \ldots, d_{s-1}) = \vec{0}.$$

Comparing components, we have

$$r' d_i \equiv h_i \pmod{T},\ i = 2, \ldots, s-1$$

It is easy to see that r' is not a multiple of T so, taking $r \equiv (r')^{-1} \pmod{T}$, then we have the result for $d_1 = 1$. The case $d_1 \neq 1$ can be reduced to the general case, just multiplying each $d_1, d_2, \ldots, d_{s-1}$ by the inverse of d_1 modulo T. This remark finishes the proof. □

We will also use Lemma 2 from [22].

Lemma 2. *Consider a sequence (η_n), with $S(\eta_n) \leq L$ and period T. Then, for any integers $M \geq 1$, and $0 \leq e_0, \ldots, e_L$ there are some elements $c_0, \ldots, c_L$ (not all zero) such that*

$$\sum_{j=0}^{L} c_j \eta_{Mb+e_j} = 0$$

for any integer b with $0 \leq b \leq T-1$.

The next theorem gives a general inequality that relates $\mathbb{S}(\eta_n, T)$ with $S(\eta_n)$ for any sequence (η_n), when T is prime.

Proposition 1. *Let (η_n) be any T-periodic sequence with T prime, if s satisfies the following inequality*

$$s \leq \frac{\log T + \log s + 2}{\log T + \log s + 2 - \log S(\eta_n)}$$

then the sequence (η_n) passes the s-dimensional T-lattice test with any lags.

Proof. We assume that the sequence (η_n) does not pass the s-dimensional T-lattice test for some lags $0 < d_1 < \cdots < d_{s-1} < T$. Put

$$\underline{\eta_{n,\mathbf{d}}} = (\eta_n, \eta_{n+d_1}, \ldots, \eta_{n+d_{s-1}}), \text{ for } 0 \le n \le N-1.$$

for $0 \le n \le T-1$ and let V be the subspace of $\mathbb{F}_q^s$ spanned by all $\underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0}$ for $0 \le n \le T-1$. Let us denote by $V^\perp = \{\underline{u} \in \mathbb{F}_q^s : \underline{u} \cdot \underline{v} = 0 \text{ for all } \underline{v} \in V\}$ the *orthogonal space* of V, where $\cdot$ denotes the usual inner product. By our hypothesis, $\dim(V) < s$ and $\dim(V^\perp) \ge 1$, so there exists a non zero vector $\underline{\alpha} \in V^\perp$ and

$$\underline{\alpha} \cdot \left(\underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0}\right) = 0, \text{ for } 0 \le n \le T-1.$$

Equivalently, we write

$$\underline{\alpha} \cdot \underline{\eta_{n,\mathbf{d}}} = \underline{\eta_0} \cdot \underline{\alpha} = \delta, \text{ for } 0 \le n \le T-1.$$

By Lemma 1, we can rewrite as

$$\alpha_0\eta_n + \alpha_1\eta_{n+rh_1} + \ldots + \alpha_{s-1}\eta_{n+rh_{s-1}} = \delta, \text{ for } 0 \le n \le T-1$$

where $\gcd(r, T)$ and $0 < h_1, \ldots, h_{s-1} \le (4sT)^{(s-2)/(s-1)}$. We define the following sequence $(\eta_n)' = (\eta_{rn})$ and we obtain

$$\alpha_0\eta'_n + \alpha_1\eta'_{n+h_1} + \ldots + \alpha_{s-1}\eta'_{n+h_{s-1}} = \delta, \text{ for } 0 \le n \le T-1.$$

This means that $S(\eta'_n, T) \le (4sT)^{(s-2)/(s-1)}$, so if we take,

$$0, r', 2r' \ldots, hr' \text{ where } h = \lceil (4sT)^{(s-2)/(s-1)} \rceil \text{ and } r'r \equiv 1 \mod T.$$

and apply Lemma 2, we also get that $S(\eta_n, T) \le (4sT)^{(s-2)/(s-1)}$.

Operating with $S(\eta_n, T)$, we obtain the result. □

1.2 Elliptic curves

Recent developments point towards an interest in the elliptic curve analogues of pseudo-random number generators, which are reasonably new sources of pseudo-random numbers based on the group structure of elliptic curves over finite fields. These generators include the linear congruential generator on elliptic curves, the power generator on elliptic curves and the Naor-Reingold generator on elliptic curves, see the recent survey [23].

We first introduce some notions and basic facts of elliptic curves over finite fields. Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$, where $q = p^m$ is a prime power and $p > 3$, given by an affine Weierstrass equation of the standard form

$$y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{F}_q)$$

with nonzero discriminant, see [10]. It is known that the set $\mathcal{E}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of $\mathcal{E}$ forms an abelian group under an appropriate composition rule denoted by $\oplus$ and with the point at infinity $\mathcal{O}$ as the neutral element. We recall that

$$|\#\mathcal{E}(\mathbb{F}_q) - q - 1| \le 2q^{1/2},$$

where $\#\mathcal{E}(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points, including the point at infinity $\mathcal{O}$. For a given point $G \in \mathcal{E}(\mathbb{F}_q)$, the *linear congruential generator on elliptic curves*, EC-LCG, is defined as

$$U_n = G \oplus U_{n-1} = nG \oplus U_0,\ n = 0, 1, \ldots, \tag{2}$$

where U_0 is the initial point. In this article, let $G \in \mathcal{E}(\mathbb{F}_q)$ be a point of order T, that means T is the size of the cyclic group $\langle G \rangle$ generated by G. The EC-LCG is a T-periodic sequence over $\mathbb{F}_q \times \mathbb{F}_q$.

Some other important elliptic curve generators are also studied in the last decade, such as the elliptic curve power generator and the elliptic curve Naor-Reingold generator.

For a k-dimensional integer vector $(a_1, \ldots, a_k) \in \mathbb{Z}_T^k$, the *elliptic curve Naor-Reingold generator*, EC-NRG, is defined as the sequence:

$$F_a(n) = a_1^{n_1} \cdots a_k^{n_k} G,\ \ n = 0, 1, \cdots, \tag{3}$$

where $n = n_1 \ldots n_k$ is the bit representation of n, $0 \le n \le 2^k - 1$, addding zeros until length k.

The translation map by $W \in \mathcal{E}(\mathbb{F}_q)$ on $\mathcal{E}(\mathbb{F}_q)$ is defined as

$$\tau_W : \mathcal{E}(\mathbb{F}_q) \to \mathcal{E}(\mathbb{F}_q),\ G \mapsto G \oplus W.$$

It is obvious that $(f \circ \tau_W)(G) = f(G \oplus W)$.

We conclude this section with some results on rational functions, which are needed in our proofs. Let $\mathbb{F}_q(\mathcal{E})$ be the function field of $\mathcal{E}$ defined over $\mathbb{F}_q$. For any f (or $f(x, y)$) in $\mathbb{F}_q(\mathcal{E})$ and $G \in \mathcal{E}(\overline{\mathbb{F}_q})$, G is called a *zero* (resp. a *pole*) of f if $f(G) = 0$ (resp. $f(G) = \infty$). Any rational function has only a finite number of zeros and poles. Let $\mathrm{ord}_G(f)$ be the *order* of f at G. In fact,

$$\mathrm{ord}_G(f) : \mathbb{F}_q(\mathcal{E}) \to \mathbb{Z} \cup \{\infty\}$$

is a *discrete valuation* of $\mathbb{F}_q(\mathcal{E})$, see [10, p.22] or [24, Definition I.1.9]. Obviously, $\mathrm{ord}_G(f) = 0$ for all but finitely many $G \in \mathcal{E}(\overline{\mathbb{F}_q})$ and $\mathrm{ord}_G(f) > 0$ if G is a zero of f while $\mathrm{ord}_G(f) < 0$ if G is a pole of f.

Any nonconstant polynomial $f \in \mathbb{F}_q(\mathcal{E})$ has the only pole at $\mathcal{O}$. The *degree* of f is $\deg(f) = \sum_{\mathrm{ord}_G(f)>0} \mathrm{ord}_G(f) = \sum_{\mathrm{ord}_G(f)<0} |\mathrm{ord}_G(f)|$. For example, $\deg(x) = 2$ and $\deg(y) = 3$. We need the following results.

Lemma 3. *Let $f, g \in \mathbb{F}_q(\mathcal{E})$ be rational functions, we have*

$$\mathrm{ord}_G(f+g) \ge \min\{\mathrm{ord}_G(f), \mathrm{ord}_G(f)\},\ \textit{for any } G \in \mathcal{E}(\overline{\mathbb{F}_q}).$$

The equality holds if $\mathrm{ord}_G(f) \ne \mathrm{ord}_G(g)$.

Proof. See [10, Proposition 2.14] or [24, Lemma I.1.10]. □

Lemma 4. *Let $f, g \in \mathbb{F}_q(\mathcal{E})$ be rational functions such that $f+g$ is nonconstant. Then we have* $\deg(f+g) \le \deg(f) + \deg(g)$.

Proof. Using the definition of deg and Lemma 3,

$$\deg(f+g) = \sum_{G \text{ with } \mathrm{ord}_G(f+g)<0} |\mathrm{ord}_G(f+g)| \leq \sum_{\mathrm{ord}_G(f+g)<0} |\min\{\mathrm{ord}_G(f), \mathrm{ord}_G(g)\}|$$

Now, we separate the sum in two different sums, one where $\mathrm{ord}_G(f) \leq \mathrm{ord}_G(g)$ and another where $\mathrm{ord}_G(f) > \mathrm{ord}_G(g)$. It is clear

$$\sum_{0>\mathrm{ord}_G(f+g)\geq \mathrm{ord}_G(f)} |\mathrm{ord}_G(f)| \leq \deg(f).$$

In the same way, we get that the other summand is less than the degree of g, this finishes the proof. □

Lemma 5. *Let $f, g \in \mathbb{F}_q(\mathcal{E})$ be nonconstant rational functions with disjoint pole sets. Then $f+g$ is nonconstant.*

Proof. Suppose G is a pole of f, then G is not a pole of g, so $\mathrm{ord}_G(f) < \mathrm{ord}_G(g) = 0$. Then by Lemma 3, we have

$$\mathrm{ord}_G(f+g) < 0$$

i.e., G is a pole of $f+g$, so function $f+g$ is nonconstant. □

Remark. The proof of Lemma 5 also indicates that the set of poles of $f+g$ is exactly the union of the poles of f and g with disjoint pole sets.

2 Lattice profile of EC-LCG

We will consider the lattice test with lags for sequences derived from the EC-LCG in general fields. Using the generator (U_n) defined by (2) and a function $f \in \mathbb{F}_q(\mathcal{E})$ with a single pole, the linear congruential sequence with elliptic curves is defined by

$$\eta_n = f(U_n), \text{ for } n = 0, 1, \ldots \tag{4}$$

From Proposition 1 and the result in [14] we get a lower bound for $\mathbb{S}(\eta_n, T)$, however, in the next Theorem, we prove a stronger lower bound.

Theorem 1. *Let f be a rational function with a single pole H on $\mathcal{E}$. For the T-periodic sequence (4) with EC-LCG (U_n) defined by (2), we have*

$$\mathbb{S}(\eta_n, N) \geq \begin{cases} \frac{N}{1+\deg(f)} - 1, & \text{if } U_0 \in \langle G \rangle \oplus H, \\ \frac{N}{\deg(f)} - 1, & \text{in other case,} \end{cases} \quad \text{for } 1 \leq N \leq T-1.$$

In particular,

$$\mathbb{S}(\eta_n) = \mathbb{S}(\eta_n, T) \geq \begin{cases} \frac{T}{1+\deg(f)} - 1, & \textit{if } U_0 \in \langle G \rangle \oplus H, \\ \frac{T}{\deg(f)} - 1, & \textit{in other case,} \end{cases}$$

Proof. We assume that the sequence (η_n) does not pass the s-dimensional N-lattice test for some lags $0 < d_1 < \cdots < d_{s-1} < T$. Put

$$\underline{\eta_{n,\mathbf{d}}} = (\eta_n, \eta_{n+d_1}, \ldots, \eta_{n+d_{s-1}}), \quad 0 \leq n \leq N-1.$$

for $0 \leq n \leq T-1$ and let V be the subspace of $\mathbb{F}_q^s$ spanned by all $\underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0}$ for $0 \leq n \leq T-1$. Let us denote by $V^\perp = \{\underline{u} \in \mathbb{F}_q^s : \underline{u} \cdot \underline{v} = 0 \text{ for all } \underline{v} \in V\}$ the *orthogonal space* of V, where $\cdot$ denotes the usual inner product. Then $\dim(V) < s$ and $\dim(V^\perp) \geq 1$. Take $\underline{0} \neq \underline{\alpha} \in V^\perp$, then

$$\underline{\alpha} \cdot \left(\underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0}\right) = 0, \text{ for } 0 \leq n \leq T-1.$$

Equivalently, we write

$$\underline{\alpha} \cdot \underline{\eta_{n,\mathbf{d}}} = \underline{\eta_0} \cdot \underline{\alpha} = \delta, \text{ for } 0 \leq n \leq T-1.$$

If $\underline{\alpha}) = (\alpha_0, \ldots, \alpha_{s-1})$, then let j be the smallest index with $\alpha_j \neq 0$ (so $0 \leq j < s$). Then with $d_0 = 0$ if $j = 0$ and for $0 \leq n \leq N-1$,

$$\alpha_j \eta_{n+d_j} + \alpha_{j+1}\eta_{n+d_{j+1}} + \cdots + \alpha_{s-1}\eta_{n+d_{s-1}} = \delta.$$

That is,

$$\alpha_j f((n+d_j)G \oplus U_0) + \alpha_{j+1} f((n+d_{j+1})G \oplus U_0) + \cdots + \alpha_{s-1} f((n+d_{s-1})G \oplus U_0) = \delta, \tag{5}$$

where $0 \leq n \leq N-1$. Let Q be a generic rational point and

$$F(Q) := (\alpha_j f \circ \tau_{d_j G \oplus U_0} + \alpha_{j+1} f \circ \tau_{d_{j+1} G \oplus U_0} + \cdots + \alpha_{s-1} f \circ \tau_{d_{s-1} G \oplus U_0})(Q) - \delta.$$

Since H is the single pole of f, we see that $H \ominus (d_i G \oplus U_0)$ is the only pole of $f \circ \tau_W(d_i G \oplus W)$. By Lemma 5 it is easy to see that F is a nonconstant rational function since the points $H \ominus (d_i G \oplus U_0)$ are poles of F if $\alpha_i \neq 0$, $j \leq i \leq s-1$, where $\ominus$ is the inversive operation of $\oplus$. Furthermore, by Lemma 4 we have

$$\deg(F) \leq (s-j)\deg(f) \leq s\deg(f).$$

According to (5), at least M points $nG : 0 \leq n \leq N-1$ are zeros of F, where

$$M = \begin{cases} N-s, & \text{if } U_0 \in \langle G \rangle \oplus H, \\ N, & \text{otherwise.} \end{cases}$$

So we have

$$M \leq \deg(F) \leq s\deg(f),$$

which leads to the desired result. □

For $f(x,y) = x$, a frequently case studied, like in [11, 23] and the survey [25], we have the following corollary.

Corollary 1. *For the T-periodic sequence $(\eta_n) = (x(U_n))$ with EC-LCG (U_n) defined by (2), we have*

$$\mathbb{S}(\eta_n, N) \geq \begin{cases} \frac{N}{3} - 1, & \text{if } U_0 \in \langle G \rangle, \\ \frac{N}{2} - 1, & \text{in other case,} \end{cases} \quad \text{for } 1 \leq N \leq T-1.$$

For Naor-Reingold sequences with elliptic curves, Proposition 1 and the results of [5] says that the sequence passes the 2-lattice test, for almost all choices of $a_1, \ldots, a_k$.

Theorem 2. *For $\gamma > 0$ and the T-periodic sequence $(\eta_n) = (x(U_n))$ with Naor Reingold generator (U_n) with period T prime and $k \geq 2\log T$. Then this sequence passes the $2-$lattice test with any lags for almost all choices of $a_1, \ldots, a_k$.*

Theorem 1 can be extended to r-dimensional sequences investigated in [14]. We first define the lattice profile for r-dimensional sequences. Let

$$\eta_n = \{(\Sigma_{n,1}, \Sigma_{n,2}, \ldots, \Sigma_{n,r}),\ n = 0, 1, \ldots, T-1\}$$

be a r-dimensional sequence over the finite field $\mathbb{F}_q$. Since $\mathbb{F}_q^r$ is isomorphic to $\mathbb{F}_{q^r}$ as vector space over $\mathbb{F}_q$, one can view $(\Sigma_{n,1}, \Sigma_{n,2}, \ldots, \Sigma_{n,r})$ as an element of $\mathbb{F}_{q^r}$ by the relationship

$$\eta_n := \Sigma_1\gamma_1 + \Sigma_2\gamma_2 + \ldots + \Sigma_r\gamma_r \in \mathbb{F}_{q^r}$$

where $\gamma_1, \ldots, \gamma_r$ is a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. For given integers $s \geq 1, 0 < d_1 < d_2 \cdots < d_r$, and $N \geq 2$, we say that (η_n) passes the *s-dimensional N-lattice test with lags $d_1, \ldots, d_{s-1}$* if the vectors $\{\underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0} \ : \ 1 \leq n \leq N-1\}$ span $\mathbb{F}_{q^r}^s$, where

$$\underline{\eta_{n,\mathbf{d}}} = (\eta_n, \eta_{n+d_1}, \ldots, \eta_{n+d_{s-1}}),\ 0 \leq n \leq N-1.$$

The largest dimension s such that (η_n) satisfies the s-dimensional N-lattice test for all lags $d_1, \ldots, d_s$ is denoted by $\mathbb{S}(\eta_n, N)$, i.e.,

$$\mathbb{S}(\eta_n, N) = \max\left\{s : \forall 0 < d_1 < \cdots < d_{s-1} < T, \langle \underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0},\ 0 \leq n \leq N-1\rangle = \mathbb{F}_{q^r}^s\right\}.$$

which is called the *generalized lattice profile* at N of (η_n). Now we introduce r-dimensional elliptic curve sequences studied in [14].

Let H be a place of degree d of $\mathcal{E}$ and let

$$\mathcal{C} = \{f_1, f_2, \ldots, f_r\} \subseteq \mathbb{F}_q(\mathcal{E}) \tag{6}$$

be a set of $r \geq 1$ rational functions with pole divisors of the form

$$\mathrm{div}(f_i)_\infty = (i + \epsilon)[H], \quad 1 \leq i \leq r$$

where

$$\epsilon = \begin{cases} 1, & \text{if } d = 1, \\ 0, & \text{if } d \geq 2. \end{cases}$$

Since $\mathcal{E}$ has genus one, such functions always exist by the theorem of Riemann-Roch.

We define $\rho = r + \epsilon$. For $r = 2$ and $H = \mathcal{O}$ a natural example is given by $f_1(P) = x(P)$ and $f_2(P) = y(P)$, where $P = (x(P), y(P)) \neq \mathcal{O}$. In this case, $d = 1, \rho = 3$ (see [14]).

Then we define the k-dimensional sequence with EC-LCG in (2) and rational functions in (6) by

$$(f_1(U_n), f_2(U_n), \ldots, f_k(U_n)), \quad n = 0, 1, \ldots, T-1. \tag{7}$$

Theorem 3. *For the k-dimensional sequence (η_n) with*

$$\eta_n = (f_1(U_n), f_2(U_n), \ldots, f_k(U_n)) \quad n = 0, 1, \ldots, T-1.$$

we have

$$\mathbb{S}(\eta_n, N) = \begin{cases} \frac{N}{1+d\rho} - 1, & \text{if } U_0 \in \langle G \rangle \oplus H, \\ \frac{N}{d\rho} - 1, & \text{in other case,} \end{cases} \quad \text{for } 1 \leq N \leq T-1.$$

Proof. We will not distinguish between the vectors in $\mathbb{F}_q^k$ and the elements in $\mathbb{F}_{q^r}$. That is,

$$\eta_n = (f_1(U_n), f_2(U_n), \ldots, f_k(U_n)) = f_1(U_1)\gamma_1 + f_2(U_n)\gamma_2 + \cdots + f_k(U_n)\gamma_k$$

where $\gamma_1, \ldots, \gamma_k$ is a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.

Now assume that in $\mathbb{F}_{q^r}$ the sequence (η_n) does not pass the s-dimensional N-lattice test for some lags $0 < d_1 < \cdots < d_{s-1} < T$. Put

$$\underline{\eta_{n,\mathbf{d}}} = (\eta_n, \eta_{n+d_1}, \ldots, \eta_{n+d_{s-1}}), 0 \leq n \leq N-1.$$

Following the ideas in the proof of Theorem 2, we get

$$\underline{\alpha} \cdot \left(\underline{\eta_{n,\mathbf{d}}} - \underline{\eta_0} \right) = 0, \text{ for } 0 \leq n \leq T-1$$

Equivalently, we write

$$\underline{\alpha} \cdot \underline{\eta_{n,\mathbf{d}}} = \underline{\alpha} \cdot \underline{\eta_0} = \delta, \ 0 \leq n \leq T-1$$

for $\underline{\alpha} = (\alpha_0, \ldots, \alpha_{s-1}) \in \mathbb{F}_{q^r}^s$. Let j be the smallest index with $\alpha_j \neq 0$ (so $0 \leq j < s$). Then with $d_0 = 0$ if $j = 0$ and for $0 \leq n \leq N-1$, we get

$$\alpha_j \eta_{n+d_j} + \alpha_1 \eta_{n+d_{j+1}} + \ldots + \alpha_{s-1} \eta_{n+d_{s-1}} = \delta.$$

That is,

$$\begin{aligned}\delta &= \alpha_j(f_1(U_{n+d_j})\gamma_1 + f_2(U_{n+d_j})\gamma_2 + \cdots + f_r(U_{n+d_j})\gamma_k) \\ &\quad + \alpha_{j+1}(f_1(U_{n+d_{j+1}})\gamma_1 + f_2(U_{n+d_{j+1}})\gamma_2 + \cdots + f_r(U_{n+d_{j+1}})\gamma_k) \\ &\quad + \alpha_{s-1}(f_1(U_{n+d_{s-1}})\gamma_1 + f_2(U_{n+d_{s-1}})\gamma_2 + \cdots + f_r(U_{n+d_{s-1}})\gamma_k) \\ &= (\alpha_j f_1(U_{n+d_j}) + \alpha_{j+1}f_1(U_{n+d_{j+1}}) + \cdots \alpha_{s-1}f_1(U_{n+d_{s-1}}))\gamma_1 + \cdots \\ &\quad + (\alpha_j f_r(U_{n+d_j}) + \alpha_{j+1}f_r(U_{n+d_{j+1}}) + \cdots \alpha_{s-1}f_r(U_{n+d_{s-1}}))\gamma_r \quad (8)\end{aligned}$$

where $0 \le n \le N-1$. For $1 \le l \le k$, we are going to define,

$$F_l = \alpha_j f_l \circ \tau_{d_j G \oplus U_0} + \alpha_{j+1} f_l \circ \tau_{d_{j+1} G \oplus U_0} + \cdots + \alpha s - 1 f_l \circ \tau_{d_{s-1} G \oplus U_0} \in \mathcal{E}(\mathbb{F}_q).$$

By Lemma 5 and Remark 1, the poles of F_l for all $1 \le l \le r$ are

$$H \ominus (d_i G \oplus U_0), \quad j \le i \le s-1 \tag{9}$$

with $\alpha_i \neq 0$. On the other hand, using (6) we have for $j \le l \le s-1$

$$\mathrm{ord}_{H \ominus (d_i G \oplus U_0)}(F_1) < \mathrm{ord}_{H \ominus (d_i G \oplus U_0)}(F_2) < \cdots < \mathrm{ord}_{H \ominus (d_i G \oplus U_0)}(F_k).$$

Thus F_i's are non-constant rational functions and

$$\deg(F_1) < \deg(F_2) < \cdots < \deg(F_r) \le (s-j)\deg(f_r) \le s \deg(f_r) \le sd\rho.$$

Using (8), we have

$$\delta = \gamma_1 F_1(nG) + \gamma_2 F_2(nG) + \cdots + \gamma_k F_k(nG) = (\gamma_1 F_1 + \gamma_2 F_2 + \cdots + \gamma_k F_k)\,(nG)$$

for $0 \le n \le N-1$. At last, we have to show that this function is not constant.

Let k be the largest index with $\alpha_k \neq 0$ in $\{\alpha_j, \alpha_{j+1}, \ldots, \alpha_{s-1}\}$. Then each F_i has a pole at $H \ominus (d_k G \oplus U_0)$ of order $d(i+\epsilon)$. So $\gamma_1 F_1 + \gamma_2 F_2 + \cdots + \gamma_k F_k$ is non-constant and the degree is bounded by $sd\rho$ by Lemma 3. By Equation (9), it has no poles in $\langle G \rangle$ if $H \notin \langle G \rangle \oplus U_0$, and at most s different poles in $\langle G \rangle$ if $H \in \langle G \rangle \oplus U_0$. This gives

$$sd\rho \ge \begin{cases} N-s, & \text{if } H \in \langle G \rangle \oplus H, \\ N, & \text{otherwise,} \end{cases}$$

which leads to the desired result. □

3 Linear Complexity of some binary sequences derived from EC-LCG

In [17], Mauduit and Sárközy introduced the notion of the *correlation measure of order k*, an important measure of pseudorandomness for finite binary sequences. Let

$$E_T = \{e_0, e_1, \ldots, e_{T-1}\} \in \{0,1\}^T,$$

then the *correlation measure of order* k of E_T is defined as

$$C_k(E_T) = \max_{M,D} \left| \sum_{n=1}^{M} (-1)^{e_{n+d_1}+e_{n+d_2}+\cdots+e_{n+d_k}} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ with non-negative integers $0 \le d_1 < \ldots < d_k < T$ and M such that $M + d_k \le T - 1$.

We may consider E_T as an infinite sequence of period T. We recall that the *linear complexity profile* $L(E_T, N)$ is the least order L of a linear recurrence relation over $\mathbb{F}_2$

$$e_{n+L} = c_0 e_n + c_1 e_{n+1} + \cdots + c_{L-1} e_{n+L-1}, \text{ for } 0 \le n \le N - L - 1$$

which is satisfied by the first N terms of E_T, and the *linear complexity* $L(E_T)$ is defined as

$$L(E_T) = \sup_{N \ge 1} L(E_T, N),$$

see [26, 25] for details on the linear complexity and also [8] for the relation with lattice tests. In [1, Theorem 1], Brandstätter and Winterhof used the correlation measure of order k to estimate a lower bound on the linear complexity profile $L(E_T, N)$ for E_T.

Lemma 6. *For any $T-$periodic binary sequence E_T, the following inequality holds*

$$L(E_T, N) \ge N - \max_{1 \le k \le L(E_T,N)+1} C_k(E_T)$$

where $2 \le N \le T - 1$.

Below we present some binary sequences constructed using elliptic curves over the prime field $\mathbb{F}_p$ in the literature. (We note that some of our references deal actually with the corresponding sequences $e'_n = (-1)^{e_n}$ over $\{+1, -1\}$.) Here we recall some notations. Let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ and $G \in \mathcal{E}(\mathbb{F}_p)$ be a rational point of order T. We write $x(iG) = x_i$ and $y(iG) = y_i$ for $iG = (x_i, y_i)$.

In [3], the following five types of finite binary sequences $S_T = \{s_0, \ldots, s_{T-1}\}$ of length T are defined:

$$s_i = \begin{cases} 1, & y(iG) > \frac{p}{2}, \\ 0, & \text{otherwise.} \end{cases} \qquad s_i = \begin{cases} 1, & x(iG) < y(iG), \\ 0, & \text{otherwise.} \end{cases} \tag{10}$$

$$s_i = \begin{cases} 1, & y(iG) \text{ is even}, \\ 0, & \text{otherwise.} \end{cases} \quad s_i = \begin{cases} 1, & x(iG) \text{ is even}, \\ 0, & \text{otherwise.} \end{cases} \quad s_i = \begin{cases} 1, & x(iG) > \frac{p}{2}, \\ 0, & \text{otherwise.} \end{cases} \tag{11}$$

Theorem 4. *For any $S_T = \{s_0, \ldots, s_{T-1}\}$ defined in* (10) *and in* (11). *If $k < T$, we have*

$$C_k(S_T) \le 2^k k p^{1/2} (1 + \log p)^k (1 + \log T).$$

Proof. See [3] for details. □

Theorem 4 and Lemma 6 yield the following result.

Corollary 2. *For any* $S_T = \{s_0, \ldots, s_{T-1}\}$ *in* (10)*, we have*

$$L(S_T, N) = \Omega\left(\frac{\log(Np^{-1/2})}{\log\log p}\right)$$

for $1 \le N \le T-1$.

In [2], taking the Legendre symbol, the first author constructed a family of binary sequences $S_T = \{s_0, \ldots, s_{T-1}\}$ along elliptic curves by defining

$$s_i = \begin{cases} 0, & \text{if } \left(\frac{f(iG)}{p}\right) = 1 \text{ or } f(iG) = 0, \infty, \\ 1, & \text{if } \left(\frac{f(iG)}{p}\right) = -1, \end{cases} \tag{12}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Here the function f should be selected carefully. We note that the restricted conditions of "$f(x,y) \in \mathbb{F}_q(\mathcal{E})$ being a rational function with $f(x,y) \neq z^2(x,y)$ for all $z(x,y) \in \overline{\mathbb{F}_q(\mathcal{E})}$" in [2] are not enough, as the example below shows.

Example. We recall that T is the order of G and suppose that $m > 1$ is a divisor of T. For ANY rational function $g(x,y)$, if we select

$$f(Q) = g(Q)g(Q + \frac{N}{m}G)g(Q + \frac{2N}{m}G)\cdots g(Q + \frac{(m-1)N}{m}G),$$

where Q is a generic rational point, we note that here f is not a square, but

$$f(nG)f(nG + \frac{m}{T}G) = (g(nG)g(nG + \frac{T}{m}G)g(nG + \frac{2T}{m}G)\cdots g(nG + \frac{(m-1)T}{m}G))^2,$$

which leads to $C_2(S_T)$ for (12) is trivial. □

So for appropriate f, we have the following result as proved in [2, Theorem 3].

Corollary 3. *For* $S_T = \{s_0, \ldots, s_{T-1}\}$ *in (12), we have*

$$L(S_T, N) = \Omega\left(\frac{N}{p^{1/2}\log T}\right)$$

for $1 \le N \le T-1$.

In [4], the first author, Li and Xiao defined a family of binary sequences using discrete logarithm along elliptic curves. Let g be a fixed primitive root modulo p. For each $x \in \mathbb{F}_p^*$, let $\mathrm{ind}(x)$ denote the index (discrete logarithm) of x (to the base g) so that

$$g^{\mathrm{ind}(x)} \equiv x \pmod{p}.$$

We add the condition

$$1 \le \mathrm{ind}(x) \le p-1$$

to make the value of index unique. The sequence $S_T = \{s_0, \ldots, s_{T-1}\}$ is defined by

$$s_i := \begin{cases} 0, & \text{if } 1 \le \mathrm{ind}(f(iG)) \le (p-1)/2, \\ 1, & \text{if } (p+1)/2 \le \mathrm{ind}(f(iG)) \le p-1 \text{ or } p | f(iG). \end{cases} \tag{13}$$

The construction in (13) is an elliptic curve analogue of [13]. As Example above shows, we also select f carefully in this construction.

Theorem 5 ([4]). *For $S_T = \{s_0, \ldots, s_{T-1}\}$ in (13) and $k < T$, we have*

$$C_k(S_T) \le 4^k k p^{1/2} (1 + \log p)^k (1 + \log T).$$

Theorem 5 and Lemma 6 yield the following result.

Corollary 4. *For $S_T = \{s_0, \ldots, s_{T-1}\}$ in (13), we have*

$$L(S_T, N) = \Omega\left(\frac{\log(Np^{-3/4})}{\log\log p}\right)$$

for $1 \le N \le T-1$.

Finally, we remark that in the recent paper [18], Mérai pointed out some sufficient conditions for selecting appropriate f in (12) and (13) using ideas similar to the ones in [12].

Acknowledgement

Parts of this paper was written during a pleasant visit of Z.X.C. to Linz. He wishes to thank the Austrian Academy of Sciences for hospitality and support. The authors wish to thank Arne Winterhof for helpful discussions and pointing out the example in this article. D. G. also wants to express his gratitude to his coauthors for the interesting discussions and their help during all steps of the research.

Z.X.C. was partially supported by the National Natural Science Foundation of China under grant No.61170246 and the Program for New Century Excellent Talents in Fujian Province University under grant JK2010047. G.P. was partially supported by the Austrian Science Fund (FWF) under research grant S9609.

References

[1] N. BRANDSTÄTTER and A. WINTERHOF. Linear complexity profile of binary sequences with small correlation measure, *Period. Math. Hungar.*, 52(2) (2006), 1-8.

[2] Z. CHEN. Elliptic curve analogue of Legendre sequences, *Monatsh. Math.*, 154(1) (2008), 1-10.

[3] Z. CHEN and G. XIAO. Pseudo-random binary sequences from elliptic curves, http://eprint.iacr.org/2007/275.pdf.

[4] Z. CHEN, S. LI and G. XIAO. Construction of pseudo-random binary sequences from elliptic curves by using discrete logarithm, *Sequences and Their Applications*-SETA2006, Lecture Notes in Computer Science 4086, Springer, Berlin, 2006, 285-294.

[5] M. CRUZ, D. GÓMEZ and D. SADORNIL. On the linear complexity of the Naor-Reingold sequence with elliptic curves, *Finite Fields and Their Applications*, 16(5) (2010), 329-333.

[6] G. DORFER. Lattice profile and linear complexity profile of pseudorandom number sequences, *Finite Fields and Applications*, Lecture Notes in Computer Science 2948, Springer, Berlin, 2004, 69-78.

[7] G. DORFER, W. MEIDL and A. WINTERHOF. Counting functions and expected values for the lattice profile at n, *Finite Fields and Their Applications*, 10(4) (2004), 636-652.

[8] 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.

[9] G. DORFER and A. WINTERHOF. Lattice structure of nonlinear pseudorandom number generators in parts of the period, *Monte Carlo and quasi-Monte Carlo methods* 2002, Springer, Berlin, 2004, 199-211.

[10] A. ENGE. *Elliptic Curves and Their Applications to Cryptoraphy: an Introduction*, Kluwer Academic Publishers, Dordrecht, 1999.

[11] G. GONG, A. BERSON and R. STINSON. Elliptic curve pseudorandom sequence generators, *Selected areas in cryptography*, Lecture Notes in Computer Science 1758, Springer, Berlin, 2000, 34-48.

[12] L. GOUBIN, C. MAUDUIT and A. SÁRKÖZY. Construction of large families of pseudorandom binary sequences, *J. Number Theory*, 106(1) (2004), 56-69.

[13] K. GYARMATI, C. MAUDUIT and A. SÁRKÖZY. Constructions of pseudorandom binary lattices, *Unif. Distrib. Theory*, 4(2) (2009), 59-80.

[14] F. HESS and I. E. SHPARLINSKI. On the linear complexity and multidimensional distribution of congruential generators over elliptic curves, *Des. Codes Cryptogr.*, 35(1) (2005), 111-117.

[15] A. JOUX and J. STERN. Lattice reduction: a toolbox for the cryptanalyst, *J. Cryptology*, 11(3) (1998), 161-185.

[16] G. MARSAGLIA. The structure of linear congruential sequences, *Applications of Number Theory to Numerical Analysis (Proc. Sympos., Univ. Montreal, Montreal, Que., 1971)*, Academic Press, New York, 1972, 249-285.

[17] C. MAUDUIT and A. SÁRKÖZY. On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol, Acta Arith., 82(4) (1997) 365-377.

[18] L. MÉRAI. Constructions of pseudorandom binary lattices using elliptic curves, *Proc. Amer. Math. Soc.*, 139(2) (2011), 407-420.

[19] H. NIEDERREITER and A. WINTERHOF. Lattice structure and linear complexity of nonlinear pseudorandom numbers, *Appl. Algebra Engrg. Comm. Comput.*, 13(4) (2002), 319-326.

[20] H. NIEDERREITER and A. WINTERHOF. On the structure of inversive pseudorandom number generators, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Lecture Notes in Computer Science 4851, Springer, Berlin, 2007, 208-216.

[21] G. PIRSIC and A. WINTERHOF. On the structure of digital explicit nonlinear and inversive pseudorandom number generators, *J. Complexity*, 26(1) (2010), 43-50.

[22] I. E. SHPARLINSKI. On the Naor-Reingold pseudorandom function from elliptic curves, *Appl. Algebra Engrg. Comm. Comput.*, 11(1) (2000), 27-34.

[23] I. E. SHPARLINSKI. Pseudorandom number generators from elliptic curves, *Contemp. Math. -Recent Trends in Cryptography* 477, Amer. Math. Soc., Providence, RI, 2009, 121-141.

[24] H. STICHTENOTH. *Algebraic Function Fields and Codes*, Graduate Texts in Mathematics 254, second edition, Springer-Verlag, Berlin, 2009.

[25] A. TOPUZOĞLU and A. WINTERHOF. Pseudorandom sequences, *Topics in Geometry, Coding Theory and Cryptography*, Algebr. Appl. 6, Springer, Dordrecht, 2007, 135-166.

[26] 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 23, Birkhä

user, Basel, 2004, 359-367.