*Bull. Aust. Math. Soc.* **102** (2020), 342–352
doi:10.1017/S0004972719001321

# ON THE $k$-ERROR LINEAR COMPLEXITY OF SEQUENCES FROM FUNCTION FIELDS

YUHUI ZHOU, YUHUI HAN and YANG DING✉

(Received 26 September 2019; accepted 25 October 2019; first published online 8 January 2020)

**Abstract**

The linear complexity and the error linear complexity are two important security measures for stream ciphers. We construct periodic sequences from function fields and show that the error linear complexity of these periodic sequences is large. We also give a lower bound for the error linear complexity of a class of nonperiodic sequences.

2010 *Mathematics subject classification*: primary 94A55.

*Keywords and phrases*: sequence, linear complexity, error linear complexity, algebraic function fields, local expansion.

## 1. Introduction

A necessary condition for the security of a stream cipher is that it has large linear complexity to thwart an attack by the Berlekamp–Massey algorithm. For stability, the linear complexity of a sequence should not decrease significantly if a few terms are changed. For this purpose, Ding *et al.* [2] introduced the concept of *sphere complexity* in 1991 and Stamp and Martin [13] introduced the *k-error linear complexity* in 1993. The $k$-error linear complexity has proved to be a useful measure of the stability of a pseudorandom sequence (see [1, 5, 7–9, 12, 15, 16]).

We consider periodic sequences from function fields, based on the constructions in [4, 10, 16], and we obtain improved lower bounds for the linear complexity and new lower bounds for the error linear complexity. We also analyse the error linear complexity of a class of nonperiodic sequences. This use of algebraic function fields in sequence construction is not new (see [4, 10, 15–18]).

In this paper, we focus on the linear complexity and error linear complexity. While large linear complexity is a necessary condition for cryptographic security, it is not sufficient. The sequences we consider have some nonrandom properties.

The paper is organised as follows. The next section presents some basic notation and definitions for linear complexity and error linear complexity and basic results on

This work was supported by the National Natural Science Foundation of China under Grant No. 11671248.

the function fields that we will use. Section 3 deals with the error linear complexity of periodic sequences. Section 4 gives a lower bound for the error linear complexity of the nonperiodic sequences constructed in [17].

## 2. Preliminaries

Throughout this paper, $\mathbb{F}_q$ denotes the finite field with $q$ elements.

**2.1. Linear complexity.** We first introduce some basic definitions about linear complexity and error linear complexity of sequences.

Definition 2.1.

(1) Let $\mathbf{s} = (s_0, s_1, s_2, \ldots)$ be an infinite sequence of elements of $\mathbb{F}_q$ and let $n$ be a positive integer. The $n$th linear complexity of $\mathbf{s}$, denoted by $L_n(\mathbf{s})$, is the smallest positive integer $l$ such that there exist $l+1$ elements $\lambda_0, \lambda_1, \ldots, \lambda_l \in \mathbb{F}_q$ with $\lambda_0 \neq 0, \lambda_l = 1$ satisfying $\sum_{i=0}^{l} \lambda_i s_{i+v} = 0$ for $0 \leq v \leq n-l-1$.

(2) Let $\mathbf{S} = (s_0, s_1, s_2, \ldots)$ be an $N$-periodic sequence of elements of $\mathbb{F}_q$. The linear complexity of $\mathbf{S}$, denoted by $L(\mathbf{S})$, is the smallest positive integer $l$ such that there exist $l+1$ elements $\lambda_0, \lambda_1, \ldots, \lambda_l \in \mathbb{F}_q$ with $\lambda_0 \neq 0, \lambda_l = 1$ satisfying $\sum_{i=0}^{l} \lambda_i s_{i+v} = 0$ for all $v$.

It is well known that the linear complexity of nonperiodic infinite sequences cannot exceed $\frac{1}{2}n$. This is the basis for the following definition [11].

Definition 2.2. An infinite sequence $\mathbf{s} = \{s_0, s_1, s_2 \ldots\}$ of elements of $\mathbb{F}_q$ is called $d$-perfect for a positive integer $d$ if $L_n(\mathbf{s}) \geq \frac{1}{2}(n+1-d)$ for all $n \geq 1$.

For the stability of the keystream, changing a few terms of the sequence should not cause a significant decrease in the linear complexity. According to this requirement, a new measure of complexity was proposed by Stamp and Martin in [13].

Definition 2.3.

(1) Let $\mathbf{S}$ be an $N$-periodic sequence of elements of $\mathbb{F}_q$. For an integer $k$ with $0 \leq k \leq N-1$, the $k$-error linear complexity of $\mathbf{S}$ is

$$L_k(\mathbf{S}) := \min_{\mathbf{T}} L(\mathbf{T}),$$

where the minimum is taken over all $N$-periodic sequences $\mathbf{T}$ obtained from $\mathbf{S}$ by changing $k$ or fewer terms in one period.

(2) Let $\mathbf{s}$ be an infinite sequence of elements of $\mathbb{F}_q$. For integers $k$ and $n$ with $0 \leq k \leq n-1$, the $n$th $k$-error linear complexity of $\mathbf{s}$ is

$$L_{n,k}(\mathbf{s}) := \min_{\mathbf{t}} L_n(\mathbf{t}),$$

where the minimum is taken over all infinite sequences $\mathbf{t}$ obtained from $\mathbf{s}$ by changing $k$ or fewer terms in the first $n$ positions.

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

**2.2. Function fields.** Now we recall some properties of function fields (see [14] for more details). Let $F/\mathbb{F}_q$ be a global function field with genus $g$. Denote by $\mathbb{P}_F$ the set of all places of $F$ and by $\mathbb{P}_F^{(1)}$ the set of all rational places of $F$. Let $R \in \mathbb{P}_F^{(1)}$ and $t \in F$ be a local parameter of $R$. For a given nonzero function $f \in F$, there exist an integer $v = v(R)$ and an infinite sequence $\{a_r\}_{r=v}^{\infty}$ over $\mathbb{F}_q$ such that

$$f = \sum_{r=v}^{\infty} a_r t^r.$$

The above equation is called the *local expansion* of $f$ at $R$.

For a divisor $G$, we define the Riemann–Roch space

$$\mathcal{L}(G) = \{f \mid f \in F\backslash\{0\}, \operatorname{div}(f) + G \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(G)$ is a finite-dimensional vector space over $\mathbb{F}_q$. Moreover, by the Riemann–Roch theorem, $\dim_{\mathbb{F}_q} \mathcal{L}(G) \geq \deg(G) + 1 - g$ and equality holds if $\deg(G) \geq 2g - 1$.

Let $\operatorname{Aut}(F/\mathbb{F}_q)$ denote the $\mathbb{F}_q$-automorphism group of $F$. The following properties of automorphisms can be found in [14].

LEMMA 2.4. *Let $\sigma \in \operatorname{Aut}(F/\mathbb{F}_q)$, $P \in \mathbb{P}_F$ and $f \in F$. Then:*

(1) *$\sigma(P)$ is also a place of $F$ with $\deg(\sigma(P)) = \deg(P)$;*
(2) *$v_{\sigma(P)}(\sigma(f)) = v_P(f)$;*
(3) *$\sigma(f)(\sigma(P)) = f(P)$ if $v_P(f) \geq 0$.*

## 3. *k*-error linear complexity for periodic sequences

In this section, we present a construction of periodic sequences from function fields and calculate the $k$-error linear complexity for these sequences. We will show that both the linear complexity and the error linear complexity are large.

We fix the following notation for this section:

- $F$—a global function field over $\mathbb{F}_q$ with genus $g$;
- $\sigma$—an $\mathbb{F}_q$-automorphism of $F/\mathbb{F}_q$;
- $P$—a rational place of $F$;
- $N$—the least positive integer satisfying $\sigma^N(P) = P$;
- $D$—a positive divisor of $F$ fixed by $\sigma$ with $\deg(D) = d$.

Let $Q \in \mathbb{P}_F \setminus \{P, \sigma(P), \ldots, \sigma^{N-1}(P)\}$ be a place of $F$ with degree $d'$ such that $Q, \sigma(Q), \ldots, \sigma^{N-1}(Q)$ are pairwise distinct. Choose the positive divisor $D$ such that

$$\mathcal{L}(D + Q) \setminus \mathcal{L}(D) \neq \emptyset.$$

Then there is a function $f \in \mathcal{L}(D + Q)$ such that $(f)_\infty = D' + Q$ for some positive divisor $D' \leq D$. We define a sequence $\mathbf{S}(f)$ over $\mathbb{F}_q$ by

$$\mathbf{S}(f) := (f(\sigma^j(P)))_{j=0}^{\infty}.$$

Obviously, the period of the sequence $\mathbf{S}(f)$ is at most $N$.

THEOREM 3.1. *With the above notation, if $d < N - 2d'$, then the period of $\mathbf{S}(f)$ is $N$.*

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

PROOF. Suppose that the period $u$ of $\mathbf{S}(f)$ is less than $N$. Consider the function

$$z = f - \sigma^{-u}(f).$$

Note that $Q$ and $\sigma^{-u}(Q)$ are the poles of $z$, so that $z$ is a nonzero element. Moreover, $z \in \mathcal{L}(D + Q + \sigma^{-u}(Q))$. Since $\sigma^{-u}(f)(\sigma^i(P)) = \sigma^{-u}(f)(\sigma^{-u}(\sigma^{i+u}(P))) = f(\sigma^{i+u}(P))$ by Lemma 2.4(3),

$$z(\sigma^i(P)) = (f - \sigma^{-u}(f))(\sigma^i(P)) = f(\sigma^i(P)) - f(\sigma^{i+u}(P)) = 0$$

for all $i \geq 0$, that is, $P, \sigma(P), \ldots, \sigma^{n-1}(P)$ are zeros of $z$. Thus,

$$0 \neq z \in \mathcal{L}\Big(D + Q + \sigma^{-u}(Q) - \sum_{i=0}^{N-1} \sigma^i(P)\Big).$$

This holds only if

$$\deg\Big(D + Q + \sigma^{-u}(Q) - \sum_{i=0}^{N-1} \sigma^i(P)\Big) \geq 0,$$

that is,

$$d \geq N - 2d'.$$

This contradicts our condition. Hence, the period of $\mathbf{S}(f)$ is $N$. □

Now we consider the linear complexity of the sequence.

THEOREM 3.2. *If $d < N - 2d'$, then the linear complexity of the sequence $\mathbf{S}(f)$ satisfies*

$$L(\mathbf{S}(f)) \geq \frac{N - d - d'}{d'}.$$

PROOF. Set $l = L(\mathbf{S}(f))$. If $l = N$, we have nothing to prove. Hence, we may assume that $l < N$. Then there exist $l + 1$ elements $\lambda_0, \lambda_1, \ldots, \lambda_l \in \mathbb{F}_q$ with $\lambda_0 \neq 0, \lambda_l = 1$ satisfying

$$\sum_{i=0}^{l} \lambda_i f(\sigma^{i+v}(P)) = 0$$

for all $v \geq 0$. This is equivalent to

$$\Big(\sum_{i=0}^{l} \lambda_i \sigma^{-i}(f)\Big)(\sigma^v(P)) = 0. \tag{3.1}$$

Put

$$z = \sum_{i=0}^{l} \lambda_i \sigma^{-i}(f).$$

We claim that $z = \sum_{i=0}^{l} \lambda_i \sigma^{-i}(f)$ is nonzero. This follows from the facts:

(1) $\sigma^{-i}(Q)$ are distinct for $i = 0, 1, \ldots, l$;
(2) $\sigma^j(Q)$ is a pole of $\sigma^i(f)$ if and only if $i = j$ for $0 \leq i, j \leq l$;
(3) $\sigma^l(Q)$ is a pole of $\sum_{i=0}^{l} \lambda_i \sigma^{-i}(f)$.

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

So,

$$0 \neq z \in \mathcal{L}\Big(D + \sum_{i=0}^{l} a\sigma^{-i}(Q)\Big).$$

By (3.1),

$$0 \neq z \in \mathcal{L}\Big(D + a\sum_{i=0}^{l} \sigma^{-i}(Q) - \sum_{v=0}^{N-1} \sigma^{v}(P)\Big).$$

This can only happen when

$$\deg\Big(D + \sum_{i=0}^{l} \sigma^{-i}(Q) - \sum_{v=0}^{N-1} \sigma^{v}(P)\Big) \geq 0,$$

that is,

$$d + (l+1)d' \geq N.$$

Our result follows. □

Remark 3.3.

(1) The above theorem indicates that the linear complexity of $\mathbf{S}(f)$ is good if $d'$ and $d$ are as small as possible.

(2) For the construction of $D$ satisfying $\mathcal{L}(D+Q) \setminus \mathcal{L}(D) \neq \emptyset$, we often choose $d \geq 2g-1$, because then, by the Riemann–Roch theorem,

$$\dim(\mathcal{L}(D+Q)) - \dim(\mathcal{L}(D)) = \deg(Q) > 0.$$

The following theorem gives the lower bound of the error linear complexity.

Theorem 3.4. *Let $k$ be a positive integer with $0 \leq k \leq N-1$. If $d < N - 2d'$, then the $k$-error linear complexity of $\mathbf{S}(f)$ satisfies*

$$L_k(\mathbf{S}(f)) \geq \frac{N - d - d' - k}{d' + k}.$$

Proof. Let $\mathbf{S}_1$ be a periodic sequence of period $N$ obtained from $\mathbf{S}(f)$ by changing $r$ $(0 \leq r \leq k)$ positions in the first period of length $N$ and then continuing the changes periodically. Suppose that the linear complexity of $\mathbf{S}_1$ is $l$. Then there are $l+1$ elements $\lambda_0, \lambda_1, \ldots, \lambda_l \in \mathbb{F}_q$ with $\lambda_0 \neq 0, \lambda_l = 1$ satisfying

$$\sum_{i=0}^{l} \lambda_i s_{i+v} = 0 \quad \text{for } 0 \leq v \leq N-1. \tag{3.2}$$

Substitute $\mathbf{S}(f)$ into (3.2). Since every term of $\mathbf{S}(f)$ occurs in at most $l+1$ equations, (3.2) is true for $\mathbf{S}(f)$ for at least $N - r(l+1)$ values of $v$. This means that $z = \sum_{i=0}^{l} \lambda_i \sigma^{-i}(f)$ has at least $N - r(l+1)$ zeros amongst $P, \sigma(P), \ldots, \sigma^{N-1}(P)$; denote these zeros by $P_1, \ldots, P_{N-r(l+1)}$. Thus,

$$0 \neq z \in \mathcal{L}\Big(D + \sum_{i=0}^{l} \sigma^{-i}(Q) - \sum_{j=1}^{N-r(l+1)} P_j\Big).$$

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

This can only happen when

$$\deg\Big(D + \sum_{i=0}^{l} \sigma^{-i}(Q) - \sum_{j=1}^{N-r(l+1)} P_j\Big) \geq 0,$$

that is,

$$d + (l+1)d' \geq N - r(l+1) \geq N - k(l+1).$$

Our result follows. □

Now we present some specific examples of this construction.

Example 3.5 (Rational function field). Let $F = \mathbb{F}_q(x)$ be a rational function field over $\mathbb{F}_q$ with $q$ odd and let $\zeta$ be a primitive element of $\mathbb{F}_q$. Let $\mathbb{P}_F^{(1)}$ be the set of all rational places of $F$, so that $\#P_F^{(1)} = q+1$. Let $P_1$ be the unique zero of $x - \zeta$ and $P_2$ the unique zero of $x - \zeta^2$. Let $P_0$ and $P_\infty$ be the zero and pole of $x$, respectively.

Let $\phi$ be the automorphism of $F/\mathbb{F}_q$ defined by $\phi(x) = \zeta x$ and set $\sigma = \phi^2$. The action of $\sigma$ on $\mathbb{P}_F^{(1)} \setminus \{P_0, P_\infty\}$ gives two orbits of length $N = \frac{1}{2}(q-1)$, which we label

$$\{\sigma^j(P_1) \mid \ 0 \leq j \leq N-1\}; \quad \{\sigma^j(P_2) \mid \ 0 \leq j \leq N-1\}.$$

Now we can take $D = 0, Q = P_2$. Since $g(F) = 0$, the Riemann–Roch theorem gives $\mathcal{L}(Q) \setminus \mathcal{L}(0) \neq \emptyset$. Let $f \in \mathcal{L}(Q) \setminus \mathbb{F}_q$. Our construction gives a periodic sequence

$$\mathbf{S}(f) = (f(P_1), \ldots, f(\sigma^{N-1}(P_1)))^\infty.$$

Then $d = 0, d' = 1$ and, by Theorems 3.1, 3.2 and 3.4, respectively:

(1) the period of $\mathbf{S}(f)$ is $N$;
(2) the linear complexity of $\mathbf{S}(f)$ satisfies $L(\mathbf{S}(f)) \geq N - 1$;
(3) the $k$-error linear complexity of $\mathbf{S}(f)$ satisfies $L_k(\mathbf{S}(f)) \geq (N - 1 - k)/(k+1)$.

Remark 3.6. The lower bound for the linear complexity of this sequence improves the estimate given in [10], namely

$$L(\mathbf{S}(f)) \geq \min\Big\{\frac{2N-1}{3}, \frac{q-3}{4}\Big\}.$$

While the linear complexity is large, the sequence is cryptographically weak because the parameters can be computed from any three consecutive terms.

For the next example we need the following lemma.

Lemma 3.7 [6]. *Let $F$ be the cyclic function field over $\mathbb{F}_q$ with $N = 1 + q + t$ rational places. Let $R$ be a generator of $\mathbb{P}_F^{(1)}$ and $Q$ a place of degree $d$. If $\gcd(N, d) = 1$, then $\sigma^i(Q), \ldots, \sigma^{i+N-1}(Q)$ are pairwise distinct and $\sigma^{i+N}(Q) = \sigma^i(Q)$ for any $i \in \mathbb{Z}$.*

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

Example 3.8 (Elliptic function field). Let $F$ be the cyclic function field over $\mathbb{F}_q$ with $N = 1 + q + t$ rational places, that is, the set of rational places, $\mathbb{P}_F^{(1)}$, is a cyclic group and $-2\sqrt{q} \le t \le 2\sqrt{q}$. Let $R$ be a generator of $\mathbb{P}_F^{(1)}$, that is, $\mathbb{P}_F^{(1)} = \{[i]R \mid 0 \le i \le N-1\}$. From [3], there is a unique $\sigma_R \in \mathrm{Aut}(F/\mathbb{F}_q)$ such that $\sigma_R([i]R) = [i+1]R$. Let $\sigma = \sigma_R$. The action of $\sigma$ on all the rational places forms an orbit of length $n$, which we label as

$$\{\sigma^j(R) \mid j = 0, 1, \ldots, N-1\} = \mathbb{P}_F^{(1)}.$$

Now suppose that $n$ is an odd number. Take $D = 0$ and $Q$ a place of degree two. Since $g(F) = 1$, the Riemann–Roch theorem gives $\mathcal{L}(Q) \setminus \mathcal{L}(0) \neq \emptyset$. Let $f \in \mathcal{L}(D + [2]R) \setminus \mathcal{L}(D)$. Our construction gives a periodic sequence

$$\mathbf{S}(f) = (f(\sigma^0(R)), \ldots, f(\sigma^{N-1}(R)))^\infty.$$

Then $d = 0, d' = 2$ and, by Theorems 3.1, 3.2 and 3.4, respectively:

(1) the period of $\mathbf{S}(f)$ is $N$;
(2) the linear complexity of $\mathbf{S}(f)$ satisfies $(\mathbf{S}(f)) \ge (N-2)/2$;
(3) the $k$-error linear complexity of $\mathbf{S}(f)$ satisfies $L_k(\mathbf{S}(f)) \ge (N-2-k)/(k+2)$.

Remark 3.9. The sequence in Example 3.8 is a special case of [4]. The lower bound for the linear complexity improves the estimate $L(\mathbf{S}(f)) \ge N/3$ given in [4].

Finally we give an example over a Hermitian function field. This construction was used to define a multisequence in [16], but the lower bound for the linear complexity in [16] is not valid for a single sequence.

Example 3.10 (Hermitian function field). Let $q > 3$ be a prime power. The Hermitian function field over $\mathbb{F}_{q^2}$ is the function field $\mathbb{F}_{q^2}(x, y)$, where $x, y$ are two variables over $\mathbb{F}_{q^2}$ satisfying

$$y^q + y = x^{q+1}.$$

This is a nonsingular plane curve with genus $g = \frac{1}{2}(q+1-1)(q+1-2) = \frac{1}{2}q(q-1)$.

Let $\epsilon$ be a primitive element of $\mathbb{F}_{q^2}$. Then the automorphism $\phi = \sigma_{\epsilon,0,0}$ is of order $q^2 - 1$, where $\sigma_{a,b,c}$ represents the automorphism

$$\sigma_{a,b,c}(x) = ax + b, \quad \sigma_{a,b,c}(y) = a^{q+1}y + ab^q x + c.$$

Moreover, we have the following properties from [16]:

(1) $\phi(P_\infty) = P_\infty$, where $P_\infty$ is the unique common pole of $x$ and $y$;
(2) the action of $\phi$ on all rational places $\neq P_\infty, P_{(0,0)}$ gives rise to $q+1$ orbits among which one contains $q-1$ elements and each of the others contains exactly $q^2 - 1$ elements.

Take two rational places $R, Q$ generating orbits of length $N = q^2 - 1$ in $\mathbb{P}_F^{(1)}$ and label them as

$$\{\sigma^j(R) \mid j = 0, 1, \ldots, N-1\} \quad \text{and} \quad \{\sigma^j(Q) \mid j = 0, 1, \ldots, N-1\},$$

where $\deg(R) = 1, \deg(Q) = d' = 1$.

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

Let $D = (2g-1)P_\infty$. Then $D$ is fixed by $\phi$ and $d = \deg(D) = 2g-1 = q^2-q-1$. By the Riemann–Roch theorem, $\dim(\mathcal{L}(D+Q)) - \dim(\mathcal{L}(D)) = \deg(Q) = 1$. Choose $f \in \mathcal{L}(D+Q) \setminus \mathcal{L}(D)$ and generate a periodic sequence $\mathbf{S}(f) = (f(\phi^i(R)))_{i=0}^{\infty}$. Then $d = q^2-q-1 < q^2-1-2 = N-2d'$ and, by Theorems 3.1, 3.2 and 3.4, respectively:

(1) the period of $\mathbf{S}(f)$ is $q^2-1$;
(2) the linear complexity of $\mathbf{S}(f)$ satisfies $L(\mathbf{S}(f)) \geq q-1$;
(3) the $k$-error linear complexity of $\mathbf{S}(f)$ satisfies $L_k(\mathbf{S}(f)) \geq (q-1-k)/(k+1)$.

## 4. $k$-error linear complexity for a nonperiodic sequence

In this section, we calculate the $k$-error linear complexity for a nonperiodic infinite sequence constructed by Xing and Lam in [17]. We first recall the construction of [17]. We fix the following notation for this section:

- $F$—global function field with full constant field $\mathbb{F}_q$;
- $P$—a rational place of $F$;
- $t$—a local parameter at $P$ with $\deg((t)_\infty) = 2$;
- $f$—a function in $F \setminus \mathbb{F}_q(t)$.

Choose $f \in F$ with $v_P(f) \geq 0$. Let $f = \sum_{n=0}^{\infty} a_n t^n$ be the local expansion of $f$ at $P$, where $a_n \in \mathbb{F}_q$, and define the sequence $\mathbf{s}(f)$ by

$$\mathbf{s}(f) = (a_1, a_2, a_3, \ldots).$$

Lemma 4.1 [17]. *If $d \geq \deg((f)_\infty)$ and $v_P(f) \geq 0$, then the sequence $\mathbf{s}(f)$ constructed above is $d$-perfect, that is, $L_n(\mathbf{s}(f)) \geq \frac{1}{2}(n+1-d)$ for all $n \geq 1$.*

The sequence constructed above retains its linear complexity profile if a limited number of terms are changed.

Lemma 4.2 [18]. *If $d \geq \deg((f)_\infty)$ and $v_P(f) \geq 0$, then any sequence $\mathbf{s}$ obtained by changing the first $k$ terms of $\mathbf{s}(f)$ is $(d+2k)$-perfect. Moreover, if the divisor $(t)_\infty$ satisfies $k(t)_\infty \leq (f)_\infty$, then $\mathbf{s}$ is still $d$-perfect.*

Now we consider $k$-error linear complexity of $\mathbf{s}(f)$ for arbitrary $k$.

Proposition 4.3. *Let $k$ be a positive integer. If $d \geq \deg((f)_\infty)$ and $v_P(f) \geq 0$, then the $n$th $k$-error linear complexity of $\mathbf{s}(f)$ satisfies*

$$L_{n,k}(\mathbf{s}(f)) \geq \frac{n + (2^{k+1}-1) - (2^{k+1}-1)d}{2(2^{k+1}-1)}.$$

Proof. By Lemma 4.1, the sequence $\mathbf{s}(f)$ is $d$-perfect. For any positive integer $n$, let $\mathbf{s}_n$ be the sequence of length $n$ formed by the first $n$ terms of the sequence $\mathbf{s}$. It is easy to see that $L_n(\mathbf{s}) = L_n(\mathbf{s}_n)$ and $L_n(\mathbf{s}) \leq L_{n'}(\mathbf{s})$ when $n \leq n'$.

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

Let $\mathbf{s}$ be a sequence obtained from $\mathbf{s}(f)$ by changing $k$ of the first $n$ terms. We prove the proposition by induction on $k$. When $k = 0$, the result follows by Lemma 4.1. Assume that the result is true for any integer less than $k$, that is, for $1 \le t < k$,

$$L_{n,t}(\mathbf{s}(f)) \ge \frac{n + (2^{t+1} - 1) - (2^{t+1} - 1)d}{2(2^{t+1} - 1)}$$

for all $n \ge t$. Let $\lambda \in [0, 1]$ be a rational number.

*Case 1: all $k$ errors appear in the first $\lambda n$ terms.* By Lemma 4.2, the linear complexity of $\mathbf{s}$ satisfies

$$L_n(\mathbf{s}) \ge \frac{n + 1 - d - 2\lambda n}{2},$$

that is,

$$L_{n,k}(\mathbf{s}(f)) \ge \frac{n + 1 - d - 2\lambda n}{2}.$$

*Case 2: all $k$ errors appear in the last $(1 - \lambda)n$ terms.* Since the first $\lambda n$ terms of $\mathbf{s}$ and $\mathbf{s}(f)$ are same,

$$L_n(\mathbf{s}) \ge L_{\lambda n}(\mathbf{s}) = L_{\lambda n}(\mathbf{s}(f)).$$

However, $\mathbf{s}(f)$ is $d$-perfect, so that

$$L_{\lambda n}(\mathbf{s}(f)) \ge \frac{\lambda n + 1 - d}{2},$$

that is,

$$L_{n,k}(\mathbf{s}(f)) \ge \frac{\lambda n + 1 - d}{2}.$$

*Case 3: $r$ errors appear in the first $\lambda n$ terms with $r \le k - 1$.* Now

$$L_n(\mathbf{s}) L_{\lambda n}(\mathbf{s}) \ge L_{\lambda n, r}(\mathbf{s}(f)) \ge L_{\lambda n, k-1}(\mathbf{s}(f)).$$

By induction,

$$L_{\lambda n,k-1}(\mathbf{s}(f)) \ge \frac{\lambda n + (2^k - 1) - (2^k - 1)d}{2(2^k - 1)}.$$

Thus,

$$L_{\lambda n,k}(\mathbf{s}(f)) \ge \frac{\lambda n + (2^k - 1) - (2^k - 1)d}{2(2^k - 1)}.$$

Summarising these three cases,

$$L_{n,k}(\mathbf{s}(f)) \ge \min\left\{\frac{n + 1 - d - 2\lambda n}{2}, \frac{\lambda n + 1 - d}{2}, \frac{\lambda n + (2^k - 1) - (2^k - 1)d}{2(2^k - 1)}\right\}. \quad (4.1)$$

The second of the three terms in (4.1) is never less than the third, so the maximum of the right-hand side of (4.1) occurs when

$$\frac{n + 1 - d - 2\lambda n}{2} = \frac{\lambda n + (2^k - 1) - (2^k - 1)d}{2(2^k - 1)}. \quad (4.2)$$

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

Solving (4.2) gives $\lambda = (2^k - 1)/(2^{k+1} - 1)$ and substituting $\lambda$ in (4.1) gives

$$L_{n,k}(\mathbf{s}(f)) \geq \frac{n + (2^{k+1} - 1) - (2^{k+1} - 1)d}{2(2^{k+1} - 1)}.$$

Our result follows. □

Remark 4.4. From Proposition 4.3, when the error $k$ is much smaller than the length $n$, the sequence $\mathbf{s}(f)$ has both large linear complexity and large error linear complexity. However, the sequence is an example of an automatic sequence and has weak randomness properties.

## References


[1] Z. Chen, V. Edemskiy, P. Ke and C. Wu, 'On $k$-error linear complexity of pseudorandom binary sequences derived from Euler quotients', *Adv. Math. Comm.* **12** (2018), 805–816.

[2] C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science, 561 (Springer, Berlin, 1991).

[3] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions* (Academic Press, New York, 1951).

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

[5] H. Hu, G. Gong and D. Feng, 'New results on periodic sequences with large $k$-error linear complexity', in: *Proc. Int. Sympos. Information Theory, Toronto, Canada, 2008* (IEEE, New York, 2008), 2409–2413.

[6] H. Hu, L. Hu and D. Feng, 'On a class of pseudorandom sequences from elliptic curves over finite fields', *IEEE Trans. Inform. Theory* **53** (2007), 2598–2605.

[7] K. Kurosawa, F. Sato, T. Sakata and W. Kishimoto, 'A relationship between linear complexity and $k$-error linear complexity', *IEEE Trans. Inform. Theory* **46** (2000), 694–698.

[8] 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** (2002), 2817–2825.

[9] W. Meidl and H. Niederreiter, 'Linear complexity, $k$-error linear complexity, and the discrete Fourier transform', *J. Complexity* **18** (2002), 87–103.

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

[11] H. Niederreiter, 'Sequences with almost perfect linear complexity profile', in: *Advances in Cryptology—EUROCRYPT'87*, Lecture Notes in Computer Science, 304 (Springer, Heidelberg, 1988), 37–51.

[12] H. Niederreiter, 'Periodic sequences with large $k$-error linear complexity', *IEEE Trans. Inform. Theory* **49** (2003), 501–505.

[13] 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** (1993), 1398–1401.

[14] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd edn, Graduate Texts in Mathematics, 254 (Springer, Berlin, Heidelberg, 1993).

[15] H. Tong, 'Multisequences with large linear and $k$-error linear complexity from a tower of Artin–Schreier extensions of function fields', *Finite Fields Appl.* **18** (2012), 842–854.

[16] C. Xing and Y. Ding, 'Multi-sequences with large linear complexity and $k$-error linear complexity from Hermitian function fields', *IEEE Trans. Inform. Theory* **55** (2009), 3858–3863.

[17] C. Xing and K. Y. Lam, 'Sequences with almost perfect linear complexity profile and curves over finite fields', *IEEE Trans. Inform. Theory* **45** (1999), 1267–1270.

[18] C. Xing, H. Niederreiter, K. Y. Lam and C. Ding, 'Constructions of sequences with almost perfect linear complexity profile from curves over finite fields', *Finite Fields Appl.* **5** (1999), 301–313.


https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press

YUHUI ZHOU, Department of Mathematics,
Shanghai University, Shanghai, China
e-mail: yuhui1234@shu.edu.cn

YUHUI HAN, Department of Mathematics,
Shanghai University, Shanghai, China
e-mail: 97Aimee@shu.edu.cn

YANG DING, Department of Mathematics,
Shanghai University, Shanghai, China
e-mail: dingyang@t.shu.edu.cn

https://doi.org/10.1017/S0004972719001321 Published online by Cambridge University Press