On k-error linear complexity over $\mathbb{F}_N$ of interleaved binary sequences derived from four N-periodic ones

V Edemskiy[1], X Du[2] and Z Chen[3]

[1] Yaroslav-the-Wise Novgorod State University, ul. B. St. Petersburgskaya, 41 173003 Veliky Novgorod, Russia
[2]College of Mathematics and Statistics, Northwest Normal University, Lanzhou, Gansu 730070, P.R. China
[3]School of Mathematics, Putian University, Putian, Fujian 351100, P.R. China

E-mail: Vladimir.Edemsky@novsu.ru

Abstract. We estimate the k-error linear complexity of some interleaved sequences with period $4N$ over the finite field of order N (N an odd prime). Furthermore, we obtain the exact value of the k-error linear complexity for small value of k of the interleaved sequences obtained from the cyclotomic sequences. In particular, we study the interleaved sequences obtained from Legendre sequences and Hall's sextic residue sequences, respectively. Our results show that these sequences are quite stable.

1. Introduction

1.1. Motivications and Objects

Let M and N be positive integers. An NM-periodic sequence $\underline{u}$, written as $\underline{u} = (u_0, \dots, u_{NM-1})$, can be read row by row from the following $N \times M$ matrix

$$\begin{bmatrix} u_0 & u_1 & \cdots & u_{M-1} \\ u_M & u_{M+1} & \cdots & u_{2M-1} \\ \vdots & \vdots & \vdots & \vdots \\ u_{(N-1)M} & u_{(N-1)M+1} & \cdots & u_{NM-1} \end{bmatrix}.$$

Sometimes $\underline{u}$ is also called an *interleaved sequence* [1]. If we write the i-th column of the matrix above as $\underline{a}^{(i)} = (u_i, u_{i+M}, \dots, u_{i+(N-1)M})$ for $0 \le i < M$, which forms an N-periodic sequence, then the following notation is used to denote $\underline{u}$: $\underline{u} = \mathcal{I}(\underline{a}^{(0)}, \underline{a}^{(1)}, \dots, \underline{a}^{(M-1)})$, where $\mathcal{I}$ is called the *interleaved operator*.

In particular in the past several years, for an odd prime N and an N-periodic binary sequence $\underline{v} = (v_0, v_1, \dots, v_{N-1})$ over the finite field $\mathbb{F}_2 = \{0,1\}$, a special family of interleaved binary sequences of the form

$$\underline{u} = \mathcal{I}(\underline{v}, L^m(\underline{v}), L^{(N+1)/2}(\underline{v}), L^{m+(N+1)/2}(\underline{v}) \oplus \underline{1}), 0 \le m < N, \quad (1)$$

was investigated in the literature, see [2-4] for details, where $\oplus$ is the addition in $\mathbb{F}_2$ and L denotes the left cyclic shift operator of a sequence, i.e., $L^m(\underline{a}) = (a_m, a_{m+1}, \dots, a_{m-1})$ for $\underline{a} = (a_0, a_1, \dots, a_{N-1})$.

In [2], Tang and Gong proved that the sequence of form $\underline{u}$ has optimal autocorrelation value $\{0, -4\}$ if v is a sequence of period $N \equiv 3 \pmod 4$ with optimal autocorrelation value $\{N, -1\}$. It is well known

that binary Legendre sequences and Hall's sextic residue sequences have optimal autocorrelation value. The linear complexity over $\mathbb{F}_2$ of $\underline{u}$ has been investigated in [5,6]. In this work, we turn to consider the k-error linear complexity of $\underline{u}$.

We will view the binary $\underline{u}$ as a sequence over $\mathbb{F}_N$ and consider its k-error linear complexity over $\mathbb{F}_N$. In Section 2 we prove some general results. In Section 3, we give some results when $\underline{v}$ is a cyclotomic sequence, in particular if $\underline{v}$ is Legendre sequence or Hall sequence.

1.2. Notion of k-error linear complexity

We conclude this section by introducing the notions of the linear complexity and the k-error linear complexity of periodic sequences.

Let $\mathbb{F}$ be a field. For a T-periodic sequence $\underline{s} = (s_0, s_1, \dots, s_{T-1})$ over $\mathbb{F}$, we recall that the *linear complexity* over $\mathbb{F}$, denoted by $LC^{\mathbb{F}}(\underline{s})$, is the least order $\mathcal{L}$ of a linear recurrence relation over $\mathbb{F}$

$$s_{u+\mathcal{L}} = c_{\mathcal{L}-1}s_{u+\mathcal{L}-1} + \cdots + c_1 s_{u+1} + c_0 s_u \quad \text{for} \quad u \geq 0,$$

which is satisfied by $\underline{s}$ and where $c_0 \neq 0, c_1, \dots, c_{\mathcal{L}-1} \in \mathbb{F}$. Let $G_{\underline{s}}(X) = s_0 + s_1 X + s_2 X^2 + \cdots + s_{T-1}X^{T-1} \in \mathbb{F}[X]$, which is called the *generating polynomial* of $\underline{s}$. Then the linear complexity over $\mathbb{F}$ of $\underline{s}$ is computed by

$$LC^{\mathbb{F}}(\underline{s}) = T - \deg\big(\gcd(X^T - 1, G_{\underline{s}}(X))\big), \tag{2}$$

see, e.g. [7] for details. For integers $k \geq 0$, the *k-error linear complexity* over $\mathbb{F}$ of $\underline{s}$, denoted by $LC_k^{\mathbb{F}}(\underline{s})$, is the smallest linear complexity (over $\mathbb{F}$) that can be obtained by changing at most k terms of the sequence per period, see [8-10], and see [11] for the related even earlier defined sphere complexity. Clearly $LC_0^{\mathbb{F}}(\underline{s}) = LC^{\mathbb{F}}(\underline{s})$ and

$$T \geq LC_0^{\mathbb{F}}(\underline{s}) \geq LC_1^{\mathbb{F}}(\underline{s}) \geq \cdots \geq LC_n^{\mathbb{F}}(\underline{s}) = 0$$

when n equals the number of nonzero terms of $\underline{s}$ per period, i.e., the Hamming weight of $\underline{s}$ denoted by $wt(\underline{s})$. Define the Hamming weight of polynomial $G_{\underline{s}}(X)$, denoted by $wt(G_{\underline{s}}(X))$, as the number of its nonzero coefficients. It can be easily seen that $wt(G_{\underline{s}}(X)) = wt(\underline{s})$.

Linear complexity and k-error linear complexity are important cryptographic characteristics of sequences and provide information on the predictability and thus unsuitability for cryptography. For a sequence to be cryptographically strong, its linear complexity should be large, but not significantly reduced by changing a few terms. And according to the Berlekamp-Massey algorithm [12, 13], the linear complexity should be at least a half of the period.

2. Bounds on error linear complexity

We always suppose that $\underline{v}$ is a binary sequence of least period N, i.e., $\underline{v}$ is not $(0,0,\dots,0)$ or $(1,1,\dots,1)$. Our main results are the lower and upper bounds for $LC_k^{\mathbb{F}_N}(\underline{u})$ presented in the following two theorems.

Theorem 1. Let $N > 3$ be an odd prime and $\underline{v}$ an N-periodic binary sequence. Let $\underline{u}$ be the interleaved binary sequence defined in (1). If we view $\underline{u}$ as a sequence over $\mathbb{F}_N$, we have for any integer $k \geq 0$

$$LC_k^{\mathbb{F}_N}(\underline{u}) \geq 4LC_k^{\mathbb{F}_N}(\underline{v}).$$

In particular, $LC^{\mathbb{F}_N}(\underline{u}) = LC_0^{\mathbb{F}_N}(\underline{u}) = 4N$.

Theorem 2. Let $N > 3$ be an odd prime and $\underline{v}$ an N-periodic binary sequence. Let $\underline{u}$ be the interleaved binary sequence defined in (1). If we view $\underline{u}$ as a sequence over $\mathbb{F}_N$, we have for any integer $k \geq 0$

$$LC_k^{\mathbb{F}_N}(\underline{u}) \leq \min_{2k_1+2k_2 \leq k} 2\Big(\max(LC_{k_1}^{\mathbb{F}_N}(\underline{v}),1) + \max(LC_{k_2}^{\mathbb{F}_N}(\underline{v}),1)\Big).$$

We divide the proofs of Theorems 1 and 2 into following several lemmas.

Lemma 3. Let $\underline{a}$ be an N-periodic sequence over $\mathbb{F}_N$ and $G_{\underline{a}}(X) \in \mathbb{F}_N[X]$ be the generating polynomial of $\underline{a}$. Then the generating polynomial of $\underline{b} = L^m(\underline{a})$ is

$$G_{\underline{b}}(X) = X^{N-m}G_{\underline{a}}(X) (\text{mod } X^N - 1).$$

Proof. It comes from [14].

Lemma 4. Let $\underline{a}$ be an N-periodic binary sequence over $\mathbb{F}_2$. Write $\underline{b} = \underline{a} \oplus \underline{1}$, i.e., $\underline{b}$ is the complement sequence of $\underline{a}$ over $\mathbb{F}_2$. If we view $\underline{a}$ and $\underline{b}$ as sequences over $\mathbb{F}_N$, then the generating polynomial (over $\mathbb{F}_N$) of $\underline{b}$ is

$$G_{\underline{b}}(X) = (X-1)^{N-1} - G_{\underline{a}}(X) \in \mathbb{F}_N[X] (\mathrm{mod}\, X^N - 1),$$

where $G_{\underline{a}}(X) \in \mathbb{F}_N[X]$ is the generating polynomial of $\underline{a}$ over $\mathbb{F}_N$.

Proof. Indeed, the generating polynomial of $\underline{b}$ (as a sequence over $\mathbb{F}_N$) is

$$G_{\underline{b}}(X) = \frac{X^N - 1}{X - 1} - G_{\underline{a}}(X) \in \mathbb{F}_N[X] (\mathrm{mod}\, X^N - 1).$$

Then the fact that $X^N - 1 = (X-1)^N$ over $\mathbb{F}_N$ helps us to reduce the fraction above.

Lemma 5. Let $\underline{a}$ be an N-periodic sequence over $\mathbb{F}_N$ with the k-error linear complexity $LC_k^{\mathbb{F}_N}(\underline{a})$ for $k \geq 0$. Then there always exists an N-periodic sequence $\underline{e}$ over $\mathbb{F}_N$ with $wt(\underline{e}) \leq k$ such that

$$(X-1)^{N - LC_k^{\mathbb{F}_N}(\underline{a})} | (G_{\underline{a}}(X) - G_{\underline{e}}(X)).$$

Proof. By (2) we can get the desired result.

In fact, $(X-1)^{N - LC_k^{\mathbb{F}_N}(\underline{a})+1} \nmid (G_{\underline{a}}(X) - G_{\underline{e}}(X))$. So we refer such $\underline{e}$ as to a reference error-sequence with respect to the value $LC_k^{\mathbb{F}_N}(\underline{a})$.

Let β be a primitive 4-th root of unity in $\overline{\mathbb{F}}_N$, which is the spilt field of $\mathbb{F}_N$. We have

$$X^4 - 1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X-\beta)(X-\beta^3) \in \overline{\mathbb{F}}_N[X].$$

We remark that $\beta \in \mathbb{F}_N$ if $N \equiv 1 (\mathrm{mod}\, 4)$, and $\beta \in \overline{\mathbb{F}}_N \backslash \mathbb{F}_N$ if $N \equiv 3 (\mathrm{mod}\, 4)$.

Let $\underline{e}$ be an error-sequences with respect to the value $LC_k^{\mathbb{F}_N}(\underline{u})$. For $G_{\underline{u}}(X)$ and $G_{\underline{e}}(X)$ over $\mathbb{F}_N$, the generating polynomials of $\underline{u}$ and $\underline{e}$, respectively, then there must exist $n_i \in \mathbb{N}, i = 0,1,2,3$ such that

$$G_{\underline{u}}(X) - G_{\underline{e}}(X) \equiv 0 (\mathrm{mod}\, (X-1)^{n_0}(X-\beta)^{n_1}(X+1)^{n_2}(X-\beta^3)^{n_3}) \quad (3)$$

and

$$n_0 + n_1 + n_2 + n_3 = 4N - LC_k^{\mathbb{F}_N}(\underline{u}). \quad (4)$$

Lemma 6. Let $N > 3$ be an odd prime and $\underline{v}$ an N-periodic binary sequence. Let $\underline{u}$ be the interleaved binary sequence defined in (1). Let $\underline{e}$ be an error-sequences with respect to the value $LC_k^{\mathbb{F}_N}(\underline{u})$ over $\mathbb{F}_N$ of period $4N$. Then we have

$$\max\{n_0, n_1, n_2, n_3\} \leq N - LC_k^{\mathbb{F}_N}(\underline{v})$$

when $\underline{e}$ takes over all possible sequences with at most $k \geq 0$ many non-zero entries in one period and $LC_k^{\mathbb{F}_N}(\underline{v}) > 1$.

Proof. Write $\underline{b} = L^m(\underline{v})$, $\underline{c} = L^{(N+1)/2}(\underline{v})$ and $\underline{d} = L^{m+(N+1)/2}(\underline{v}) \oplus \underline{1}$. From the structure of $\underline{u}$ (over $\mathbb{F}_N$), we have $G_{\underline{u}}(X) = G_{\underline{v}}(X^4) + XG_{\underline{b}}(X^4) + X^2 G_{\underline{c}}(X^4) + X^3 G_{\underline{d}}(X^4)$.

Let $K = 4N - 4m + 1$. Then after simple calculations we get

$$G_{\underline{u}}(X) \equiv ((X^2+1)^N - X^K(X^2-1)^N) G_{\underline{v}}(X^4) + X^3(X^4-1)^{N-1} (\mathrm{mod}\, X^{4N} - 1) \quad (5)$$

by Lemmas 3 and 4. From above we see that

$$G_{\underline{u}}(X) \equiv 2G_{\underline{v}}(X^4) (\mathrm{mod}\, (X^2-1)^{N-1}) \text{ and } G_{\underline{u}}(X) \equiv 2X^K G_{\underline{v}}(X^4) (\mathrm{mod}\, (X^2+1)^{N-1}).$$

So according to the known conditions, we have

$$0 \equiv G_{\underline{u}}(X) - G_{\underline{e}}(X) \equiv \begin{cases} 2G_{\underline{v}}(X^4) - G_{\underline{e}}(X) (\mathrm{mod}\, (X-1)^{\min\{n_0, N-1\}}), \\ 2G_{\underline{v}}(X^4) - G_{\underline{e}}(X) (\mathrm{mod}\, (X+1)^{\min\{n_2, N-1\}}), \\ 2X^K G_{\underline{v}}(X^4) - G_{\underline{e}}(X) (\mathrm{mod}\, (X-\beta)^{\min\{n_1, N-1\}}), \\ 2X^K G_{\underline{v}}(X^4) - G_{\underline{e}}(X) (\mathrm{mod}\, (X-\beta^3)^{\min\{n_3, N-1\}}). \end{cases}$$

Let $\ell \in \mathbb{N}$ satisfy $2^\ell \equiv 1 (\mathrm{mod}\, N)$. Replacing X by $X^{2^{\ell-2}}$ in the first comparison above, we get

$$2G_{\underline{v}}(X^{2^\ell}) - G_{\underline{e}}(X^{2^{\ell-2}}) \equiv 0 (\mathrm{mod}\, (X^{2^{\ell-2}} - 1)^{\min\{n_0, N-1\}}).$$

Due to the fact $G_{\underline{v}}(X^{2^\ell}) \equiv G_{\underline{v}}(X)(\mathrm{mod}\ X^N - 1)$, we derive

$$G_{\underline{v}}(X) - 2^{-1}G_{\underline{e}}(X^{2^{\ell-2}}) \equiv 0(\mathrm{mod}\ (X-1)^{\min\{n_0, N-1\}}),$$

which means that

$$(X-1)^{\min\{n_0,N-1\}} | \gcd(G_{\underline{v}}(X) - 2^{-1}G_{\underline{e}}(X^{2^{\ell-2}}), (X-1)^N),$$

from which we derive

$$LC_k^{\mathbb{F}_N}(\underline{v}) \le N - \min(n_0, N-1)$$

by (2). Since $LC_k^{\mathbb{F}_N}(\underline{v}) > 1$, we derive $n_0 \le N - LC_k^{\mathbb{F}_N}(\underline{v})$.

Now, replacing X by $-X$ in the second comparison above, we get

$$2G_{\underline{v}}(X^4) - G_{\underline{e}}(-X) \equiv 0(\mathrm{mod}(X-1)^{\min\{n_2,N-1\}}).$$

So, as earlier, we obtain that

$$(X-1)^{\min\{n_2,N-1\}} \mid \gcd(G_{\underline{v}}(X) - 2^{-1}G_{\underline{e}}(-X^{2^{\ell-2}}), (X-1)^N),$$

and

$$LC_k^{\mathbb{F}_N}(\underline{v}) \le N - \min(n_2, N-1)$$

or $n_2 \le N - LC_k^{\mathbb{F}_N}(\underline{v})$.

Now we consider the cases of n_1 and n_3.

(i). Suppose $N \equiv 1(\mathrm{mod}4)$; then $\beta \in \mathbb{F}_N$ and replacing X by βX in the third equation above, we have

$$2\beta X^K G_{\underline{v}}(X^4) - G_{\underline{e}}(\beta X) \equiv 0(\mathrm{mod}\ (\beta X - \beta)^{\min\{n_1,N-1\}})$$

or

$$G_{\underline{v}}(X^4) - (2\beta)^{-1}X^{4m-1}G_{\underline{e}}(\beta X) \equiv 0(\mathrm{mod}\ (X-1)^{\min\{n_1,N-1\}}).$$

It means that

$$(X-1)^{\min\{n_1,N-1\}} | \gcd(G_{\underline{v}}(X) - (2\beta)^{-1}X^{4m-1}G_{\underline{e}}(\beta X^{2^{\ell-2}}), (X-1)^N),$$

and

$$LC_k^{\mathbb{F}_N}(\underline{v}) \le N - \min(n_1, N-1)$$

by (2) or $n_1 \le N - LC_k^{\mathbb{F}_N}(\underline{v})$.

Inequality $n_3 \le N - LC_k^{\mathbb{F}_N}(\underline{v})$ may be proved similarly.

(ii). Suppose $N \equiv 3(\mathrm{mod}4)$; then $\beta \notin \mathbb{F}_N$, $n_1 = n_3$ and

$$2X^K G_{\underline{v}}(X^4) - G_{\underline{e}}(X) = 0(\mathrm{mod}\ (X^2+1)^{\min\{n_1,N-1\}}).$$

Write

$$G_{\underline{e}}(X) = G_{\underline{e,0}}(X^2) + XG_{\underline{e,1}}(X^2). \tag{6}$$

Then we have

$$2X^K G_{\underline{v}}(X^4) - G_{\underline{e,0}}(X^2) - XG_{\underline{e,1}}(X^2) \equiv 0(\mathrm{mod}\ (X^2+1)^{\min\{n_1,N-1\}}).$$

Replacing X by $-X$ in the equation above, we obtain

$$-2X^K G_{\underline{v}}(X^4) - G_{\underline{e,0}}(X^2) + XG_{\underline{e,1}}(X^2) \equiv 0(\mathrm{mod}\ (X^2+1)^{\min\{n_1,N-1\}}).$$

From the last two congruences above, we get

$$2X^{K-1}G_{\underline{v}}(X^4) - G_{\underline{e,1}}(X^2) \equiv 0(\mathrm{mod}\ (X^2+1)^{\min\{n_1,N-1\}})$$

or

$$2X^{K-1}G_{\underline{v}}(X^4) - G_{\underline{e,1}}(-X^2) \equiv 0(\mathrm{mod}\ (X^2-1)^{\min\{n_1,N-1\}})$$

So, as before, we obtain that

$$(X-1)^{\min\{n_1,N-1\}} | \gcd(G_{\underline{v}}(X) - 2^{-1}X^{4m}G_{\underline{e,1}}(-X^{2^{\ell-2}}), (X-1)^N),$$

and

$$LC_k^{\mathbb{F}_N}(\underline{v}) \le N - \min(n_1, N-1) = N - \min(n_3, N-1)$$

by (2) or $n_1 = n_3 \le N - LC_k^{\mathbb{F}_N}(\underline{v})$.

We note that we carry the operations in the field of characteristic N.

Now we turn to prove Theorems 1 and 2.

Proof. (proof of Theorem 1.) For $LC_k^{\mathbb{F}_N}(\underline{v}) = 0$ the statement of this theorem is obvious. Otherwise, we consider two cases.

(i). First, we suppose that $LC_k^{\mathbb{F}_N}(\underline{v}) > 1$. Then by Lemma 6 we obtain

$$n_0 + n_1 + n_2 + n_3 \le 4N - 4LC_k^{\mathbb{F}_N}(\underline{v}).$$

So, by (4) $4N - LC_k^{\mathbb{F}_N}(\underline{u}) \le 4N - 4LC_k^{\mathbb{F}_N}(\underline{v})$ or $LC_k^{\mathbb{F}_N}(\underline{u}) \ge 4LC_k^{\mathbb{F}_N}(\underline{v})$.

(ii). Now, we suppose that $LC_k^{\mathbb{F}_N}(\underline{v}) = 1$, so $k < N$. We prove the case by contradiction. Let $LC_k^{\mathbb{F}_N}(\underline{u}) < 4$. Then by (4) there exist $i: n_i = N, 0 \le i \le 3$.

First, let $n_0 = N$. Then, by (5), we obtain that

$$2G_{\underline{v}}(X^4) - G_{\underline{e}}(X) + X^3(X^4 - 1)^{N-1} \equiv 0 (\mathrm{mod}\ (X-1)^N).$$

Denote by $\overline{G_{\underline{v}}(X^4)}$, $\overline{G_{\underline{e}}(X)}$ the remainders of dividing the polynomials $G_{\underline{v}}(X^4), G_{\underline{e}}(X)$ by $X^N - 1$, respectively. Since $X^3(X^4-1)^{N-1} = X^3 + X^{3+4} + \cdots + X^{3+4(N-1)}$ and $\{(3+4n)(\mathrm{mod} N): n = 0, \dots, N-1\} = \{0,1 \dots, N-1\}$, then we have $\overline{G_{\underline{e}}(X)} = 2\overline{G_{\underline{v}}(X^4)} + X^{N-1} + \cdots + X + 1$.

By condition $\underline{v}$ is the binary sequence with the period N, hence $\overline{G_{\underline{v}}(X^4)} = \sum_{i=0}^{N-1} f_i x^i$ where $f_i \in \{0,1\}$. So, we see that $\overline{G_{\underline{e}}(X)} = \sum_{i=0}^{N-1} (1 + 2f_i)x^i$ and $1 + 2f_i \ne 0$ in $\mathbb{F}_N$ for $N > 3$. Hence, $wt(\overline{G_{\underline{e}}(X)}) = N$ and $wt(\underline{e}) = k \ge N$. We get a contradiction. Cases when $n_i = N, i = 1,2,3$ can be considered similarly.

By Theorem 1, if $\underline{v}$ is a ``good" sequence so is $\underline{u}$. Now we give an upper bound for the k-error linear complexity of $\underline{u}$.

Proof. (proof of Theorem 2) To prove this theorem, we will construct the sequence $\underline{f}$ for $\underline{u}$ in a special way. Let $k_1, k_2: 2k_1 + 2k_2 \le k$. Applying Lemma 5, we get that there must exist reference error-sequences $\underline{e_1}$ and $\underline{e_2}$ such that

$$G_{\underline{v}}(X) - G_{\underline{e_i}}(X) \equiv 0 (\mathrm{mod}\ (X-1)^{N - LC_{k_i}^{\mathbb{F}_N}(\underline{v})}), i = 0,1$$

where $wt(\underline{e_i}) \le k_i$. Hence, there exist polynomials $E_i(X) \in \mathbb{F}_N[X], i = 1,2$ such that

$$G_{\underline{v}}(X^4) - G_{\underline{e_i}}(X^4) = (X^4 - 1)^{N - LC_{k_i}^{\mathbb{F}_N}(\underline{v})} E_i(X^4), i = 0,1.$$

We will take $\underline{f}: G_{\underline{f}}(X) = (X^2+1)^N G_{\underline{e_1}}(X^4) + X^K(1-X^2)^N G_{\underline{e_2}}(X^4)$, where $K = 4N - 4m + 1$. Then $wt\left(\underline{f}\right) \le 2k_1 + 2k_2 \le k$. By (5) we see that $G_{\underline{u}}(X) - G_{\underline{f}}(X) \equiv$

$$(X^2+1)^N \left(G_{\underline{v}}(X^4) - G_{\underline{e_1}}(X^4)\right) - X^K(X^2-1)^N \left(G_{\underline{v}}(X^4) - G_{\underline{e_2}}(X^4)\right) (\mathrm{mod}\ (X^4-1)^{N-1})$$

or

$$G_{\underline{u}}(X) - G_{\underline{f}}(X) \equiv (X^2+1)^N (X^4-1)^{N - LC_{k_1}^{\mathbb{F}_N}(\underline{v})} E_1(X^4) +$$

$$X^K(1-X^2)^N (X^4-1)^{N - LC_{k_2}^{\mathbb{F}_N}(\underline{v})} E_2(X^4) (\mathrm{mod}\ (X^4-1)^{N-1}).$$

So, we obtain

$$G_{\underline{u}}(X) - G_{\underline{f}}(X) \equiv 0 \left(\mathrm{mod}\ (X^2+1)^{N - \max(LC_{k_2}^{\mathbb{F}_N}(\underline{v}),1)} (X^2-1)^{N - \max(LC_{k_1}^{\mathbb{F}_N}(\underline{v}),1)}\right).$$

Hence, there exists an error-sequences $\underline{e}$ such that

$$n_0 + n_1 + n_2 + n_3 \ge 2\left(2N - \max(LC_{k_2}^{\mathbb{F}_N}(\underline{v}),1) - \max(LC_{k_1}^{\mathbb{F}_N}(\underline{v}),1\right).$$

This completes the proof of Theorem 2.

Thus, by Theorems 1 and 2, if $\underline{v}$ is a "good" sequence so is $\underline{u}$ and vice versa.

Remark 7. Let $N = 3$ and $\underline{v} = 0,0,1$ then $\underline{u} = 0,0,1,0,0,0,0,1,1,1,0,1$ for $m = 0$. Let $k_1 = k_2 = 1, k = 4$. Then we have $LC_1^{\mathbb{F}_N}(\underline{v}) = 0$ and $LC_4^{\mathbb{F}_N}(\underline{u}) = 3 \ge 0 = \min_{2k_1 + 2k_2 \le k} 2\left(LC_{k_1}^{\mathbb{F}_N}(\underline{v}) + LC_{k_2}^{\mathbb{F}_N}(\underline{v})\right)$.

3. Some applications

In this section we determine the exact values for the k-error linear complexity of $\underline{u}$ in (1) when $\underline{v}$ is a cyclotomic sequence of period $N > 3$.

Let N be an odd prime. If $d > 1$ is a divisor of $N-1$ and g is a fixed element of $\mathbb{F}_N$, then the cyclotomic classes of order d give a partition of $\mathbb{F}_N^* = \mathbb{F}_N \backslash \{0\}$ defined by

$$D_0 = \{g^{dn}: 0 \le n \le (N-1)/d - 1\} \text{ and } D_j = g^j D_0, 1 \le j \le d-1.$$

For fixed $c_0, c_1, \dots, c_{d-1} \in \mathbb{F}_N$ a *cyclotomic sequence* of order d is the N-periodic sequence $\underline{v} = (v_0, v_1, \dots, v_{N-1})$ defined by

$$v_i = \begin{cases} 0, \text{if } p|i, \\ c_j, \text{if } i(\text{mod } N) \in D_j, i = 0,1,2,\dots \end{cases}$$

We consider two examples.

Let $d = 2$, $N \equiv 3(\text{mod}4)$. The Legendre sequence $\underline{l} = \{l_i\}$ of period N is defined by

$$l_i = \begin{cases} 1, \text{if } i(\text{mod}N) \in D_0, \\ 0, \text{otherwise.} \end{cases}$$

Let $d = 6$, $N = A^2 + 27, A \equiv 1(\text{mod}3)$ and let $D = D_0 \cup D_1 \cup D_3$ be a Hall's difference set [15] ($3 \in D_1$). Denote by $\underline{h}$ a Hall's sextic residue sequence, i.e.

$$h_i = \begin{cases} 1, \text{if } i(\text{mod}N) \in D, \\ 0, \text{otherwise.} \end{cases}$$

Earlier, the linear complexity and the k-error linear complexity over $\mathbb{F}_N$ of the Legendre sequences and series of other cyclotomic sequences were investigated in [16, 17].

Lemma 8. [17] Let $\underline{v}$ be a cyclotomic sequence of order d of least period N. If $LC^{\mathbb{F}_N}(\underline{v}) = N$, then there exist $t: 1 \le t < d$ such that $LC_k^{\mathbb{F}_N}(\underline{v}) = N - t(N-1)/d$ for $1 \le k < t(N-1)/d$. Moreover, $t = 1$ for Legendre sequences and Hall's sextic residue sequences.

In the following we always suppose $(N-1)/d$ is large, or at least $(N-1)/d > 3$.

Theorem 9. Let $\underline{v}$ be a cyclotomic sequence of order d of least period N and $\underline{u}$ the interleaved binary sequence defined in (1). Let t be determined in Lemma 8.

(i). For $4 \le k < t(N-1)/d$, we have $LC_k^{\mathbb{F}_N}(\underline{u}) = 4LC_k^{\mathbb{F}_N}(\underline{v})$.

(ii). For $k \ge t(N-1)/d$, we have

$$LC_k^{\mathbb{F}_N}(\underline{u}) \le \begin{cases} 2LC_1^{\mathbb{F}_N}(\underline{v}) + 2\max(LC_{k-4}^{\mathbb{F}_N}(\underline{v}),1), \text{if } m \ne (N+1)/4, \\ LC_1^{\mathbb{F}_N}(\underline{v}) + 3\max(LC_{k-4}^{\mathbb{F}_N}(\underline{v}),1), \text{if } m = (N+1)/4. \end{cases}$$

Proof. (i). It follows from Theorem 1 that $4LC_k^{\mathbb{F}_N}(\underline{v}) \le LC_k^{\mathbb{F}_N}(\underline{u})$. Then by Theorem 2 we get that $LC_k^{\mathbb{F}_N}(\underline{u}) \le 4LC_1^{\mathbb{F}_N}(\underline{v})$. On the other hand, using $LC_k^{\mathbb{F}_N}(\underline{v}) = LC_1^{\mathbb{F}_N}(\underline{v})$ for $4 \le k < t(N-1)/d$ by [17], we prove the desired result.

(ii). By Lemma 5 there exist $\underline{e_i}, i = 1,2$, with $wt(\underline{e_1}) = 1$ and $wt(\underline{e_2}) \le k-4$, such that

$$G_{\underline{v}}(X) - G_{\underline{e_1}}(X) = (X-1)^{N-LC_1^{\mathbb{F}_N}(\underline{v})} H_1(X) \text{ and } G_{\underline{v}}(X) - G_{\underline{e_2}}(X) = (X-1)^{N-LC_{k-4}^{\mathbb{F}_N}(\underline{v})} H_2(X),$$

where $\gcd(H_i(x), x-1) = 1$.

Let $G_{\underline{f}}(X) = (1+X^2)^N(1-X^K)G_{\underline{e_1}}(X^4) + 2X^K G_{\underline{e_2}}(X^4)$. Then $wt(\underline{f}) \le k$. By (5) we obtain

$$\begin{aligned} G_{\underline{u}}(X) - G_{\underline{f}}(X) \quad &\equiv \quad (X^2+1)^N(1-X^K)\left(G_{\underline{v}}(X^4) - G_{\underline{e_1}}(X^4)\right) \\ &+ \quad 2X^K\left(G_{\underline{v}}(X^4) - G_{\underline{e_2}}(X^4)\right) + X^3(X^4-1)^{N-1} \\ &\equiv \quad (X^2+1)^N(1-X^K)(X^4-1)^{N-LC_1^{\mathbb{F}_N}(\underline{v})}H_1(X^4) + \quad 2X^M(X^4-1)^{N-LC_{k-4}^{\mathbb{F}_N}(\underline{v})}H_2(X^4) \\ &+ \quad X^3(X^4-1)^{N-1}(\text{mod } (X^4-1)^N) \end{aligned}$$

Since

$$G_{\underline{u}}(X) - G_{\underline{f}}(X) \equiv 0(\text{mod } (X^2+1)^{\min(N-LC_{k-4}^{\mathbb{F}_N}(\underline{v}),N-1)}(X^2-1)^{N-LC_1^{\mathbb{F}_N}(\underline{v})})$$

if $m \neq (N+1)/4$, and

$$G_{\underline{u}}(X) - G_{\underline{f}}(X) \equiv 0(\mathrm{mod}((X^2+1)(X-1))^{\min(N-LC_{k-4}^{\mathbb{F}_N}(\underline{v}),N-1)}(X+1)^{N-LC_1^{\mathbb{F}_N}(\underline{v})})$$

if $m = (N+1)/4$, so we have $LC_k^{\mathbb{F}_N}(\underline{u}) \leq 2LC_1^{\mathbb{F}_N}(\underline{v}) + 2\max(LC_{k-4}^{\mathbb{F}_N}(\underline{v}),1)$, if $m \neq (N+1)/4$, and $LC_k^{\mathbb{F}_N}(\underline{u}) \leq LC_1^{\mathbb{F}_N}(\underline{v}) + 3\max(LC_{k-4}^{\mathbb{F}_N}(\underline{v}),1)$ if $m = (N+1)/4$.

However, for $1 \leq k \leq 3$, we have following two theorems.

Theorem 10. Let $\underline{v}$ be a cyclotomic sequence of order d of least period N and $\underline{u}$ the interleaved binary sequence defined in (1). If $m \neq (N+1)/4$, we have

$$LC_k^{\mathbb{F}_N}(\underline{u}) = \begin{cases} 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 1, \text{if } k = 1,2, \\ 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 2, \text{if } k = 3. \end{cases}$$

Theorem 11. Let $\underline{v}$ be a cyclotomic sequence of order d of least period N and $\underline{u}$ the interleaved binary sequence defined in (1). If $m = (N+1)/4$. we have for $1 \leq k \leq 3$

$$LC_k^{\mathbb{F}_N}(\underline{u}) = N + 3LC_k^{\mathbb{F}_N}(\underline{v}).$$

To prove Thereoms 10 and 11, we need following discussion.

By formula (2.2) in [17], there exists $F(X) \in \mathbb{F}_N[X]$, $F(1) \neq 0$ such that

$$G_{\underline{v}}(X) = G_{\underline{v}}(1) + (X-1)^{t(N-1)/d}F(X).$$

So, by (5), we get

$$G_{\underline{u}}(X) \equiv G_{\underline{v}}(1)((X^2+1)^N - X^K(X^2-1)^N)(\mathrm{mod}\ (X^4-1)^{t(N-1)/d}). \quad (7)$$

Also, there exists $T(X) \in \mathbb{F}_N[X], T(1) \neq 0$ such that

$$G_{\underline{u}}(X) \equiv G_{\underline{v}}(1)((X^2+1)^N - X^K(X^2-1)^N) + (X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}\ (X^4-1)^{t(N-1)/d+1})$$

Lemma 12. If α is a root of the polynomial $Q(X)$ with the multiplicity $n < N$, then $wt(Q(X)) \geq n+1$.

Proof. Let $Q(X) = \sum_i a_i X^{k_i}$. Without loss of generality, we can assume that $\alpha = 1$. Denote $\sum_i a_i X^{k_i(\mathrm{mod}\ N)}$ by $\bar{Q}(X)$. Then $Q(x) \equiv \bar{Q}(X)(\mathrm{mod}(X-1)^N)$ and $wt(Q(X)) \geq wt(\bar{Q}(X))$.

Now we show that $wt(\bar{Q}(X)) \geq n+1$ by contradiction. Let $\bar{Q}(X) = \sum_{i=0}^{f} b_i X^{l_i}$ with $b_i \neq 0$, $f < n$ and $0 \leq l_i \leq N-1$. Let $Q^{(j)}(X)$ be a formal derivative of order j of the polynomial $Q(X)$ and $Q^{(0)}(X) = Q(X)$. Since $\bar{Q}^{(j)}(1) = 0$ for $0 \leq j \leq f-1$ and $(X^l)^{(j)}|_{X=1} = l(l-1)(l-2)\dots(l-j+1)$ for all $1 \leq j \leq l$, then we have $\sum_{i=0}^{f-1} b_i l_i^j = 0$, for all $j = 0,1,\dots,f-1$.

Thus we obtain the linear system of f-equations over the field $\mathbb{F}_N$, and the Vandermonde determinate $|l_i^j|_{i,j=0}^{f-1} \neq 0$. Hence, $b_i = 0$ for all $0 \leq i \leq f-1$. This contradicts the fact that $Q(X) \not\equiv 0(\mathrm{mod}(X-1)^N)$.

The following lemma is useful for us to investigate $G_{\underline{e}}(X)$ in (6) in the proof of Lemma 6.

Lemma 13. Let $G_{\underline{u}}(X)$ and $G_{\underline{e}}(X)$ satisfy (3). Let $m_0 = min\{n_0, n_2\}$ and $m_1 = min\{n_1, n_3\}$. Then we have

(1) $wt(G_{\underline{e,0}}) \geq m_1 + 1$ if $G_{\underline{e,0}}(X^2) \not\equiv 0(\mathrm{mod}\ (X^2+1)^N)$;

(2) $wt(G_{\underline{e,1}}) \geq m_0 + 1$ if $G_{\underline{e,1}}(X^2) \not\equiv 0(\mathrm{mod}\ (X^2-1)^N)$;

(3) $wt(G_{\underline{e,0}}) \geq m_0$ if $2G_{\underline{v}}(1) - G_{\underline{e,0}}(X^2) \not\equiv 0(\mathrm{mod}\ (X^2-1)^N)$;

(4) $wt(G_{\underline{e,1}}) \geq m_1$ if $2G_{\underline{v}}(1)X^{K-1} - G_{\underline{e,1}}(X^2) \not\equiv 0(\mathrm{mod}\ (X^2+1)^N)$

where $G_{\underline{e}}(X) = G_{\underline{e,0}}(X^2) + XG_{\underline{e,1}}(X^2)$ with $wt(G_{\underline{e,i}}(X)) < t(N-1)/d, i = 0,1$.

Proof. Using $G_{\underline{u}}(X), G_{\underline{u}}(-X)$ as in the proof of Lemma 6, then by (5) we get that

$$\begin{cases} G_{\underline{v}}(X^4)(X^2+1)^N - G_{\underline{e,0}}(X^2) \equiv 0(\mathrm{mod}\ (X^2-1)^{m_0}(X^2+1)^{m_1}) \\ X^K G_{\underline{v}}(X^4)(1-X^2)^N - XG_{\underline{e,1}}(X^2) - X^3(X^4-1)^{N-1} \equiv 0(\mathrm{mod}(X^2-1)^{m_0}(X^2+1)^{m_1}). \end{cases}$$

From this and (7) we can establish that

$$\begin{cases} G_{\underline{e},0}(X^2) \equiv 0(\mathrm{mod}\ (X^2+1)^{m_1}) \\ 2G_{\underline{v}}(1) - G_{\underline{e},0}(X^2) \equiv 0(\mathrm{mod}\ (X^2-1)^{\min(t(N-1)/d, m_0)}) \\ G_{\underline{e},1}(X^2) \equiv 0(\mathrm{mod}\ (X^2-1)^{\min(m_0, N-1)}) \\ 2G_{\underline{v}}(1)X^{K-1} - G_{\underline{e},1}(X^2) \equiv 0(\mathrm{mod}\ (X^2+1)^{\min(t(N-1)/d, m_1)}) \end{cases} \tag{8}$$

Then the assertions of this lemma follow immediately from (8) and Lemma 12.

Lemma 14. Let $G_{\underline{u}}(X)$ and $G_{\underline{e}}(X)$ satisfy (3). Then we have

- $n_0 = n_2$ if $G_{\underline{e},1}(X^2) = 0$;
- $n_1 = n_3$ if $G_{\underline{e},0}(X^2) = 0$.

Proof. By (7), we have $G_{\underline{u}}(1) = G_{\underline{u}}(-1)$ and $G_{\underline{u}}(\beta) = -G_{\underline{u}}(-\beta)$. Thus we can get the desired result.

Proof. (proof of Theorem 10) (i). Suppose that $k = 1,2$. Since $(X^2-1)^N + 2 = (X^2+1)^N$ in $\mathbb{F}_N[X]$, then by (7) we have

$$G_{\underline{u}}(X) \equiv G_{\underline{v}}(1)((X^2+1)^N(1-X^K) + 2X^K)(\mathrm{mod}(X^4-1)^{t(N-1)/d}),$$

where $K = 4N - 4m + 1$, that is,

$$G_{\underline{u}}(X) - 2X^K G_{\underline{v}}(1) \equiv G_{\underline{v}}(1)(X^2+1)^N(1-X^K)(\mathrm{mod}(X^4-1)^{t(N-1)/d}).$$

So, $(X^2+1)^{t(N-1)/d}(X-1) | (G_{\underline{u}}(X) - 2X^K G_{\underline{v}}(1))$. Hence, by (4) and Lemma 8, we have $LC_k^{\mathbb{F}_N}(\underline{u}) \le 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 1$.

Now we show that $LC_k^{\mathbb{F}_N}(\underline{u}) = 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 1$. Conversely, suppose that $LC_k^{\mathbb{F}_N}(\underline{u}) < 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 1$. Then there exists $G_{\underline{e}}(X)$ with $wt(G_{\underline{e}}(X)) \le 2$ such that (3) holds and $n_0 + n_1 + n_2 + n_3 \ge 2N - 2LC_k^{\mathbb{F}_N}(v) + 2$, that is

$$n_0 + n_1 + n_2 + n_3 + 2LC_k^{\mathbb{F}_N}(v) \ge 2N + 2. \tag{9}$$

It follows from Lemma 6 that $m_0 + m_1 \ge 2$. So we obtain $G_{\underline{e},0}(X^2) \equiv 0(\mathrm{mod}(X^2+1)^N)$ or $G_{\underline{e},1}(X^2) \equiv 0(\mathrm{mod}(X^2-1)^N)$ by Lemma 13(1).

We consider four cases.

(1.1). Let $G_{\underline{e},0}(X^2) = 0$. Lemmas 13(3) and 14 lead to that $m_0 = 0$ and $m_1 = n_1 = n_3$. By Lemma 8, we have $n_1 + n_3 \ge N - LC_k^{\mathbb{F}_N}(\underline{v}) + 2 > k + 2$. It follows from Lemma 13(4) that

$$G_{\underline{e},1}(X^2) = 2G_{\underline{v}}(1)X^{K-1} + A(X^2)(X^2+1)^N,$$

where $A(X^2) = aX^{K-1}$ or $A(X^2) = aX^{K-1-2N}$ with $a \in \mathbb{F}_N$ and $\deg A(X^2) < 2N$. So, by (8) we have

$$G_{\underline{u}}(X) - G_{\underline{e}}(X) \equiv G_{\underline{v}}(1)(X^2+1)^N(1-X^K - XA(X^2)) + (X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}(X^4-1)^{t(N-1)/d+1}).$$

Here, $n_1 = n_3 = t(N-1)/d$, $\max(n_0, n_2) = 1$ for $K \not\equiv 0(\mathrm{mod}N)$, i.e., $m \ne (N+1)/4$. Then we have $n_0 + n_1 + n_2 + n_3 + 2LC_k^{\mathbb{F}_N}(v) = 2N + 1$ by Lemma 8. This is in contradiction with (10).

(1.2). Let $G_{\underline{e},0}(X^2) \equiv 0(\mathrm{mod}(X^2+1)^N)$ and $G_{\underline{e},0}(X^2) \ne 0$. Then we have $G_{\underline{e},1}(X^2) = 0$. Thus by Lemmas 13(4) and 14, we have $m_1 = 0$ and $m_0 = n_0 = n_2$. Lemma 13(3) leads to that $G_{\underline{e},0}(X^2) = 2G_{\underline{v}}(1) + b(X^2-1)^N$ with $b \in \mathbb{F}_N$. So we obtain that

$$G_{\underline{u}}(X) - G_{\underline{e},0}(X^2) \equiv G_{\underline{v}}(1)(X^2-1)^N(1-X^K) - b(X^2-1)^N + (X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}(X^4-1)^{t(N-1)/d+1})$$

by (8). Thus, $n_0 = n_2 = t(N-1)/d$, $\max(n_1, n_3) \le 1$ for $K \not\equiv 0(\mathrm{mod}N)$. Similar to the proof of (1.1), we have a contradiction.

(1.3). Let $G_{\underline{e},1}(X^2) = 0$. Similar to the proof of (1.2), we get a contradiction.

(1.4). Let $G_{\underline{e},1}(X^2) = C(X^2)(X^2-1)^N$, where $C(X) \ne 0$ and $C(X) \in \mathbb{F}_N[X]$. Then we have $G_{\underline{e},0}(X^2) = 0$. Similar to the proof of (1.1), we get a contradiction.

(ii). Let $k = 3$. Consider

$$G_{\underline{f}}(X) \equiv 2G_{\underline{v}}(1)(X^{(N+K)/2+2N} + X^{(N+K)/2} - X^{K+2N})$$
$$\equiv 2G_{\underline{v}}(1)(X^K + (X^{(N+K)/2} - X^K)(X^2+1)^N)(\mathrm{mod}(X^4-1)^N),$$

then we have

$$G_{\underline{u}}(X) - G_{\underline{f}}(X) \equiv G_{\underline{v}}(1)(X^2+1)^N\big(1 + X^K - 2X^{(N+K)/2}\big)(\mathrm{mod}(X^4-1)^{t(N-1)/d}).$$

Hence $(X^2+1)^{t(N-1)/d}(X-1)^2 | (G_{\underline{u}}(X) - G_{\underline{f}}(X))$. Thus, there exists an error sequence $\underline{e}$ such that $LC_k^{\mathbb{F}_N}(\underline{u}) \le 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 2$ by Lemma 8 and (4).

The assertion that $LC_k^{\mathbb{F}_N}(\underline{u}) = 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 2$ can be proved similarly to that of (i) of this Lemma, so we only give a sketched proof.

If $LC_k^{\mathbb{F}_N}(\underline{u}) < 2N + 2LC_k^{\mathbb{F}_N}(\underline{v}) - 2$, then we obtain that

$$n_0 + n_1 + n_2 + n_3 \ge 2N - 2LC_k^{\mathbb{F}_N}(v) + 3, \tag{10}$$

and $m_0 + m_1 \ge 3$ by Lemma 8, and $G_{\underline{e,0}}(X^2) \equiv 0(\mathrm{mod}(X^2+1)^N)$ or $G_{\underline{e,1}}(X^2) \equiv 0(\mathrm{mod}\ (X^2-1)^N)$ by Lemma 13.

Again, we consider four cases.

(2.1). Let $G_{\underline{e,0}}(X^2) = 0$. Then by Lemmas 13(3) and 14 we get $m_0 = 0$ and $m_1 = n_1 = n_3$. Lemma 8 leads to that $n_1 + n_3 \ge N - LC_k^{\mathbb{F}_N}(\underline{v}) + 3 > k + 3$ and Lemma 13(4) leads to that $G_{\underline{e,1}}(X^2) \equiv G_{\underline{v}}(1)X^{K-1}(\mathrm{mod}(X^2+1)^N)$. Therefore, we obtain

$$G_{\underline{e,1}}(X^2) = 2G_{\underline{v}}(1)\big(X^{K-1} + (aX^l - X^{K-1})(X^2+1)^N\big)$$

or

$$G_{\underline{e,1}}(X^2) = 2G_{\underline{v}}(1)\big(X^{K-1} + (aX^l - X^{K-1-2N})(X^2+1)^N\big)$$

where $a \in \mathbb{F}_N$, $0 \le l < 2N$. So we have by (8) that

$$G_{\underline{u}}(X) - XG_{\underline{e,1}}(X^2) \equiv G_{\underline{v}}(1)(X^2+1)^N\big(1 + X^K - 2aX^l\big) +$$
$$(X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}\ (X^4-1)^{t(N-1)/d+1}),$$

or

$$G_{\underline{u}}(X) - XG_{\underline{e,1}}(X^2) \equiv G_{\underline{v}}(1)(X^2+1)^N\big(1 - X^K - 2aX^l + 2X^{K-2N}\big) +$$
$$(X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}\ (X^4-1)^{t(N-1)/d+1}).$$

So, $n_1 = n_3 = t(N-1)/d$, $\max(n_0, n_2) = 2$ for $K \not\equiv 0(\mathrm{mod}\ N)$ for both case, which is in contradiction with (10).

(2.2). Let $G_{\underline{e,0}}(X^2) \equiv 0(\mathrm{mod}\ (X^2+1)^N)$ and $G_{\underline{e,0}}(X^2) \ne 0$. Then $wt(G_{\underline{e,1}}(X^2)) \le 1$.

If $wt(G_{\underline{e,1}}(X^2))) = 1$, then $G_{\underline{e,0}}(X^2) = aX^l(X^2+1)^N, a \in \mathbb{F}_N, 0 \le l < 2N$. By Lemma 13 (2) and (4), $m_0 = 0$ and $G_{\underline{e,1}}(X^2) = 2G_{\underline{v}}(1)X^{K-1}$ or $G_{\underline{e,1}}(X^2) = 2G_{\underline{v}}(1)X^{K-1-2N}$. Thus

$$G_{\underline{u}}(X) - G_{\underline{e}}(X) \equiv G_{\underline{v}}(1)(X^2+1)^N(1 - X^K) - 2aX^l(X^2+1)^N +$$
$$(X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}\ (X^4-1)^{t(N-1)/d+1})$$

or

$$G_{\underline{u}}(X) - G_{\underline{e}}(X) \equiv G_{\underline{v}}(1)(X^2+1)^N(1 - X^K) - 2aX^l(X^2+1)^N$$
$$-2G_{\underline{v}}(1)X^{K-2N}(X^{2N}-1) + (X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}\ (X^4-1)^{t(N-1)/d+1}).$$

So, $n_0 + n_1 + 2n_2 \le 2N - 2LC_k^{\mathbb{F}}(\underline{v}) + 2$ for $K \not\equiv 0(\mathrm{mod}\ N)$.

Now, let $G_{\underline{e,1}}(X^2) = 0$. By Lemmas 13(4) and 10, $m_1 = 0$ and $m_0 = n_0 = n_2 \ge 3$. By Lemma 13 (3), $G_{\underline{e,0}}(X^2) = 2G_{\underline{v}}(1) + C(X^2)(X^2-1)^N$ for some $C(X) \in \mathbb{F}_N[X]$. Therefore, since $G_{\underline{e,0}}(X^2) \equiv 0(\mathrm{mod}(X^2+1)^N)$ we get $2G_{\underline{v}}(1) - 2C(X^2) \equiv 0(\mathrm{mod}(X^2+1)^N)$. So, $G_{\underline{e}}(X) \equiv 2G_{\underline{v}}(1)(X^2-1)^N(\mathrm{mod}\ (X^4-1)^N)$. We obtain a contradiction since $wt(G_{\underline{e,0}}(X^2)) = 3$.

(2.3). Let $G_{\underline{e},1}(X^2)=0$. Similarly to that of (2.2), we can get a contradiction.

(2.4). Let $G_{\underline{e},1}(X^2)=C(X^2)(X^2-1)^N$, where $C(X)\neq 0$ and $C(X)\in\mathbb{F}_N[X]$. Since $wt(G_{\underline{e}}(X))\leq 3$, then $wt(G_{\underline{e},0}(X^2))\leq 1$.

If $wt(G_{\underline{e},0}(X^2))=1$, then $G_{\underline{e},1}(X^2)=cX^r(X^2-1)^N, c\in\mathbb{F}_N, 0\leq r<2N$. By Lemma 13 (1) and (3), $m_1=0$ and $G_{\underline{e},0}(X^2)=2G_{\underline{v}}(1)$. Thus, by (8) we have

$$G_{\underline{u}}(X)-G_{\underline{e}}(X)\equiv G_{\underline{v}}(1)(X^2-1)^N(1-X^K)-cX^r(X^2-1)^N+$$
$$(X^4-1)^{t(N-1)/d}T(X^4)(\mathrm{mod}\ (X^4-1)^{t(N-1)/d+1}).$$

So, $n_0+n_1+2n_2\leq 2N-2LC_k^{\mathbb{F}}(\underline{v})+2$ for $K\not\equiv 0(\mathrm{mod}\ N)$. This is in contradiction with (11).

Now, let $G_{\underline{e},0}(X^2)=0$. By Lemmas 13 (3) and 14 $m_1=0$ and $m_0=n_0=n_2\geq 3$. By Lemma 9 (4), $G_{\underline{e},0}(X^2)=2G_{\underline{v}}(1)X^{K-1}+D(X^2)(X^2+1)^N$ for some $D(X^2)\in\mathbb{F}_N[X]$. Therefore, since $G_{\underline{e},1}(X^2)\equiv 0(\mathrm{mod}(X^2-1)^N)$ we get $2G_{\underline{v}}(1)X^{K-1}-2D(X^2)\equiv 0(\mathrm{mod}\ (X^2-1)^N)$. So,

$$G_{\underline{e}}(X)\equiv 2G_{\underline{v}}(1)X^{K-1}(X^2-1)^N(\mathrm{mod}\ (X^4-1)^N).$$

We obtain a contradiction since $wt(G_{\underline{e},0}(X^2))=3$.

Remark 15. The assertion $LC_k^{\mathbb{F}_N}(\underline{u})=2N+2LC_k^{\mathbb{F}_N}(\underline{v})-1, k=1,2$ is true for any N periodic cyclotomic sequence $\underline{v}$ with $LC_k^{\mathbb{F}_N}(\underline{v})>1$.

Proof. (proof of Theorem 11) If $m=(N+1)/4$ then $K=3N$. By (7),

$$G_{\underline{u}}(X)-2G_{\underline{v}}(1)X^{3N}\equiv(X^2+1)^NF(X^4)(1-X^{3N})(\mathrm{mod}\ (X^4-1)^{t(N-1)/d}).$$

So, $(X^2+1)^{t(N-1)/d}(X-1)^{t(N-1)/d}|(G_{\underline{u}}(X)-2G_{\underline{v}}(1)X^{3N})$. Thus, by Lemma 8 and (4),

$$LC_k^{\mathbb{F}_N}(\underline{u})\leq 4N-3t(N-1)/d \text{ or } LC_k^{\mathbb{F}_N}(\underline{u})\leq N+3LC_k^{\mathbb{F}_N}(\underline{v}).$$

If $LC_k^{\mathbb{F}_N}(\underline{u})\leq N+3LC_k^{\mathbb{F}_N}(\underline{v})$, then there exists $G_{\underline{e}}(X)\in\mathbb{F}_N[X]$ with $wt(G_{\underline{e}}(X))\leq k$ such that (3) holds for $n_0+n_1+n_2+n_3>3N-3LC_k^{\mathbb{F}^{\mathbb{F}_N}}(\underline{v})$. Lemma 6 leads to that $n_i\geq 1, i=0,1,2,3$, and $m_0+m_1>k$. By Lemma 13 (3) and (4), we get $G_{\underline{e},0}(X^2)\neq 0$ and $G_{\underline{e},1}(X^2)\neq 0$. Then, by Lemma 13 (1) and (2), $wt(G_{\underline{e},0}(X^2))\geq 2$ and $wt(G_{\underline{e},1}(X^2))\geq 2$, which is in contradiction with $k<4$.

Thus, we have established the following.

Corollary 16. (i). Let $\underline{v}$ be the N periodic Legendre sequence and $\underline{u}$ be defined by (1). Then

$$LC_k^{\mathbb{F}_N}(\underline{u})=\begin{cases}3N, & \text{if } k=1,2 \text{ and } m\neq(N+1)/4,\\ 3N-1, & \text{if } k=3 \text{ and } m\neq(N+1)/4,\\ (5N+3)/2, & \text{if } k=1,2,3 \text{ and } m=(N+1)/4,\\ 2N+2, & \text{if } 4\leq k<(N-1)/2.\end{cases}$$

(ii). Let $\underline{v}$ be the N periodic Hall's sextic residue sequence and $\underline{u}$ be defined by (1). Then

$$LC_k^{\mathbb{F}_N}(\underline{u})=\begin{cases}(11N-2)/3, & \text{if } k=1,2 \text{ and } m\neq(N+1)/4,\\ (11N-5)/3, & \text{if } k=3 \text{ and } m\neq(N+1)/4,\\ (7N+1)/2, & \text{if } k=1,2,3 \text{ and } m=(N+1)/4,\\ (10N+2)/3, & \text{if } 4\leq k<(N-1)/6.\end{cases}$$

In a conclusion, we give an upper bound for $k\geq t(N-1)/d$.

Corollary 17. (i). Let $\underline{v}$ be the N periodic Legendre sequence, and $\underline{u}$ be defined by (1). If $k\geq(N-1)/2+4$, then

$$LC_k^{\mathbb{F}_N}(\underline{u})\leq\begin{cases}N+3, & \text{if } m\neq(N+1)/4,\\ (N+3)/2, & \text{if } m=(N+1)/4.\end{cases}$$

(ii). Let $\underline{v}$ be the N periodic Hall's sextic residue sequence, and $\underline{u}$ be defined by (1). If $k\geq(N-1)/6+4$, then

$$LC_k^{\mathbb{F}_N}(u)\leq\begin{cases}3N+1, & \text{if } m\neq(N+1)/4,\\ (17N+7)/6, & \text{if } m=(N+1)/4.\end{cases}$$

The investigation of the k-error linear complexity of $\underline{u}$ obtained from Legendre sequence or Hall's sextic residue sequence may be continued in the same way. But for the other values of k we have a significant decrease of the linear complexity. So, further research is not worth the effort.

4. Conclusion

In this paper, we first established over the finite field $\mathbb{F}_N$ the relation between the k-error linear complexity of the binary interleaved sequences of period $4N$ and that of the binary sequences of period N from which the interleaved sequences derived. Then, as applications, we obtained the exact value of the k-error linear complexity for small value of k of the series of interleaved sequences derived from the cyclotomic sequences. We also studied the k-error linear complexity of the interleaved sequences obtained from Legendre sequences and Hall's sextic residue sequences, respectively. Our results show that these sequences are quite stable.

Acknowledgements

The reported study was funded by RFBR and NSFC according to the research project no. 19-51-53003. X. Du is partially supported by the National Natural Science Foundation of China under grants no.61562077 and no.61772022.

References

[1] Gong G 1995 Theory and applications of q-ary interleaved sequences *IEEE Trans. Information Theory* **41** 400–411
[2] Tang X H and Gong G 2010 New constructions of binary sequences with optimal autocorrelation value/magnitude *IEEE Trans. Inf. Theory* **56** 1278–1286
[3] Tang X H and Ding C 2010 New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value *IEEE Trans. Inf. Theory* **56** 6398–6405
[4] Yan T, Chen Z and Li B 2014 A general construction of binary interleaved sequences of period $4N$ with optimal autocorrelation *Inf. Sci.* **287** 26–31
[5] Li N and Tang X 2011 On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude *IEEE Trans. Inf. Theory* **57** 7597–7604
[6] Xiong H, Qu L, Li C, and Fu S 2013 Linear complexity of binary sequences with interleaved structure *IET Communications* **7 (15)** 1688–1696
[7] Lidl R and Niederreiter H 1983 *Finite Fields* (Addison-Wesley)
[8] Meidl W and Niederreiter H 2013 Periodic sequences with maximal linear complexity and large k-error linear complexity *AAECC* **14** 273–286.
[9] Niederreiter H 2003 Linear complexity and related complexity measures for sequences. Progress in Cryptology-Indocrypt 2003 *Lecture Notes in Computer Science* **2904** ed T Johansson and S Maitra (Springer-Verlag Berlin) 1–17
[10] Stamp M and Martin C F 1993 An algorithm for the k-error linear complexity of binary sequences with period 2^n *IEEE Trans. Inform. Theory* **39** 1398–1401
[11] Ding C, Xiao G and Shan W 1991 The Stability Theory of Stream Ciphers. *Lecture Notes in Computer Science* (Springer-Verlag, Berlin) p 561
[12] Massey J L and Serconek S 1996 Linear complexity of periodic Sequences: A General Theory, Journal of Complexity *Lecture Notes in Computer Science* (Springer-Verlag Berlin) 358–371
[13] Rueppel R A 1986 *Analysis and Design of Stream Ciphers* (Springer-Verlag Berlin)
[14] Wang Q and Du X N 2010 The linear complexity of binary sequences with optimal autocorrelation *IEEE Trans. Inf. Theory* **56 (12)** 6388–6397
[15] Hall M 1975 *Combinatorial Theory* (Wiley, New York)
[16] Aly H and Winterhof A 2006 On the k-error linear complexity over F_p of Legendre and Sidelnikov sequences *Des. Codes Cryptogr.* **40** 369–374
[17] Aly H, Meidl W and Winterhof A 2007 On the k-error linear complexity of cyclotomic sequences *J. Math. Crypt.* **1** 1–14