On the $k$-error linear complexity of $l$-sequences

Lin Tan$^a$, Wen-Feng Qi$^a,b,*$

$^a$ Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, P.O. Box 1001-745, 450002, Zhengzhou, PR China

$^b$ State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, PR China

Abstract

This paper studies the stability of the linear complexity of $l$-sequences. Let $\xi$ be an $l$-sequence with linear complexity attaining the maximum $\text{per}(\xi)/2 + 1$. A tight lower bound and an upper bound on $\text{minerror}(\xi)$, i.e., the minimal value $k$ for which the $k$-error linear complexity of $\xi$ is strictly less than its linear complexity, are given. In particular, for an $l$-sequence $\xi$ based on a prime number of the form $2r + 1$, where $r$ is an odd prime number with primitive root 2, it is shown that $\text{minerror}(\xi)$ is very close to $r$, which implies that this kind of $l$-sequences have very stable linear complexity.

© 2010 Published by Elsevier Inc.

1. Introduction

Let $\xi = (s_0, s_1, \ldots)$ be a sequence over the finite field $\mathbb{F}_2$. If there exists a positive integer $T$ such that $s_i = s_{i+T}$ for all $i \geq 0$, then $\xi$ is called a $T$-periodic sequence and denoted by $\xi = (s_0, s_1, \ldots, s_{T-1})^\infty$. The minimum value of $T$ is called the period of $\xi$ and denoted by $\text{per}(\xi)$. If $\xi = (s_0, s_1, \ldots)$ satisfies the linear recurrence relation

$$s_i + d_1s_{i-1} + \cdots + d_Ls_{i-L} = 0, \quad i \geq L,$$

where $d_1, d_2, \ldots, d_L \in \mathbb{F}_2$, then the polynomial $f(x) = x^L + d_1x^{L-1} + \cdots + d_L$ is called a characteristic polynomial of $\xi$. Furthermore, if $m_2(x) \in \mathbb{F}_2[x]$ is a characteristic polynomial of $\xi$, and all characteristic polynomials of $\xi$ are divisible by $m_2(x)$, then $m_2(x)$ is called the minimal polynomial of $\xi$. The degree

$*$ This work was supported by the NSF of China under Grant Number 60833008.

* Corresponding author at: Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, P.O. Box 1001-745, 450002, Zhengzhou, PR China.

E-mail addresses: tanlin100@163.com (L. Tan), wenfeng.qi@263.net (W.-F. Qi).

1071-5797/$ – see front matter © 2010 Published by Elsevier Inc.
of $m_2(x)$ is called the linear complexity of $s$ and denoted by $LC(s)$. In engineering terms, $LC(s)$ is the length of the shortest linear feedback shift register that can generate $s$. The linear complexity of the zero sequence is defined to be 0.

A cryptographically strong sequence should not only have a large linear complexity, but also the change of a few terms should not cause significant decrease of linear complexity. This leads to the notion of $k$-error linear complexity proposed by Stamp and Martin in [9], which is similar to the earlier notion of sphere complexity in [8]. The $k$-error linear complexity of a periodic sequence $s$ is the minimum linear complexity that can be obtained for $s$ by modifying up to $k$ terms in one period (and modifying all other periods in the same way). In [10], K. Kurosawa et al. introduced $minerror(s)$ to denote the minimum number of terms that have to be changed within one period to decrease the linear complexity of $s$, and gave its explicit formula for $2^n$-periodic binary sequences. For a $p^n$-periodic binary sequence $s$, where $p$ is an odd prime number and $2$ is a primitive root modulo $p^2$, the tight lower and upper bounds on $minerror(s)$ were derived in [11]. Later the results were generalized to $p^n$-periodic sequences over the finite field $\mathbb{F}_q$ in [12]. For a $2p^n$-periodic binary sequence $s$, where $p$ is an odd prime number and $2$ is a primitive root modulo $p^2$, the lower and upper bounds on $minerror(s)$ were also given in [13].

Feedback with carry shift registers (FCSRs) are a class of nonlinear sequence generators and were introduced by A. Klapper and M. Goresky in [1]. Maximal length FCSR sequences are called l-sequences. It is well known that l-sequences have very good pseudorandom properties, such as good distribution properties, correlation properties and large linear complexity, see [2–7].

Let $p$ be a prime number. If 2 is a primitive root modulo $p$, then $p$ is called a 2-prime number. Moreover, if $p = 2r + 1$ is a 2-prime number and $r$ is itself a 2-prime number, then $p$ is called a strong 2-prime number.

So far the linear complexity of l-sequences has not been theoretically determined except the case of l-sequences based on strong 2-prime numbers. The upper bound on the linear complexity of an l-sequence $s$ is known to be $\text{per}(s)/2 + 1$, and the lower bound was studied in [6] and [7]. Experiments show that there are a large number of l-sequences whose linear complexity attain the upper bound.

In this paper we study $minerror(s)$ for an l-sequence $s$ with the maximal linear complexity, i.e., $LC(s) = \text{per}(s)/2 + 1$. A tight lower bound and an upper bound on $minerror(s)$ are provided. For an l-sequence $s$ based on strong 2-prime number, we drive the explicit formula of $minerror(s)$ and prove that when connection integer is large, the linear complexity is very stable.

The paper is organized as follows. In Section 2, we review some properties of l-sequences, and give a lower bound on the $k$-error linear complexity of binary periodic sequences with complementarity property. In Section 3 a lower bound and an upper bound on $minerror(s)$ are provided. In Section 4 an explicit formula of $minerror(s)$ for an l-sequence based on a strong 2-prime number is presented and its asymptotic value is given.

In this paper, for any positive integer $n$, $\{0, 1, \ldots, n - 1\}$ is chosen as the complete set of representatives for the elements of the integer residue ring $\mathbb{Z}/(n)$.

2. Preliminaries

2.1. l-Sequences

A detailed introduction on FCSRs can be found in [2]. An l-sequence is the output sequence from a maximum period FCSR with connection integer $p^s$, where $p$ is an odd prime number and 2 is a primitive root modulo $p^s$. Its period is $\varphi(p^s)$, where $\varphi$ is Euler’s phi function. It has the exponential representation as follows.

**Lemma 2.1.** (See [2].) Let $s = (s_0, s_1, \ldots)$ be an l-sequence based on $p^s$, and $\gamma = 2^{-1} \in \mathbb{Z}/(p^s)$ be the multiplicative inverse of 2 in the ring $\mathbb{Z}/(p^s)$. Then there exists a unique $A \in \mathbb{Z}/(p^s)$ such that $\gcd(A, p) = 1$ and

$$s_i = A \cdot \gamma^i \pmod{p^s} \pmod{2}, \quad i \geq 0.$$  (1)
Here the notation \((\mod p^e)(\mod 2)\) means that first the number \(A \cdot \gamma^i\) is reduced modulo \(p^e\) to give a number between 0 and \(p^e - 1\), then that number is reduced modulo 2 to give an element in \(\{0, 1\}\).

For a binary sequence \(\xi\) of even period \(T\), if \(\xi_i + \xi_{i+T/2} = 1\) for \(0 \leq i < T/2\), then we say that \(\xi\) has the complementarity property. From Lemma 2.1 it can be seen that \(l\)-sequences have the complementarity property. With respect to the linear complexity of \(l\)-sequences, the following results hold.

**Lemma 2.2.** (See [6].) Let \(\xi\) be an \(l\)-sequence based on \(p^e\) and \(T = \varphi(p^e)\). Then \(LC(\xi) \leq T/2 + 1\).

**Lemma 2.3.** (See [6].) Let \(q = 2r + 1\) be a strong 2-prime number and \(\xi\) be an \(l\)-sequence based on \(q\). Then \(LC(\xi) = r + 1\).

### 2.2. Linear complexity and \(k\)-error linear complexity

Let \(\xi = (s_0, s_1, \ldots, s_{T-1})^\infty\) be a binary sequence of period \(T\). The generating function of \(\xi\) is defined as

\[
s(x) = s_0 + s_1x + \cdots + s_ix^i + \cdots = \sum_{i=0}^{\infty} s_ix^i.\]

Denote

\[
s^T(x) = s_0 + s_1x + \cdots + s_{T-1}x^{T-1},\]

which can be seen as the generating function of the vector \((s_0, s_1, \ldots, s_{T-1})\). Then

\[
s(x) = \frac{s^T(x)}{1 + x^T} = \frac{s^T(x) / \gcd(s^T(x), 1 + x^T)}{(1 + x^T)/ \gcd(s^T(x), 1 + x^T)}. \tag{2}\]

The linear complexity of \(\xi\) can be given by (cf. [8,15])

\[
LC(\xi) = T - \deg(\gcd(1 + x^T, s^T(x))). \tag{3}\]

Suppose \(T\) is even and that \(\xi\) has the complementarity property. Let \(s^{T/2}(x)\) denote the generating function of the vector \((s_0, s_1, \ldots, s_{T/2-1})\), that is

\[
s^{T/2}(x) = \sum_{i=0}^{T/2-1} s_i x^i, \tag{4}\]

and denote \(s'(x) = (1 + x)s^{T/2}(x) + x^{T/2}\). Then

\[
s^T(x) = s^{T/2}(x) + x^{T/2} \cdot \left( s^{T/2}(x) + \frac{1 + x^{T/2}}{1 + x} \right) = s'(x) \cdot \frac{1 + x^{T/2}}{1 + x}. \tag{5}\]

Thus \((1 + x)(1 + x^{T/2})\) is a characteristic polynomial of \(\xi\).
Let $W_H(s)$ denote the Hamming weight of binary sequence $s$, i.e., the number of 1’s in one period of $s$, and for a $T$-periodic binary sequence $s$, let $W_H(s, T)$ denote the number of 1’s in one $T$-periodic length of $s$. For any integer $0 \leq k \leq T$, the $k$-error linear complexity $LC_k(s)$ of $s$ can be given by

$$LC_k(s) = \min_{W_H(e, T) \leq k} LC(s + e),$$

where $e$ runs over all $T$-periodic binary sequences with $W_H(e, T) \leq k$.

For a polynomial $f(x) \in F_2[x]$, let $W(f(x))$ denote its weight, i.e., the number of the nonzero coefficients of $f(x)$.

**Lemma 2.4.** Let $f(x) \in F_2[x]$. If $W(f(x))$ is odd, then for any polynomial $g(x) \in F_2[x]$, there exists a polynomial $h(x) \in F_2[x]$ such that $\deg(h(x)) < \deg(f(x))$ and $g(x) \equiv (1 + x)h(x) \pmod{f(x)}$.

**Proof.** Since $W(f(x))$ is odd, it follows that $\gcd(1 + x, f(x)) = 1$. Then there exists a polynomial $h(x) \in F_2[x]$ such that $1 = (1 + x)h(x) \pmod{f(x)}$. Thus the lemma holds. □

**Lemma 2.5.** Let $T = 2^n$, $\gcd(2, n) = 1$, $0 \leq k < T/2$, and $s$ be a binary sequence with complementarity property and period $T$. If $e$ is a $T$-periodic binary sequence such that $W_H(e, T) \leq k$ and $LC_k(s) = LC(s + e)$, then $2^t \mid \mbox{per}(s + e)$.

**Proof.** If $t = 0$, the result is trivial. In the following assume $t > 0$. If $2^t \nmid \mbox{per}(s + e)$, then $\mbox{per}(s + e) \nmid T/2$, that is,

$$s_i + e_i = s_{i + T/2} + e_{i + T/2}, \quad i \geq 0. \quad (6)$$

Since $s$ has the complementarity property, it follows that $e_i + e_{i + T/2} = 1$ for $i \geq 0$. It implies $W_H(e, T) = T/2$. This leads to a contradiction with $W_H(e, T) \leq k < T/2$. Thus $2^t \mid \mbox{per}(s + e)$. □

**Corollary 2.1.** Let $T = 2^n$, $\gcd(2, n) = 1$, and $s$ be a binary sequence with complementarity property and period $T$. For any integer $0 \leq k < T/2$, it follows that

$$LC_k(s) \geq 2^{t-1} + 1. \quad (7)$$

**Proof.** Suppose $e$ be a $T$-periodic binary sequence such that $LC_k(s) = LC(s + e)$, and let $m_{e+\xi}(x)$ be the minimum polynomial of $s + e$. From Lemma 2.5 we know $2^t \mid \mbox{per}(s + e)$. Let $\mbox{per}(s + e) = 2^t \nu$ with $\nu \mid n$, and let

$$1 + x^\nu = \prod_{i=0}^{r} f_i(x),$$

where $f_0(x) = 1 + x$ and $f_i(x)$ is an irreducible polynomial over $F_2$ for $1 \leq i \leq r$. Since

$$m_{e+\xi}(x) \mid (1 + x^\nu)^{2^t}$$

and the order of $m_{e+\xi}(x)$ is $2^t \nu$, there must exist some $0 \leq j \leq r$ such that

$$f_j(x)^{2^{t-1} + 1} \mid m_{e+\xi}(x).$$

Thus $LC(s + e) \geq 2^{t-1} + 1$. □
3. Basic results

In this section, we provide a tight lower bound and an upper bound on \( \minerror(s) \) for an \( l \)-sequence \( s \) with the maximal linear complexity.

**Theorem 3.1.** Let \( s = (s_0, s_1, \ldots, s_{T-1})^\infty \) be an \( l \)-sequence based on \( q \) of period \( T \). Then \( \minerror(s) \geq 2 \).

Furthermore, if \( q > 13 \) and \( \minerror(s) = 2 \), then the two bits to be changed must be \( s_i \) and \( s_{i + T/2} \) for some \( 0 \leq i < T/2 \).

**Proof.** Let \( e \) be any binary sequence of period \( T \) such that \( W_H(e) = 1 \), and let \( e^T(x) = x^i \) with \( 0 \leq i \leq T - 1 \). Then by (5) we have

\[
s^T(x) + e^T(x) = s'(x) \cdot \frac{1 + x^{T/2}}{1 + x} + x^i.
\]

It follows that

\[
\gcd\left(s^T(x) + e^T(x), \frac{1 + x^{T/2}}{1 + x}\right) = 1,
\]

and so by (3) we have

\[
LC(s + e) \geq T - 2.
\]

Since \( LC(s) \leq T/2 + 1 \), it follows that \( LC(s + e) \geq LC(s) \) if \( T > 4 \). If \( T = 4 \), then it is clear that \( LC(s + e) \geq LC(s) \) also holds. It implies \( LC_1(s) = LC(s) \). Thus \( \minerror(s) \geq 2 \).

If \( \minerror(s) = 2 \), let \( e \) be a \( T \)-periodic binary sequence such that \( W_H(e, T) = 2 \) and \( LC_2(s) = LC(s + e) \), and let \( e^T(x) = x^d + x^j \), where \( 0 \leq i < j \leq T - 1 \). Then

\[
s(x) + e(x) = \frac{s'(x)(1 + x^{T/2}) + x^d(1 + x^{j-i})(1 + x)}{(1 + x^d)(1 + x)}.
\]

(8)

Assume

\[
\gcd(1 + x^{T/2}, 1 + x^{j-i}) = 1 + x^d,
\]

where \( d = \gcd(T/2, j - i) \). Then

\[
s(x) + e(x) = \frac{s'(x)(1 + x^{T/2})/((1 + x^d)(1 + x)) + x^d(1 + x^{j-i})/((1 + x^d))}{(1 + x^d)/(1 + x^d)}.
\]

(9)

For any positive integer \( n \), let \( v_2(n) \) denote the exponent of the highest power of 2 that divides \( n \), i.e., \( 2^{v_2(n)} | n \) but \( 2^{v_2(n)+1} \nmid n \).

Suppose \( v_2(j - i) < v_2(T/2) \). Then

\[
\gcd\left(1 + x^{T/2}, \frac{1 + x^{j-i}}{1 + x^d}\right) = 1.
\]
If \( v_2(T/2) > 1 \), then for any irreducible nonconstant polynomial \( f(x) \in \mathbb{F}_2[x] \) such that \( f(x) | (1 + x^T) \), we have

\[
\frac{1 + x^{T/2}}{(1 + x^d)(1 + x)} \quad \text{but} \quad \frac{x^i(1 + x^{j-i})}{1 + x^d}.
\]

Thus it follows from (9) and (3) that

\[
LC(s + e) \geq T - d.
\]

If \( v_2(T/2) = 1 \), then \( v_2(d) = 0 \) and \( v_2(T) = 2 \). For any irreducible nonconstant polynomial \( f(x) \in \mathbb{F}_2[x] \) such that \( f(x) | (1 + x^T) \) and \( f(x) \neq 1 + x \), we have

\[
\frac{1 + x^{T/2}}{(1 + x^d)(1 + x)} \quad \text{but} \quad \frac{x^i(1 + x^{j-i})}{1 + x^d}.
\]

Thus

\[
gcd \left( \frac{s'(x)(1 + x^{T/2})}{(1 + x^d)(1 + x)} + \frac{x^i(1 + x^{j-i})}{1 + x^d}, \frac{1 + x^T}{1 + x^d} \right) \mid (1 + x)^3.
\]

So it follows from (9) and (3) that

\[
LC(s + e) \geq T - d - 3.
\]

On the other hand, since \( LC(s + e) < T/2 + 1 \), we have \( T/2 < d + 4 \). Moreover, since \( d \mid T/2 \) and \( v_2(d) < v_2(T/2) \), then \( 2d \leq T/2 \). Thus \( d \leq 3 \). But if \( q > 13 \), then \( T > 12 \). It implies \( d > 3 \). Thus \( v_2(j - i) \geq v_2(T/2) \). Then by (9) and (3) we have

\[
2(T/2 - d) + 1 \leq LC(s + e) < T/2 + 1.
\]

Thus \( d = T/2 \). Then \( j = i + T/2 \). This completes the proof. \( \Box \)

**Remark 3.1.** In fact for any binary sequence \( s \) with complementarity property and period larger than 12, the result in Theorem 3.1 holds. The lower bound on \( \text{minerr}(s) \) can be reached by many \( l \)-sequences with connection integers such as \( 13^e \), \( 19^e \) and \( 37^e \).

A sequence \( u \) over \( \mathbb{Z}/(p^e) \) is called 1st-order primitive sequence if \( u \) can be generated by \( x - \gamma \), where \( \gamma \) is a primitive root modulo \( p^e \) and \( u \neq 0 \pmod{p} \). From Lemma 2.1, we know that an \( l \)-sequence based on \( p^e \) can be considered as a reduction modulo 2 of a 1st-order primitive sequence over \( \mathbb{Z}/(p^e) \). Every element in \( \mathbb{Z}/(p^e) \) has a unique \( p \)-adic expansion, so a sequence \( u \) over \( \mathbb{Z}/(p^e) \) has a unique \( p \)-adic expansion as

\[
u = u_0 + u_1 \cdot p + \cdots + u_{e-1} \cdot p^{e-1}, \tag{10}\]

where each \( u_i \) is a sequence over \( \mathbb{Z}/(p) \) and called the \( i \)th-level sequence of \( u \) for \( 0 \leq i \leq e - 1 \).

Let \( (u \mod m) \) denote the reduction sequence of \( u \) modulo \( m \), that is,

\[
(u \mod m) = (u_0 \mod m, u_1 \mod m, \ldots).
\]

For a 1st-order primitive sequence \( u \) over \( \mathbb{Z}/(p^e) \), \( e \geq 2 \), the period and a characteristic polynomial of binary sequence \( (u_{e-1} \mod 2) \) were given in [14].
Lemma 3.1. (See [14].) Let $p^e$ be an odd prime power with $e \geq 2$, $u$ be a 1st-order primitive sequence over $\mathbb{Z}/(p^e)$, and let $\text{per}(u_{e-1}, 2)$ denote the period of $(u_{e-1} \mod 2)$. Then
\[
\text{per}(u_{e-1}, 2) = p^{e-1} \cdot (p - 1)/2.
\]

Lemma 3.2. (See [14].) Let $p^e$ be an odd prime power with $e \geq 2$ and $u$ be a 1st-order primitive sequence over $\mathbb{Z}/(p^e)$. Then $(1 + x)(1 + x^{p^e-1}(p-1)/2)/(1 + x^{p^e-2}(p-1)/2)$ is a characteristic polynomial of $(u_{e-1} \mod 2)$.

In the following for an $l$-sequence $s$ based on $p^e$, we always let $u = (u_0, u_1, \ldots)$, where $u_i = A \cdot \gamma^i \,(\text{mod } p^e)$ for $i \geq 0$, be the sequence over $\mathbb{Z}/(p^e)$ such that $s = (u \mod 2)$ with period $T = p^{e-1}(p - 1)$. Let $u_n$ denote the $n$th-level sequence of $u$. $T_n = \text{per}(u_n, 2) = p^e(p - 1)/2$, and $u_n^T(x)$ be the polynomial corresponding to $(u_n \mod 2)$ for $0 \leq n \leq e - 1$.

Corollary 3.1. Let $s$ be an $l$-sequence based on $p^e$, where $e \geq 2$. If $s$ has the maximal linear complexity, then for any integer $c < e$, $l$-sequences based on $p^c$ also have the maximal linear complexity.

Proof. According to (10) we have
\[
\frac{A}{p^e} = u \text{ (mod } p^e)\,(\text{mod } 2) + (u_c \mod 2) + \cdots + (u_{e-1} \mod 2).
\]

It is clear that $u \,(\text{mod } p^c)\,(\text{mod } 2)$ is an $l$-sequence based on $p^e$. Denote $u \,(\text{mod } p^c)\,(\text{mod } 2) = g$. Then
\[
\frac{A}{p^e} = g + (u_c \mod 2) + \cdots + (u_{e-1} \mod 2).
\]

From Lemma 3.2 we know that $(1 + x)(1 + x^{p^e-1}(p-1)/2)/(1 + x^{p^e-2}(p-1)/2)$ is a characteristic polynomial of $(u_n \mod 2)$ for $c \leq n \leq e - 1$. Let $m_g(x)$ denote the minimal polynomial of $g$. If $s$ has the maximal linear complexity, then the minimal polynomial of $s$ is $(1 + x)(1 + x^{p^e-1}(p-1)/2)$. Since $(1 + x^{p^e-1}(p-1)/2)/(1 + x^{p^e-2}(p-1)/2)$, $c \leq n \leq e - 1$, are pairwise relatively prime, it follows that
\[
1 + x^{p^e-1}(p-1)/2 \mid m_g(x).
\]

On the other hand, since $\text{per}(g) = p^{e-1}(p - 1)$ and $m_g(x) \mid (1 + x)(1 + x^{p^{e-1}(p-1)/2})$, it follows that
\[
m_g(x) = (1 + x)(1 + x^{p^{e-1}(p-1)/2}).
\]

This proves the corollary. □

If a $T$-periodic binary sequence $g$ satisfies $W_H(g, T) = \text{minerror}(s)$ and $\text{LC}(s + g) < \text{LC}(s)$, then $g$ is called a critical error sequence of $s$, see [10].

Theorem 3.2. Let $s$ be an $l$-sequence based on $p^e$ with the maximal linear complexity, and let $g$ be an $l$-sequence based on $p^c$, where $c < e$. If $g$ has a per($g$)/2-periodic critical error sequence, then
\[
\text{minerror}(g) \leq \text{minerror}(q).
\]

Proof. Let $N = \text{per}(g) = p^{e-1}(p - 1)$, $a^N(x)$ be the polynomial corresponding to $g$ and $a^{N/2}(x)$ be defined as in (4). According to (11) we have
\[ s^T(x) = a N(x) \cdot \frac{1 + x^T}{1 + x^N} + \sum_{n=c}^{e-1} \left( u_n^T(x) \cdot \frac{1 + x^T}{1 + x^T_n} \right) \]

\[ = \frac{1 + x^{T/2}}{1 + x} \cdot \left( a'(x) \cdot \frac{1 + x^{T/2}}{1 + x^{N/2}} + \sum_{n=c}^{e-1} \left( u_n^T(x) \cdot \frac{(1 + x)(1 + x^{T/2})}{1 + x^T_n} \right) \right). \]

where \( a'(x) = (1 + x)a^{N/2}(x) + x^{N/2}. \)

Denote \( K(x) = a'(x) \cdot \frac{1 + x^{T/2}}{1 + x^{N/2}} + \sum_{n=c}^{e-1} \left( u_n^T(x) \cdot \frac{(1 + x)(1 + x^{T/2})}{1 + x^T_n} \right). \)

From Lemma 3.2 we know that \( (1 + x)(1 + x^{T_n})/(1 + x^{T_n/p}) \) is a characteristic polynomial of \((u_n \mod 2)\) for \( c \leq n \leq e - 1. \) Then by (2) there exists a polynomial \( g(x) \) such that

\[ \frac{u_n^T(x)}{1 + x^{T_n}} = \frac{g(x)}{(1 + x)(1 + x^{T_n})(1 + x^{T_n/p})}. \]

It follows that \( u_n^T(x) = g(x)(1 + x^{T_n/p})/(1 + x). \) Thus

\[ \frac{1 + x^{T_n/p}}{1 + x} \bigg| u_n^T(x), \quad c \leq n \leq e - 1. \]

That is

\[ (1 + x^{T_n/p}) \bigg| (1 + x)u_n^T(x), \quad c \leq n \leq e - 1. \]

Since \( N/2 \big| T_n/p \) for \( c \leq n \leq e - 1, \) it follows that

\[ (1 + x^{N/2}) \bigg| (1 + x)u_n^T(x), \quad c \leq n \leq e - 1. \] (12)

Suppose \( g \) has an \( N/2 \)-periodic critical error sequence \( e, \) and denote

\[ e^N(x) = (1 + x^{N/2})e(x), \]

where \( \deg(e(x)) < N/2. \) By (3) we know that there exists a nonconstant polynomial \( f(x) \big| (1 + x^{N/2}) \) such that

\[ f(x) \bigg| (a'(x) + (1 + x)e(x)). \]

Then by (12) we have

\[ K(x) \equiv a'(x) \frac{1 + x^{T/2}}{1 + x^{N/2}} \equiv a'(x) \pmod{f(x)}. \]

Therefore

\[ f(x) \bigg| (K(x) + (1 + x)e(x)). \]
This together with (3) implies that
\[ \text{LC}(s + e) \leq \text{LC}(s) - \deg(f(x)). \]

Hence
\[ \minerror(s) \leq W\left((1 + x^{T/2})e(x)\right) = 2W(e(x)) = \minerror(g). \]

This proves the theorem. \(\square\)

According to Theorem 3.2 and Theorem 3.1, we have the following corollary.

**Corollary 3.2.** Let \( q \) be an \( l \)-sequence based on \( p^c \) and \( s \) be an \( l \)-sequence based on \( p^e \), where \( e > c \). If \( \minerror(q) = 2 \), then \( \minerror(s) = 2 \).

Let \( s \) be an \( l \)-sequence based on \( p^e > 5 \). Then it can been shown that \( T = \varphi(p^e) \) is not a power of 2. Denote
\[ S(x) = (1 + x)s^{T/2}(x) + 1 \quad (13) \]
and let \( C \) denote the set of all nonconstant polynomials that divide \( 1 + x^{T/2} \) over \( \mathbb{F}_2 \). Define the set
\[ C' = \{ g(x) \mid (1 + x)g(x) \equiv S(x) \pmod{f(x)}, \ g(x) \in \mathbb{F}_2[x], \deg(g(x)) < T/2, \ f(x) \in C \}. \quad (14) \]
Since there at least exists an irreducible polynomial \( f(x) \mid (1 + x^{T/2}) \) with \( W(f(x)) \) odd, it follows by Lemma 2.4 that the set \( C' \) is nonempty.

The following theorem gives an upper bound on \( \minerror(s) \) for an \( l \)-sequence \( s \) with \( \text{LC}(s) = \text{per}(s)/2 + 1 \).

**Theorem 3.3.** Let \( s \) be an \( l \)-sequence based on \( p^e > 5 \) with the maximal linear complexity, and let the set \( C' \) be defined as in (14). Then
\[ \minerror(s) \leq 2 \cdot \min_{g(x) \in C'} W(g(x)). \]

**Proof.** We have
\[ s^T(x) = \frac{1 + x^{T/2}}{1 + x} \cdot s'(x), \]
where \( s'(x) = (1 + x)s^{T/2}(x) + x^{T/2} \). Since \( \text{LC}(s) = T/2 + 1 \), by (3) it follows that
\[ \gcd(1 + x^{T/2}, s'(x)) = 1. \]
For any \( g(x) \in C' \), there exits some polynomial \( f(x) \in C \) such that
\[ S(x) \equiv (1 + x)g(x) \pmod{f(x)}. \quad (15) \]
Let us take
\[ e^T(x) = (1 + x^{T/2})g(x). \]
Then
\[ s^T(x) + e^T(x) = \frac{1 + x^{T/2}}{1 + x} \cdot (s'(x) + (1 + x)g(x)). \]

By (15) and the definition of \( S(x) \), we have
\[ \|s'(x) + (1 + x)g(x)\| \equiv 0 \pmod{f(x)}. \]

Let \( e \) be the \( T \)-periodic binary sequence corresponding to \( e^T(x) \). Then by (3) we know
\[ \text{LC}(s + e) \leq \text{LC}(s) - \deg(f(x)). \]

Therefore
\[ \text{minerror}(s) \leq W(e^T(x)) = 2 \cdot W(g(x)). \]

This proves the theorem. \( \square \)

**Corollary 3.3.** Let \( s \) be an l-sequence based on \( p^e \) with the maximal linear complexity. If \( p = 2n + 1 \) and \( n \) has standard factorization \( n = 2^e_0 p_1^{e_1} \cdots p_t^{e_t} \), where \( e_0 \geq 0, e_i \geq 1, p_i \) is an odd prime number, \( 1 \leq i \leq t \), then
\[ \text{minerror}(s) \leq 2 \cdot \min_{1 \leq i \leq t} \text{ord}_{p_i}(2), \]

where \( \text{ord}_{p_i}(2) \) denotes the order of 2 modulo \( p_i \).

**Proof.** We denote
\[ m = \min_{1 \leq i \leq t} \text{ord}_{p_i}(2) \]

and without loss of generality, assume the minimum holds for \( p_1 \), i.e., \( m = \text{ord}_{p_1}(2) \). Let
\[ 1 + x^{p_1} = (1 + x) \cdot \prod_{j=1}^{(p_1-1)/m} f_j(x), \]

where \( f_j(x) \) is an irreducible polynomial over \( \mathbb{F}_2 \) and \( \deg(f_j(x)) = m \) for \( 1 \leq j \leq (p_1 - 1)/m \). Then we know
\[ f_j(x) \mid (1 + x^{T/2}), \quad 1 \leq j \leq (p_1 - 1)/m. \]

It is clear that \( W(f_j(x)) \) is odd for \( 1 \leq j \leq (p_1 - 1)/m \), and so by Lemma 2.4, there exists \( h_j(x) \in \mathbb{F}_2[x] \) such that \( \deg(h_j(x)) < m \) and
\[ S(x) \equiv (1 + x)h_j(x) \pmod{f_j(x)}, \]

where \( S(x) \) is described as in (15). Then from Theorem 3.3, we have
\[ \text{minerror}(s) \leq 2 \cdot \min_{1 \leq j \leq (p_1 - 1)/m} W(h_j(x)). \]
Since $W(h_j(x)) \leq m$ for $1 \leq j \leq (p_1 - 1)/m$, it follows that

$$\text{minerror}(s) \leq 2m = 2 \cdot \min_{1 \leq i \leq t} \text{ord}_{p_i}(2). \quad \square$$

4. Further results of $l$-sequences based on strong 2-prime numbers

In this section, we determine $\text{minerror}(s)$ for an $l$-sequence $s$ based on a strong 2-prime number and analyze its asymptotic value.

Let $s^{(2)} = (s_0, s_2, s_4, \ldots)$ denote the 2-fold decimation of an $l$-sequence $s$. Firstly we estimate the element distribution in a period of $s^{(2)}$. Then by the distribution property we study the stability of the linear complexity of $l$-sequences based on strong 2-prime numbers.

### 4.1. Element distribution of 2-fold decimation of $l$-sequences

The authors of reference [3] studied the partial period distribution of $l$-sequences. In this section similar techniques are used to estimate the proportion of 1's in a period of the 2-fold decimation of $l$-sequences.

**Lemma 4.1.** Let $p$ be a prime number, $s$ be an $l$-sequence based on $q = p^e$ of period $T = p^{e-1}(p - 1)$, and let $P(1)$ denote the proportion of 1's in a period of $s^{(2)}$. Then

$$\left| P(1) - \frac{1}{2} \right| < \frac{4}{T} q^{1/2} \cdot \left( \left( \frac{\ln q}{\pi} + \frac{1}{5} \right) \cdot \left( \frac{1 - p^{-e/2}}{1 - p^{-1/2}} \right) - \frac{(p^{-1/2} - ep^{-e/2} + (e - 1)p^{-(e+1)/2}\ln p)}{\pi (1 - p^{-1/2})^2} \right) + \frac{1}{2q}.$$ 

Before giving the proof of Lemma 4.1, we introduce three lemmas. For any positive integer $m$, define the function $e_m : \mathbb{R} \rightarrow \mathbb{R}$ by $e_m(a) = e^{2\pi ia/m}$ for any real number $a$. For any integer $c$, we have

$$\sum_{a=0}^{m-1} e_m(ca) = \begin{cases} m, & \text{if } m \mid c, \\ 0, & \text{else}. \end{cases} \quad (16)$$

**Lemma 4.2.** (See [15, p. 447].) For any positive integers $m$ and $H$, we have

$$\left| \sum_{a=1}^{m-1} \left| \sum_{x=0}^{H-1} e_m(ax) \right| \right| < 2m \cdot \left( \frac{1}{\pi} \ln m + \frac{1}{5} \right),$$

where $\ln(\cdot)$ is the natural logarithm.

For the sequence $u = (u_0, u_1, \ldots)$ over $\mathbb{Z}/(p^e)$, where $u_i = A \cdot \gamma^i \mod p^e$ for $i \geq 0$ and $\gamma$ is a primitive root modulo $p^e$, we have the following results.

**Lemma 4.3.** (See [3].) Let $u$ be as above. Then for any $0 \neq a \in \mathbb{Z}/(q)$ and any integer $h$, we have

$$\left| \sum_{n=0}^{T-1} e_q(au_n)e_T(hn) \right| \leq \delta^{1/2} q^{1/2},$$

where $\delta = \gcd(a, q)$. 

Lemma 4.4. Let \( u \) be as above. Then for any \( 0 \neq a \in \mathbb{Z}/(q) \), we have

\[
\left| \frac{1}{T} \sum_{n=0}^{T-1} e_q(u a n^2) \right| \leq \delta^{1/2} q^{1/2},
\]

where \( \delta = \gcd(a, q) \).

Proof. For any integers \( n \) and \( j \), by (16) we have

\[
\frac{1}{T} \sum_{h=0}^{T-1} e_T(h \cdot (n - j)) = \begin{cases} 1, & \text{if } T \mid (n - j), \\ 0, & \text{otherwise}. \end{cases}
\] (17)

Then for \( 0 \leq n \leq T - 1 \), we have

\[
\frac{1}{T} \sum_{j=0}^{T-1} \left( \frac{1}{T} \sum_{h=0}^{T-1} e_T(h \cdot (n - 2j)) \right) = \begin{cases} 1, & \text{if } n \text{ is even}, \\ 0, & \text{if } n \text{ is odd}. \end{cases}
\] (18)

Thus

\[
\frac{1}{T} \sum_{n=0}^{T-1} e_q(u a n^2) = \sum_{n=0}^{T-1} \left( e_q(u n) \cdot \frac{1}{T} \sum_{j=0}^{T-1} e_T(h \cdot (n - 2j)) \right)
\]

\[
= \frac{1}{T} \sum_{h=0}^{T-1} \left( \sum_{n=0}^{T-1} e_q(u n) e_T(hn) \cdot \frac{1}{T} \sum_{j=0}^{T-1} e_T(-2hj) \right).
\]

Then by Lemma 4.3, we have

\[
\left| \frac{1}{T} \sum_{n=0}^{T-1} e_q(u a n^2) \right| \leq \frac{1}{T} \sum_{h=0}^{T-1} \left( \left| \sum_{n=0}^{T-1} e_q(u n) e_T(hn) \right| \cdot \left| \sum_{j=0}^{T-1} e_T(-2hj) \right| \right)
\]

\[
\leq \delta^{1/2} q^{1/2} \frac{1}{T} \sum_{h=0}^{T-1} \sum_{j=0}^{T-1} e_T(-2hj).
\]

Since

\[
\sum_{h=0}^{T-1} \sum_{j=0}^{T-1} e_T(-2hj) = \sum_{h=0}^{T-1} \sum_{j=0}^{T-1} e_T(2hj) = \sum_{h=0}^{T-1} \sum_{j=0}^{T-1} e_T(2hj) = T,
\]

the lemma follows. \( \square \)
Proof of Lemma 4.1. We know $s^{(2)} = (u^{(2)} \mod 2)$. Since $\gamma$ is a primitive root modulo $q$, it follows that $\text{per}(s^{(2)}) | T/2$. For any $n \geq 0$, we have

$$
\frac{1}{q} \sum_{x=0}^{\frac{q-1}{2}} \sum_{a=0}^{q-1} e_q((u_n - 2x - 1) \cdot a) = \begin{cases} 0, & s_n = 0, \\ 1, & s_n = 1. \end{cases}
$$

(19)

Thus, the number of 1's in a $T/2$-period length of $s^{(2)}$ can be given by

$$
W_H(s^{(2)}, T/2) = \sum_{n=0}^{\frac{T}{2} - 1} s_{2n} = \sum_{n=0}^{\frac{T}{2} - 1} \left( \frac{1}{q} \sum_{x=0}^{\frac{q-1}{2}} \sum_{a=0}^{q-1} e_q((u_{2n} - 2x - 1) \cdot a) \right)
$$

$$
= \frac{1}{q} \sum_{a=0}^{q-1} \left( e_q(-a) \sum_{n=0}^{\frac{T}{2} - 1} e_q(a u_{2n}) \sum_{x=0}^{\frac{q-1}{2}} e_q(-2ax) \right)
$$

$$
= \frac{T(q-1)}{4q} + \frac{1}{q} \sum_{a=1}^{q-1} \left( e_q(-a) \sum_{n=0}^{\frac{T}{2} - 1} e_q(a u_{2n}) \sum_{x=0}^{\frac{q-1}{2}} e_q(-2ax) \right).
$$

Then

$$
P(1) = \frac{W_H(s^{(2)}, T/2)}{T/2} = \frac{q-1}{2q} + \frac{2}{qT} \sum_{a=1}^{q-1} \left( e_q(-a) \sum_{n=0}^{\frac{T}{2} - 1} e_q(a u_{2n}) \sum_{x=0}^{\frac{q-1}{2}} e_q(-2ax) \right).
$$

Therefore we have

$$
\left| P(1) - \frac{1}{2} \right| \leq \frac{2}{qT} \sum_{a=1}^{q-1} \left( \left| \sum_{n=0}^{\frac{T}{2} - 1} e_q(a u_{2n}) \right| \cdot \left| \sum_{x=0}^{\frac{q-1}{2}} e_q(-2ax) \right| \right) + \frac{1}{2q}.
$$

Suppose $a = a' p^l$, where $p \nmid a'$, $0 \leq l \leq e - 1$ and $1 \leq a' \leq p^{e-l} - 1$. Then

$$
\sum_{a=1}^{q-1} \left( \left| \sum_{n=0}^{\frac{T}{2} - 1} e_q(a u_{2n}) \right| \cdot \left| \sum_{x=0}^{\frac{q-1}{2}} e_q(-2ax) \right| \right) = \sum_{l=0}^{e-1} \sum_{a'=1}^{p^{e-l} - 1} \left( \left| \sum_{n=0}^{\frac{T}{2} - 1} e_q(a' p^l u_{2n}) \right| \cdot \left| \sum_{x=0}^{\frac{q-1}{2}} e_q(-2a' p^l x) \right| \right).
$$

According to Lemma 4.4, we know $| \sum_{n=0}^{\frac{T}{2} - 1} e_q(a' p^l u_{2n}) | \leq p^{l/2} q^{1/2}$, and so

$$
\left| P(1) - \frac{1}{2} \right| \leq \frac{2}{qT} \sum_{l=0}^{e-1} \sum_{a'=1}^{p^{e-l} - 1} \left( p^{l/2} q^{1/2} \cdot \left| \sum_{x=0}^{\frac{q-1}{2}} e_q(-2a' x) \right| \right) + \frac{1}{2q}
$$

$$
= \frac{2}{q} q^{-1/2} \cdot \sum_{l=0}^{e-1} \left( p^{l/2} \cdot \sum_{a'=1}^{p^{e-l} - 1} \sum_{x=0}^{\frac{q-1}{2}} e_{p^{e-l}}(-2a' x) \right) + \frac{1}{2q}.
$$
Since $\gcd(2, p) = 1$, by Lemma 4.2 we have
\[
\sum_{\alpha' = 1}^{p^{e-1}-1} \sum_{x=0}^{q-1} e^{p^{-i}(-2a'x)} \leq \sum_{\alpha' = 1}^{p^{e-1}-1} \sum_{x=0}^{q-1} e^{p^{-i}(a'x)} < 2p^{e-l}\left(\frac{1}{\pi} \ln p^{e-l} + \frac{1}{5}\right).
\]

Thus
\[
\left| P(1) - \frac{1}{2} \right| < \frac{2}{\pi} q^{-1/2} \cdot \sum_{i=0}^{e-1} \left( p^{l/2} \cdot 2p^{-i}\left(\frac{1}{\pi} \ln p^{e-l} + \frac{1}{5}\right) \right) + \frac{1}{2q}
\]
\[
= \frac{4}{\pi} q^{1/2} \cdot \sum_{i=0}^{e-1} \left( p^{-l/2} \cdot \left(\frac{1}{\pi} \ln q + \frac{1}{5} - \frac{1}{\pi} \ln p\right) \right) + \frac{1}{2q}
\]
\[
< \frac{4}{\pi} q^{1/2} \cdot \left( \sum_{i=0}^{e-1} \frac{p^{-l/2}}{p} - \frac{\ln p}{\pi} \sum_{i=0}^{e-1} \frac{p^{-l/2}}{p} \right) + \frac{1}{2q}
\]
\[
< \frac{4}{\pi} q^{1/2} \cdot \left( \sum_{i=0}^{e-1} \left(1 - p^{-l/2}\right) \left(1 - p^{-e/2}\right) \right) \frac{\ln p}{\pi (1 - p^{-1/2})^2} + \frac{1}{2q}.
\]

Lemma 4.1 implies that $|P(1) - \frac{1}{2}| \leq O(q^{-1/2} \ln q)$. Thus when the connection integer $q$ is large enough, the proportion of 1’s in a period of the 2-fold decimation of $l$-sequences approximates $1/2$.

4.2. Stability of $l$-sequences based on strong 2-prime numbers

The following theorem gives the formula of $\text{minerror}(\xi)$ for an $l$-sequence $\xi$ based on a strong 2-prime number.

**Theorem 4.1.** Let $q = 2r + 1$ be a strong 2-prime number and $\xi$ be an $l$-sequence based on $q$. Then
\[
\text{minerror}(\xi) = 2 \min(d, r - d) \quad \text{and} \quad \text{LC}_k(\xi) = 2,
\]
where $d = W_H(\xi^{(2)})$ and $k = \text{minerror}(\xi)$.

**Proof.** We know $\text{per}(\xi) = 2r$. Let $\xi = (s_0, s_1, \ldots, s_{2r-1})^\infty$ and $s'$ denote the $r$-tuple $(s_0, s_1, \ldots, s_{r-1})$. Let $a'$ denote the $r$-tuple $(0, 1, 0, 1, \ldots, 0)$, where 0 and 1 appear alternately. Since $\xi$ has the complementarity property, it can be seen that the Hamming distance between $s'$ and $a'$ is $W_H(\xi^{(2)})$.

By altering periodically $2 \min(d, r - d)$ bits for $\xi$, we can obtain a sequence with period 2, i.e., $(0, 1, 0, 1, \ldots)$ or $(1, 0, 1, 0, \ldots)$. Thus
\[
\text{minerror}(\xi) \leq 2 \min(d, r - d) < r.
\]

Let $k = \text{minerror}(\xi)$ and $\xi$ be a 2r-periodic binary sequence such that $\text{LC}_k(\xi) = \text{LC}(\xi + \xi)$. From Lemma 2.5 we know $\text{per}(\xi + \xi) = 2$ or $2r$. Let
\[
1 + x^r = (1 + x)^2 \Phi_r(x)^2,
\]
where \( \Phi_r(x) \) is the \( r \)th cyclotomic polynomial over \( \mathbb{F}_2 \). Since \( r \) is 2-prime, \( \Phi_r(x) \) is irreducible. If \( \text{per}(s + \varepsilon) = 2r \), then the minimum polynomial of \( s + \varepsilon \) is divisible by \((1 + x)^2 \Phi_r(x)\). It implies\( LC(s + \varepsilon) \geq r + 1 = LC(s) \), thus \( \text{per}(s + \varepsilon) = 2 \). Then \( \text{minerror}(s) = 2 \min(d, r - d) \). This completes the proof. □

According to Lemma 4.1, we can derive an asymptotic result given in the following theorem.

**Theorem 4.2.** Let \( q = 2r + 1 \) be a strong 2-prime number and \( s \) be an \( l \)-sequence based on \( q \). Then

\[
\lim_{r \to \infty} \frac{\text{minerror}(s)}{r} = 1.
\]

**Proof.** On one hand, by Lemma 4.1 we have

\[
\left| P(1) - \frac{1}{2} \right| < \frac{2(2r + 1)^{1/2}}{r} \cdot \left( \frac{\ln(2r + 1)}{\pi} + \frac{1}{5} \right) + \frac{1}{4r + 2},
\]

which implies that

\[
\lim_{r \to \infty} P(1) = \frac{1}{2}.
\]

On the other hand, it follows from Theorem 4.1 that

\[
\lim_{r \to \infty} \frac{\text{minerror}(s)}{r} = 2 \cdot \lim_{r \to \infty} \left( \min(P(1), 1 - P(1)) \right).
\]

Thus, the theorem follows from (21) and (22). □

It shows that the linear complexity of \( l \)-sequences based on strong 2-prime numbers is not only sufficiently large but also very stable.

For an \( l \)-sequence \( q \) based on a strong 2-prime number, its critical error sequence must be \( \text{per}(q)/2 \)-periodic. Thus by Theorem 4.1 and Theorem 3.2 we have the following corollary.

**Corollary 4.1.** Let \( q = 2r + 1 \) be a strong 2-prime number and \( a \) be an \( l \)-sequence based on \( q \). Then for any \( l \)-sequence \( s \) based on \( q^e \), we have

\[
\text{minerror}(s) \leq 2 \min(d, r - d),
\]

where \( d = W_H(a^{(2)}) \).

**Acknowledgments**

The authors are grateful to the reviewers for their helpful comments and suggestions.

**References**