LETTER

On the Distribution of p-Error Linear Complexity of p-Ary Sequences with Period p^n

Miao TANG[†], Juxiang WANG[††a)], *Nonmembers*, Minjia SHI[†††], *Member*, *and* Jing LIANG[††††], *Nonmember*

SUMMARY Linear complexity and the k-error linear complexity of periodic sequences are the important security indices of stream cipher systems. This paper focuses on the distribution of p-error linear complexity of p-ary sequences with period p^n. For p-ary sequences of period p^n with linear complexity $p^n - p + 1$, $n \geq 1$, we present all possible values of the p-error linear complexity, and derive the exact formulas to count the number of the sequences with any given p-error linear complexity.

key words: *periodic sequence, k-error linear complexity, counting function, stream ciphers*

1. Introduction

Sequences with good pseudorandomness and complexity properties are widely used as key streams in cryptographic applications [1]–[3]. Among the measures commonly used to measure the complexity of a sequence S is its linear complexity $LC(S)$. In engineering terms, the linear complexity $LC(S)$ is defined to be the length of the shortest linear feedback shift register (LFSR) that can generate S. The LFSR that generates a given sequence S can be determined by the well-known Berlekamp-Massey algorithm [4], for this algorithm requires only $2LC(S)$ consecutive bits to completely determine the linear complexity of S. Hence, high linear complexity is essential for cryptographic applications.

For a cryptographically strong sequence, the linear complexity should not decrease drastically if a few bits are changed, since knowledge of the first few terms can allow the efficient generation of a sequence which closely approximates the original sequence. This observation motivates the definition of the k-error linear complexity of sequences [2], [5]. The k-error linear complexity of a periodic sequence S, denoted by $LC_k(S)$, is defined to be the minimum linear complexity of S that can be obtained by changing up to k bits in one period and identical changes in all other periods. Cryptographically strong sequences should not only have a large linear complexity, but also have a large k-error linear complexity at least for small k.

For a given periodic binary sequence S of period $N = 2^n$, the linear complexity can be more efficiently computed via the Chan-Games algorithm [6] with $O(N)$ bit operations, while the Berlekamp-Massey algorithm requires $O(N^2)$ bit operations. Stamp and Martin [5] extended the Chan-Games algorithm for computing the k-error linear complexity of S for a fixed k. Generalization of these results to p^n-periodic sequences over the finite field $\mathbb{GF}(p^m)$, were shown in [2], [7], [8]. For binary sequences of period 2^n, Rueppel [1] presented the counting function for the number of sequences with fixed linear complexity. In [9], [10], the counting function for the number of sequences with fixed 1-error linear complexity are presented. The counting functions on k-error linear complexity in the case $k = 2$ and $k = 3$ was treated in [11] and [12], respectively. For p-ary sequences of period p^n, the counting function for the number of sequences with fixed linear complexity and fixed 1-error linear complexity, were shown in [13], [14], respectively.

The rest of this paper is arranged as follows. Section 2 introduces some basic definitions and previously related results. Section 3 presents the counting function for the number of sequences with given p-error linear complexity. The expected value of p-error linear complexity of sequences with linear complexity $p^n - p + 1$ is also calculated in Sect. 3.

2. The p-Ary Sequences of Period p^n

Let $S = s_1, s_2, \ldots$ be a p-ary sequences of period p^n, where p is a prime. The linear complexity of S is defined to be the least nonnegative integer t for which there exist coefficients $d_1, d_2, \ldots, d_t \in F_p$ such that

$$s_{i+t} + d_1 s_{i+t-1} + \cdots + d_t s_i = 0, \text{ for all integers } i \geq 1.$$

In addition, the linear complexity of the zero sequence $\mathbf{0}$ is defined to be 0. For periodic sequences, knowing one period means we know the whole sequence. Hence, we denote the linear complexity of S by $LC(S)$ or $LC(s^{(n)})$, where $s^{(n)} = (s_1, s_2, \ldots, s_{p^n})$ is one period of S. Let the vector $e^{(n)}$ has the same length with $s^{(n)}$ over F_p. The k-error linear complexity of S can be denoted by $LC_k(S)$ or $LC_k(s^{(n)})$,

$$LC_k(S) = \min\{LC(s^{(n)} + e^{(n)}) : w(e^{(n)}) \leq k\},$$

where the Hamming weight $w(e^{(n)})$ denotes the number of nonzero terms of $e^{(n)}$.

For a given p-ary sequence of period p^n, Kurosawa et

Manuscript received May 9, 2019.
Manuscript revised July 27, 2019.
Manuscript publicized September 2, 2019.

[†]The author is with the Department of Applied Mathematics, Anhui Agricultural University, Anhui 230036,China.
[††]The author is with the School of Mathematics and Physics, Anhui Jianzhu University, Anhui 230601, China.
[†††]The author is with the School of Mathematical Sciences, Anhui University, Anhui 230601,China.
[††††]The author is with the Ministry of General Education, Anhui Xinhua University, Anhui 230088,China.
a) E-mail: wjxahjzdx@163.com

DOI: 10.1587/transinf.2019EDL8093

al. [15] showed that the minimal value k_{min} for which the k-error linear complexity $LC_k(S)$ of S is strictly less than its linear complexity $LC(S)$ is exactly determined by

$$k_{min} = Prod(p^n - LC(S)),$$

where $Prod(c) = \prod_{j=0}^{n-1}(i_j + 1)$ if the integer $c = \sum_{j=0}^{n-1}(i_j p^j)$. Evidently, $k_{min} = p$ for any p-ary sequences of period p^n with linear complexity $p^n - p + 1$.

For p-ary sequences of period p^n, Meidl and Niederreiter [13] showed that the number $N(L)$ of sequences with linear complexity L, is determined by

$$N(L) = \begin{cases} 1, & L = 0, \\ (p-1)p^{L-1}, & 1 \le L \le p^n. \end{cases} \tag{1}$$

For a given p-ary sequence of period p^n with linear complexity p^n, Meidl and Venkateswarlu [14] presented that the 1-error linear complexity of S is 0 or of the form

$$p^n - p^{r+1} + c, \quad 0 \le r \le n-1,\ 1 \le c \le p^{r+1} - p^r - 1.$$

In [14], it also has been showed that the number $N_1(L)$ of sequences with linear complexity p^n and 1-error linear complexity L is given by

$$N_1(L) = \begin{cases} (p-1)p^n, & L = 0, \\ (p-1)^2 p^{L+r}, & L \ne 0. \end{cases} \tag{2}$$

Given a p-ary sequence S of period p^n, its linear complexity can efficiently be computed by the generalized Chan-Games algorithm [2]. Since we will use some aspects of the generalized Chan-Games algorithm in the following, we present a short description. Let $\varphi_u^{(n)}$, $u = 0, 1, \ldots, p-1$, be the mappings from $F_p^{p^n}$ to $F_p^{p^{n-1}}$, $n > 1$, by

$$\varphi_u^{(n)}(s^{(n)})_i = \sum_{j=0}^{p-u-1} \binom{p-j-1}{u} s_{j\cdot p^{n-1}+i}, \quad i = 1, 2, \ldots, p^{n-1}.$$

Suppose that u, $u = 0, 1, \ldots, p-1$, is the least number such that $\varphi_u^{(n)}(s^{(n)}) \ne \mathbf{0}$. Then the linear complexity of S is given by

$$LC(s^{(n)}) = (p - u - 1)p^{n-1} + LC(s^{(n-1)}),$$

where $s^{(n-1)} = \varphi_u^{(n)}(s^{(n)})$. The generalized Chan-Games algorithm is obtained by applying this result recursively until $n = 0$. In the final step we will have a sequence with period $s^{(0)}$. The linear complexity $LC(s^{(0)}) = 1$ if $s^{(0)} \ne 0$ and $LC(s^{(0)}) = 0$ if $s^{(0)} = 0$. It obviously that $s^{(0)} = 0$ if and only if S is the zero sequence $\mathbf{0}$.

Let S be a p-ary sequence of period p^n. We collect some obvious properties of the linear complexity $LC(S)$ and the mappings $\varphi_u^{(n)}$, $u = 0, 1, \ldots, p-1$, $n > 1$.
P1: $w(\varphi_u^{(n)}(s^{(n)})) \le w(s^{(n)})$, $u = 0, 1, \ldots, p-1$.
P2: $LC(S) < p^n$ if and only if $s^{(n)}$ has the zero sum property, that is, $\sum_{j=1}^{p^n} s_j = 0$.
P3: $LC(S) = 0$ if and only if $s^{(n)} = \mathbf{0}$.
P4: $LC(S) = p^n - p + 1$ if and only if $s^{(1)} = (\varphi_0^{(2)}\varphi_0^{(3)} \cdots \varphi_0^{(n)}(s^{(n)}))$ and $s^{(1)} = (a, a, \ldots, a)$, $a \ne 0 \in F_p$. Then the Hamming weight $w(s^{(r)}) \ge p$ for all $1 \le r \le n$, where $s^{(r)} = \varphi_0^{(r+1)}\varphi_0^{(r+2)} \cdots \varphi_0^{(n)}(s^{(n)})$).
P5: For any $b \in F_p$ and vector $(s_1, s_2, \ldots, s_p)$ with $\varphi_0(s_1, s_2, \ldots, s_p) \ne 0$, it suffices to alter exactly one bit in $\{s_1, s_2, \ldots, s_p\}$ to obtain $\varphi_0(s_1, s_2, \ldots, s_p) = 0$ and $\varphi_1(s_1, s_2, \ldots, s_p) = b$. Moreover, the way of the bit changes is unique.
P6: The set $(\varphi_0^{(n+1)})^{-1}(s^{(n)}) = \{v \in F_p^{p^{n+1}} | \varphi_0^{(n+1)}(v) = s^{(n)}\}$ of preimages of $s^{(n)}$ has cardinality $p^{(p-1)p^n}$.

3. Results and Proofs

In this section, we concentrate on the p-ary sequence of period p^n with linear complexity $p^n - p + 1$, $n \ge 1$.

Lemma 1. *Let S be a p-ary sequence of period p^n with linear complexity $p^n - p + 1$, $n \ge 1$. Then $w(s^{(n)}) = p$ if and only if the nonzero elements of $s^{(n)}$ are $s_{i_1p+1}, s_{i_2p+2}, \ldots, s_{i_pp+p}$ for some $i_j \in \{0, 1, 2, \ldots, p^{n-1} - 1\}$, $j = 1, 2, \ldots, p$, and $s_{i_1p+1} = s_{i_2p+2} = \ldots = s_{i_pp+p}$.*

Proof According to P4, we have $s^{(1)} = \varphi_0^{(2)}\varphi_0^{(3)} \cdots \varphi_0^{(n)}(s^{(n)})$) and $s^{(1)} = (a, a, \ldots, a)$, $a \ne 0 \in F_p$. Note that $s_j^{(1)} = \sum_{i_j=0}^{p^{n-1}-1} s_{i_jp+j}$, $j = 1, 2, \ldots, p$. Then there is exactly one nonzero element in $\{s_j, s_{p+j}, \ldots, s_{p^n-p+j}\}$ for every $j = 1, 2, \ldots, p$. Moreover, the nonzero element $s_{i_jp+j} = s_j^{(1)} = a$. □

Lemma 2. *Let S be a p-ary sequence of period p^n with linear complexity $p^n - p + 1$ and $w(s^{(n)}) = p$, $n \ge 1$. Let $\underline{S} = (s^{(n+1)})^\infty$ be a p-ary sequence of period p^{n+1} with $w(s^{(n+1)}) > p$ and $\varphi_0^{(n+1)}(s^{(n+1)}) = s^{(n)}$.*
(1) Then the p-error linear complexity of $\underline{S}$ satisfies $1 \le LC_p(\underline{S}) \le p^{n+1} - p^n - p$.
(2) For all the vectors $t^{(n+1)}$ such that $t^{(n+1)}$ is differs from $s^{(r+1)}$ at most p terms, only one $t^{(n+1)}$ satisfies $LC(t^{(n+1)}) = LC_p(s^{(n+1)})$, else, the linear complexity of $t^{(n+1)}$ is more than $p^{n+1} - p^n - p$.

Proof Suppose that $s_{i_jp+j}^{(n)}$ is the nonzero element of $s^{(n)}$ for every $j = 1, 2, \ldots, p$. Obviously, it suffices to alter appropriate p bits in $s^{(n+1)}$ to obtain $\varphi_0^{(n+1)}(s^{(n+1)}) = \mathbf{0}$. It can be obtained by exactly one element change in $\{s_{i_jp+j}^{(n+1)}, s_{p^n+i_jp+j}^{(n+1)}, \ldots, s_{(p-1)p^n+i_jp+j}^{(n+1)}\}$ for every $j = 1, 2, \ldots, p$. Let $t^{(n+1)}$ be a vector such that $LC(t^{(n+1)}) = LC_p(s^{(n+1)})$. Then the p-error linear complexity of $\underline{S}$ is

$$LC_p(s^{(n+1)}) = (p - u - 1)p^n + LC(t^{(n)}),$$

where $t^{(n)} = \varphi_u^{(n+1)}(s^{(n+1)})$ and u is the least number such that $\varphi_u^{(n+1)}(s^{(n+1)}) \ne \mathbf{0}$, $u = 1, 2, \ldots, p-1$.

In the case that $2 \le u \le p-1$, the linear complexity $LC(t^{(n)})$ could be equal to any integer between 1 and p^n. Then we have $1 \le LC_p(s^{(n+1)}) \le p^{n+1} - 2p^n$. We now show the case that $u = 1$. According to P5, it suffices to alter exactly one bit in $\{s_{i_jp+j}^{(n+1)}, s_{p^n+i_jp+j}^{(n+1)}, \ldots, s_{(p-1)p^n+i_jp+j}^{(n+1)}\}$ to obtain

$$\varphi_0(s_{i_jp+j}^{(n+1)}, s_{p^n+i_jp+j}^{(n+1)}, \ldots, s_{(p-1)p^n+i_jp+j}^{(n+1)}) = 0$$

and

$$\varphi_1(s^{(n+1)}_{i_jp+j}, s^{(n+1)}_{p^n+i_jp+j}, \ldots, s^{(n+1)}_{(p-1)p^n+i_jp+j}) = b$$

for any $b \in F_p$, $j = 1, 2, \ldots, p$. Then $t^{(n)}_{i_1p+1}, t^{(n)}_{i_2p+2}, \ldots, t^{(n)}_{i_pp+p} \in F_p$ could be arbitrary value by altered appropriate p bits in $s^{(n+1)}$. For $t^{(1)} = (\varphi_0^{(2)}\varphi_0^{(3)} \cdots \varphi_0^{(n)}(t^{(n)}))$, it suffices to select appropriate $t^{(n)}_{i_1p+1}, t^{(n)}_{i_2p+2}, \ldots, t^{(n)}_{i_pp+p} \in F_p$ to obtain $t^{(1)} = \mathbf{0}$, then we get $1 \le LC(t^{(n)}) \le p^n - p$ and $p^{n+1} - 2p^n + 1 \le LC_p(s^{(n+1)}) \le p^{n+1} - p^n - p$. This proves that the p-error linear complexity of $\underline{S}$ can be the arbitrary integer lies in $[1, p^{n+1} - p^n - p]$. Note that the way of the bit changes is unique. Then there is only one vector $t^{(n+1)}$ satisfies $LC(t^{(n+1)}) = LC_p(s^{(n+1)}) \in [1, p^{n+1} - p^n - p]$. Else, we have that $t^{(n)} = \varphi_1^{(n)}(t^{(n+1)}) \neq \mathbf{0}$. Since we can not select appropriate $t^{(n)}_{i_1p+1}, t^{(n)}_{i_2p+2}, \ldots, t^{(n)}_{i_pp+p} \in F_p$ to obtain $t^{(1)} = \varphi_0^{(2)}\varphi_0^{(3)} \cdots \varphi_0^{(n)}(t^{(n)})) = \mathbf{0}$, then we get $LC(t^{(n+1)}) > p^{n+1} - p^n - p$. □

The following theorem presents all possible values of the p-error linear complexity of p-ary sequences of period p^n with linear complexity $p^n - p + 1$, $n \ge 1$.

Theorem 1. *For any p-ary sequence S of period p^n with linear complexity $p^n - p + 1$, the p-error linear complexity of S is either zero or of the form*

$$p^n - p^{r+1} + c,$$

where $1 \le r \le n-1$ and $1 \le c \le p^{r+1} - p^r - p$.

Proof According to P4, we have $w(s^{(n)}) \ge p$. Obviously, the p-error linear complexity of S is 0 in the case that $w(s^{(n)}) = p$. We now show the case $w(s^{(n)}) > p$. Suppose that r, $1 \le r \le n-1$, is the largest integer such that $w(s^{(r)}) = p$. Then the p-error linear complexity of S is

$$LC_p(s^{(n)}) = p^n - p^{r+1} + LC_p(s^{(r+1)}).$$

Note that the p^r-periodic sequence with period $s^{(r)} = \varphi_0^{(r+1)}(s^{(r+1)})$ satisfies $LC(s^{(r)}) = p^r - p + 1$ and $w(s^{(r)}) = p$. According to Lemma 2, we have $1 \le LC_p(s^{(r+1)}) \le p^{r+1} - p^r - p$. Then the p-error linear complexity of S is of the form

$$p^n - p^{r+1} + c,$$

where $1 \le r \le n-1$ and $1 \le c \le p^{r+1} - p^r - p$. □

The following theorem presents the exact formulas to count the number of p-ary sequences of period p^n with linear complexity $p^n - p + 1$ and fixed p-error linear complexity.

Theorem 2. *The number of p-ary sequences of period p^n with linear complexity $p^n - p + 1$ and p-error linear complexity L is*

$$N_p(L) = \begin{cases} (p-1)p^{pn-p}, & if\ L = 0, \\ (p-1)^2 p^{L+pr-1}, & if\ L = p^n - p^{r+1} + c, \\ 0, & otherwise, \end{cases}$$

where $1 \le r \le n-1$ and $1 \le c \le p^{r+1} - p^r - p$.

Proof For p-ary sequences of period p^n with linear complexity $p^n - p + 1$, the sequences S with p-error linear complexity 0 are exactly the sequences with $w(s^{(n)}) = p$. According to Lemma 1, we have

$$N_p(0) = (p-1)p^{n-1}p^{n-1} \cdots p^{n-1} = (p-1)p^{pn-p}.$$

For the sequences S with p-error linear complexity $p^n - p^{r+1} + c$, $1 \le r \le n-1$, $1 \le c \le p^{r+1} - p^r - p$, the p-error linear complexity of S is

$$LC_p(s^{(n)}) = p^n - p^{r+1} + LC_p(s^{(r+1)}).$$

Let $t^{(r+1)}$ be the vector such that $LC(t^{(r+1)}) = LC_p(s^{(r+1)})$. For every integer c, $1 \le c \le p^{r+1} - p^r - p$, there are $(p-1)p^{c-1}$ choices for $t^{(r+1)}$ such that $LC(t^{(r+1)}) = c$ by (1). Note that $s^{(r+1)}$ differs from $t^{(r+1)}$ at exactly $s^{(n+1)}_{i_1p+1}, s^{(n+1)}_{i_2p+2}, \ldots, s^{(n+1)}_{i_pp+p}$ for some $i_j \in \{0, 1, 2, \ldots, p^r - 1\}$, $j = 1, 2, \ldots, p$. Then there are $(p-1)p^{c-1}(p-1)p^r p^r \cdots p^r = (p-1)^2 p^{c+pr-1}$ choices for $s^{(r+1)}$ by Lemma 2. Using P6 recursively we obtain that

$$(p-1)^2 p^{c+pr-1} p^{(p-1)p^{r+1}} \cdots p^{(p-1)p^{n-1}} = (p-1)^2 p^{p^n - p^{r+1} + c + pr - 1}$$

is the number of p-ary sequences of period p^n with linear complexity $p^n - p + 1$ and p-error linear complexity $p^n - p^{r+1} + c$. □

Theorem 2 permits the calculation of the exact formula for the expected value of the p-error linear complexity of a random p-ary sequences of period p^n with linear complexity $p^n - p + 1$, $n \ge 1$.

Theorem 3. *The expected value E_p of the p-error linear complexity of p-ary sequences of period p^n with linear complexity $p^n - p + 1$ is*

$$E_p = p^n - p - \frac{1 - p^{-p^n + pn}}{p-1} - \sum_{r=1}^{n-1} p^{-p^r + pr + 1}.$$

Proof According to (1), there are $(p-1)p^{p^n - p}$ p-ary sequences of period p^n with linear complexity $p^n - p + 1$. From Theorem 2 we have

$$\begin{aligned}
(p-1)p^{p^n-p}E_p &= \sum_L N_p(L)L \\
&= \sum_{r=1}^{n-1} \sum_{c=1}^{p^{r+1}-p^r-p} (p-1)^2 p^{p^n - p^{r+1} + c + pr - 1}(p^n - p^{r+1} + c) \\
&= (p-1)p^{p^n+n} \sum_{r=1}^{n-1} p^{-p^{r+1}+pr-1} \sum_{c=1}^{p^{r+1}-p^r-p} (p-1)p^c \\
&\quad -(p-1)p^{p^n} \sum_{r=1}^{n-1} p^{-p^{r+1}+pr+r} \sum_{c=1}^{p^{r+1}-p^r-p} (p-1)p^c \\
&\quad +p^{p^n} \sum_{r=1}^{n-1} p^{-p^{r+1}+pr-1} \sum_{c=1}^{p^{r+1}-p^r-p} (p-1)^2 c p^c \\
&= T_1 - T_2 + T_3.
\end{aligned}$$

For the first term T_1 we have

$$T_1 = (p-1)p^{p^n+n} \sum_{r=1}^{n-1} p^{-p^{r+1}+pr-1}(p^{p^{r+1}-p^r-p+1} - p)$$

$$= (p-1)p^{p^n+n}(\sum_{r=1}^{n-1} p^{-p^r+p(r-1)} - \sum_{r=1}^{n-1} p^{-p^{r+1}+pr})$$
$$= (p-1)p^{p^n-p}(p^n - p^{-p^n+pn+n}).$$

For the second term T_2 we get

$$T_2 = (p-1)p^{p^n}\sum_{r=1}^{n-1} p^{-p^{r+1}+pr+r}(p^{p^{r+1}-p^r-p+1} - p)$$
$$= (p-1)p^{p^n}(\sum_{r=1}^{n-1} p^{-p^r+p(r-1)+r+1} - \sum_{r=2}^{n} p^{-p^r+p(r-1)+r})$$
$$= (p-1)p^{p^n-p}(p^2 - p^{-p^n+pn+n} + (p-1)\sum_{r=2}^{n-1} p^{-p^r+pr+r}).$$

For the third term T_3, using the identity

$$(p-1)^2\sum_{j=1}^{m} jp^j = (p-1)mp^{m+1} - p^{m+1} + p$$

we get

$$T_3 = p^{p^n}\sum_{r=1}^{n-1} p^{-p^{r+1}+pr-1}(p-1)(p^{r+1}-p^r-p)p^{p^{r+1}-p^r-p+1}$$
$$- p^{p^n}\sum_{r=1}^{n-1} p^{-p^{r+1}+pr-1}(p^{p^{r+1}-p^r-p+1} - p)$$
$$= T_4 - T_5,$$

where

$$T_4 = (p-1)p^{p^n}\sum_{r=1}^{n-1} p^{-p^r+p(r-1)}(p^{r+1}-p^r-p)$$
$$= (p-1)p^{p^n-p}((p-1)\sum_{r=1}^{n-1} p^{-p^r+pr+r} - \sum_{r=1}^{n-1} p^{-p^r+pr+1})$$

and

$$T_5 = p^{p^n}\sum_{r=1}^{n-1} p^{-p^{r+1}+pr-1}(p^{p^{r+1}-p^r-p+1} - p)$$
$$= p^{p^n}(\sum_{r=1}^{n-1} p^{-p^r+p(r-1)} - \sum_{r=2}^{n} p^{-p^r+p(r-1)})$$
$$= p^{p^n}(p^{-p} - p^{-p^n+p(n-1)})$$
$$= (p-1)p^{p^n-p}\frac{1-p^{-p^n+pn}}{p-1}.$$

By combinbining the formulas for T_1, T_2, T_4 and T_5 we get

$$E_p = p^n - p - \frac{1-p^{-p^n+pn}}{p-1} - \sum_{r=1}^{n-1} p^{-p^r+pr+1}$$

4. Concluding Remarks

In this paper, we obtain exact results for the counting function and the expected value for the p-error linear complexity of p-ary sequences of period p^n with linear complexity $p^n - p + 1$, $n \geq 1$. Note that the value $\frac{p^{-p^n+pn}}{p-1}$ and the sum $\sum_{r=2}^{n-1} p^{-p^r+pr+1}$ in the formula for E_p is small. Hence the value of E_p is approximately equals to $p^n - 2p - \frac{1}{p-1}$. From the above discussion, we know that there are many sequences with large p-error linear complexity among all p-ary sequences of period p^n with linear complexity $p^n - p + 1$.

Acknowledgments

We would like to thank the reviewers for their helpful comments. This work was supported by the Key Projects of the Natural Science Fund of Anhui Colleges and Universities (KJ2017A136, KJ2019JD17, KJ2017A623) and the Key Projects of Support Program for Excellent Young Talents in Anhui Colleges and Universities (gxyqZD2016032).

References

[1] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.
[2] C. Ding, G. Xiao, and W. Shan, "The Stability Theory of Stream Ciphers," Lecture Notes in Computer Science, Springer-Verlag, 1991.
[3] S.W. Golomb and G. Gong, "Signal Design for Good Correlation," For Wireless Communication, Croptography and Radar, Cambridge University Press, 2005.
[4] J. Massey, "Shift-register synthesis and BCH decoding," IEEE Trans. Inf. Theory, vol.15, no.1, pp.122–127, 1969.
[5] M. Stamp and C.F. Martin, "An algorithm for the k-error linear complexity of binary sequences of period 2^n," IEEE Trans. Inf. Theory, vol.39, no.4, pp.1398–1401, 1993.
[6] R. Games and A. Chan, "A fast algorithm for determining the linear complexity of a binary sequence with period 2^n," IEEE Trans. Inf. Theory, vol.29, no.1, pp.144–146, 1983.
[7] T. Kaida, S. Uehara, and K. Imamura, "An algorithm for the k-error linear complexity of sequences over $GF(p^m)$ with period p^n, p a prime," Inform. Comput., vol.151, no.1-2, pp.134–147, 1999.
[8] T. Kaida, "On the generalized Lauder-Paterson algorithm and profiles of the k-error linear complexity for exponent periodic sequences," Sequences and Their Applications 2004, Springer, pp.166–178, 2005.
[9] W. Meidl, "On the stability of 2^n-periodic binary sequences," IEEE Trans. Inf. Theory, vol.51, pp.1151–1155, 2005.
[10] F.-W. Fu, H. Niederreiter, and M. Su, "The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity," Sequences and Their Applications 2006, Springer, pp.88–103, 2006.
[11] R. Kavulurn, "Characterization of 2^n-periodic binary sequences with fixed 2-error or 3-error linear complexity," Des. Codes Cryptogr., vol.53, no.2, pp.75–97, 2009.
[12] J. Zhou and W. Liu, "The k-error linear complexity distribution for 2^n-periodic binary sequences," Des. Codes Cryptogr., vol.73, no.1, pp.55–75, 2014.
[13] W. Meidl and H. Niederreiter, "On the expected value of the linear complexity and k-error linear complexity of periodic sequences," IEEE Trans. Inf. Theory, vol.48, no.11, pp.2817–2825, 2002.
[14] W. Meidl and A. Venkateswarlu, "Remarks on the k-error linear complexity of p^n-periodic sequences," Des. Codes Cryptogr., vol.42, no.2, pp.181–193, 2007.
[15] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k-error linear complexity," IEEE Trans. Inf. Theory, vol.46, no.2, pp.694–698, 2000.