About the k-Error Linear Complexity over $\mathbb{F}_p$ of sequences of length $2p$ with optimal three-level autocorrelation

Vladimir Edemskiy

November 26, 2018

Abstract

We investigate the $k$-error linear complexity over $\mathbb{F}_p$ of binary sequences of length $2p$ with optimal three-level autocorrelation. These balanced sequences are constructed by cyclotomic classes of order four using a method presented by Ding et al.

Keywords: binary sequences, linear complexity, cyclotomy

Mathematics Subject Classification (2010): 94A55, 94A60, 11B50.

1 Introduction

Autocorrelation is an important measure of pseudo-random sequence for their application in code-division multiple access systems, spread spectrum communication systems, radar systems and so on [7]. An important problem in sequence design is to find sequences with optimal autocorrelation. In their paper, Ding et al. [4] gave several new families of binary sequences of period $2p$ with optimal autocorrelation $\{-2, 2\}$.

The linear complexity is another important characteristic of pseudo-random sequence, which is significant for cryptographic applications. It is defined as the length of the shortest linear feedback shift register that can generate the sequence [10]. The linear complexity of above-mention sequences over the finite field of order two was investigated in [11] and in [6] over the finite field $\mathbb{F}_p$ of $p$ elements and other finite fields. However, high linear complexity can not guarantee that the sequence is secure. For example, if changing one or
few terms of a sequence can greatly reduce its linear complexity, then the resulting key stream would be cryptographically weak. Ding et al. [5] noticed this problem first in their book, and proposed the weight complexity and the sphere complexity. Stamp and Martin [12] introduced the $k$-error linear complexity, which is the minimum of the linear complexity and sphere complexity. The $k$-error linear complexity of a sequence $r$ is defined by $L_k(r) = \min_{t} L(t)$, where the minimum of the linear complexity $L(t)$ is taken over all $N$-periodic sequences $t = (t_n)$ over $\mathbb{F}_p$ for which the Hamming distance of the vectors $(r_0, r_1, \ldots, r_{N-1})$ and $(t_0, t_1, \ldots, t_{N-1})$ is at most $k$. Complexity measures for sequences over finite fields, such as the linear complexity and the $k$-error linear complexity, play an important role in cryptology. Sequences that are suitable as keystreams should possess not only a large linear complexity but also the change of a few terms must not cause a significant decrease of the linear complexity.

In this paper we derive the $k$-error linear complexity of binary sequences of length $2p$ from [4] over $\mathbb{F}_p$. These balanced sequences with optimal three-level autocorrelation are constructed by cyclotomic classes of order four. Earlier, the linear complexity and the $k$-error linear complexity over $\mathbb{F}_p$ of the Legendre sequences and series of other cyclotomic sequences of length $p$ were investigated in [1, 2].

## 2 Preliminaries

First, we briefly repeat the basic definitions from [4] and the general information.

Let $p$ be a prime of the form $p \equiv 1 \pmod{4}$, and let $\theta$ be a primitive root modulo $p$ [9]. By definition, put $D_0 = \{\theta^{4s} \mod p; s = 1, \ldots, (p-1)/4\}$ and $D_n = \theta^n D_0, n = 1, 2, 3$. Then these $D_n$ are cyclotomic classes of order four [8].

The ring of residue classes $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ under the isomorphism $\phi(a) = (a \mod 2, a \mod p)$ [9]. Ding et al. considered balanced binary sequences defined as

$$u_i = \begin{cases} 1, & \text{if } i \mod 2p \in C, \\ 0, & \text{if } i \mod 2p \notin C, \end{cases} \quad (1)$$

for $C = \phi^{-1}(\{0\} \times (\{0\} \cup D_m \cup D_j) \cup \{1\} \times (D_l \cup D_j))$ where $m, j$, and $l$ are pairwise distinct integers between 0 and 3 [4]. Here we regard them as
sequences over the finite field $\mathbb{F}_p$.

By [4], if $\{u_i\}$ has an optimal autocorrelation value then $p \equiv 5 \pmod{8}$ and $p = 1 + 4y^2$, $(m, j, l) = (0, 1, 2), (0, 3, 2), (1, 0, 3), (1, 2, 3)$ or $p = x^2 + 4$, $y = -1$, $(m, j, l) = (0, 1, 3), (0, 2, 3), (1, 2, 0), (1, 3, 0)$. Here $x, y$ are integers and $x \equiv 1 \pmod{4}$.

It is well known [3] that if $r$ is a binary sequence with period $N$, then the linear complexity $L(r)$ of this sequence is defined by

$$L(r) = N - \deg \gcd(x^N - 1, S_r(x)),$$

where $S_r(x) = r_0 + r_1x + \ldots + r_{N-1}x^{N-1}$. Let’s assume we investigate the linear complexity of $u$ over $\mathbb{F}_p$ and with a period $2p$. So,

$$L(u) = 2p - \deg \gcd((x^2 - 1)^p, S_u(x)).$$

The weight of $f(x)$, denoted as $w(f)$, is defined as the number of nonzero coefficients of $f(x)$. From our definitions it follows that if the Hamming distance of the vectors $(u_0, u_1, \ldots, u_{2p-1})$ and $(t_0, t_1, \ldots, t_{2p-1})$ is at most $k$ then there exists $f(x) \in \mathbb{F}_p$, $w(f) \leq k$ such that $S_l(x) = S_u(x) + f(x)$ and the reverse is also true. Therefore

$$L_k(u) = 2p - \max_{f(x)}(m_0 + m_1) \quad (2)$$

where $0 \leq m_j \leq p$, $S_u(x) + f(x) \equiv 0 \pmod{(x - 1)^{m_0}(x + 1)^{m_1}}$ and $f(x) \in \mathbb{F}_p[x], w(f) \leq k$.

Let $g$ be an odd number in the pair $\theta, \theta + p$, then $g$ is a primitive root modulo $2p$ [9]. By definition, put $H_0 = \{g^{4s} \pmod{2p} ; s = 1, \ldots, (p - 1)/4\}$. Denote by $H_n$ a set $g^nH_0, n = 1, 2, 3$. Let us introduce the auxiliary polynomial $S_n(x) = \sum_{i \in H_n} x^i$. The following formula was proved in [3].

$$S_u(x) \equiv (x^p + 1)S_j(x) + x^pS_m(x) + S_l(x) + 1 \pmod{(x^{2p} - 1)}. \quad (3)$$

By (3) we have

$$\begin{cases} S_u(x) \equiv 2S_j(x) + S_m(x) + S_l(x) + 1 \pmod{(x - 1)^p}, \\
S_u(x) \equiv S_l(x) - S_m(x) + 1 \pmod{(x + 1)^p}. \end{cases} \quad (4)$$

Let the sequences $\{q_i\}$ and $\{v_i\}$ be defined by

$$\begin{cases} 2, \quad \text{if } i \mod p \in D_j, \\
1, \quad \text{if } i \mod p \in \{0\} \cup D_m \cup D_l, \quad \text{and } v_i = \begin{cases} 1, \quad \text{if } i \mod p \in \{0\} \cup D_m, \\
-1, \quad \text{if } i \mod p \in D_l, \\
0, \quad \text{otherwise,} \end{cases} \\
0, \quad \text{otherwise,} \end{cases} \quad (5)$$
By definition, put $S_q(x) = \sum_{i=0}^{p-1} q_i x^i$ and $S_v(x) = \sum_{i=0}^{p-1} v_i x^i$. Then by the choice of $g$ we obtain that

$$
\begin{cases}
2S_j(x) + S_m(x) + S_l(x) + 1 \equiv S_q(x) \pmod{(x-1)^p}, \\
S_m(x) - S_l(x) + 1 \equiv S_v(x) \pmod{(x-1)^p}.
\end{cases}
$$

As noted above, the $k$-error linear complexity of cyclotomic sequences was investigated in [2]. With the aid of methods from [2] it is an easy matter to prove the following

$$L_k(q) = \begin{cases}
3(p - 1)/4 + 1, & \text{if } 0 \leq k \leq (p - 1)/4, \\
(p - 1)/2 + 1, & \text{if } (p - 1)/4 + 1 \leq k < (p - 1)/3, \\
1, & \text{if } k = (p - 1)/2,
\end{cases}
$$

and $(p - 1)/4 + 1 \leq L_k(q) \leq (p - 1)/2 + 1$ if $(p - 1)/3 \leq k < (p - 1)/2$.

$$L_k(v) = \begin{cases}
p, & \text{if } k = 0, \\
3(p - 1)/4 + 1, & \text{if } 1 \leq k < (p - 1)/4, \\
(p - 1)/2 + 1, & \text{if } (p - 1)/4 + 1 \leq k < (p - 1)/3, \\
0, & \text{if } k \geq (p - 1)/2 + 1.
\end{cases}
$$

and $9(p - 1)/16 \leq L_{(p - 1)/4}(v) \leq 3(p - 1)/4 + 1$, $(p - 1)/4 \leq L_k(v) \leq (p - 1)/2$ if $(p - 1)/3 \leq k < (p - 1)/2$.

The following statements we also obtain by [2] or by Lemma 3 from [6].

**Lemma 1.**
1. $S_n(x) = -1/4 + (x - 1)^{(p-1)/4} E_n(x)$ and $E_n(1) \neq 0, n = 0, 1, 2, 3$;
2. $S_n(x) = -1/4 + (x + 1)^{(p-1)/4} F_n(x)$ and $F_n(-1) \neq 0, n = 0, 1, 2, 3$;
3. Let $S_l(x) + S_m(x) + g(x) \equiv 0 \pmod{(x - 1)^{(p-1)/4+1}}$ and $|l - m| \neq 2$. Then $w(g(x)) \geq (p - 1)/4$.

Let us introduce the auxiliary polynomial $R(x) = \sum_{i=0}^{p} c_i S_i(x), c_i \in \mathbb{Z}$. Denote a formal derivative of order $n$ of the polynomial $R(x)$ by $R^{(n)}(x)$.

**Lemma 2.** Let $R^{(n)}(x)|_{x=\pm 1} = 0$ if $0 \leq n \leq (p-1)/4$. Then $R^{(n)}(x)|_{x=\pm 1} = 0$ for $(p - 1)/4 + 1 < n < (p - 1)/2$. 


The exact values of the $k$-error linear complexity of $u$ for $1 \leq k < (p-1)/4$

In this section we obtain the upper and lower bounds of the $k$-error linear complexity and determine the exact values for the $k$-error linear complexity $L_k(u), 1 \leq k < (p-1)/4$.

First of all, we consider the case $k = 1$. Our first contribution in this paper is the following.

**Lemma 3.** Let $\{u_i\}$ be defined by (1) for $p > 5$. Then $L_1(u) = (7p+1)/4$.

**Proof.** Since $L_1(u) \leq L(u)$ and $L(u) = (7p+1)/4$ [2], it follows that $L_1(u) \leq (7p+1)/4$. Assume that $L_1(u) < L(u)$. Then there exists $f(x) = ax^b, a \neq 0$ such that $S_u(x) + ax^b \equiv 0 \pmod{(x-1)^{m_0}(x+1)^{m_1})}$ for $m_0 + m_1 > (p-1)/4$. By (4) the last comparison is impossible for $p \neq 5$.  

If $p = 5$ then $L_1(u) = 8$.

**Lemma 4.** Let $\{u_i\}, \{q_i\}, \{v_i\}$ be defined by (1) and (3), respectively. Then $L_k(q) + L_k(v) \leq L_k(u)$.

**Proof.** Suppose $S_u(x) + f(x) \equiv 0 \pmod{(x-1)^{m_0}(x+1)^{m_1})}$, $w(f) \leq k$ and $m_0 + m_1 = 2p - L_k(u)$. Combining this with (4) and (6) we get $S_u(x) + f(x) \equiv 0 \pmod{(x-1)^{m_0})}$ and $S_l(x) - S_m(x) + 1 + f(x) \equiv 0 \pmod{(x+1)^{m_1})}$ or $S_m(x) - S_l(x) - 1 + f(-x) \equiv 0 \pmod{(x-1)^{m_1})}$ Hence $m_0 \leq p - L_k(q)$ and $m_1 \leq p - L_k(v)$. This completes the proof of Lemma 4.  

This lemma can also be proved using Lemma 2 and 3 from [6].
Lemma 5. Let \( \{u_i\} \) be defined by (1) and \( k \geq 2 \). Then \( L_k(u) \leq 3(p - 1)/4 + 1 + L_{k-2}(q) \).

Proof. From our definition it follows that there exists \( h(x) \) such that \( S_q(x) + h(x) \equiv 0 \pmod{(x - 1)^{p - L_{k-2}(q)}} \), \( w(h) \leq k - 2 \). Then, by Lemma \( \text{Lem} \) \( h(x) \equiv 0 \pmod{(x - 1)^{(p - 1)/4}} \). Let \( h(x) = \sum h_i x^{a_i} \). We consider \( f(x) = \sum f_i x^{b_i} \) where

\[
b_i = \begin{cases} a_i, & \text{if } a_i \text{ is an even,} \\ a_i + p, & \text{if } a_i \text{ is an odd.} \end{cases}
\]

By definition \( f(x) \equiv h(x) \pmod{(x - 1)^p} \), hence \( S_q(x) + f(x) \equiv 0 \pmod{(x - 1)^{p - L_{k-2}(q)}} \). Further, since \( h(x) \equiv 0 \pmod{(x - 1)^{(p - 1)/4}} \) and \( f(x) = f(-x) \), it follows that \( f(x) \equiv 0 \pmod{(x - 1)^{p - 1/4}} \).

Using (3), we obtain that \( S_u(x) + (x^p - 1)/2 + f(x) \equiv (x^p - 1)(S_j(x) + S_m(x) + 1/2) + S_q(x) + f(x) \pmod{(x^2 - 1)^p} \). From this by Lemma \( \text{Lem} \) we can establish that \( S_u(x) + (x^p - 1)/2 + f(x) \equiv 0 \pmod{(x - 1)^{p - L_{k-2}(q)}(x + 1)^{(p - 1)/4}} \).

The conclusion of this lemma then follows from (2). \( \square \)

Theorem 6. Let \( \{u_i\} \) be defined by (1) and \( 2 \leq k < (p - 1)/4 \). Then \( L_k(u) = 3(p - 1)/2 + 2 \).

Proof. By Lemmas 3 and 4 it follows that \( L_k(v) + L_k(q) \leq L_k(u) \leq 3(p - 1)/4 + 1 + L_{k-2}(q) \). To conclude the proof, it remains to note that \( L_k(v) = L_k(q) = L_{k-2}(q) = 3(p - 1)/4 + 1 \) for \( 2 \leq k < (p - 1)/4 \) by (7), (8). \( \square \)

4 The estimates of \( k \)-error linear complexity

In this section we determine the exact values of the \( k \)-error linear complexity of \( u \) for \( (p - 1)/4 + 2 \leq k < (p - 1)/3 \) and we obtain the estimates for the other values of \( k \). Farther, we consider two cases.

4.1 Let \((m, j, l) = (0, 1, 3), (0, 2, 3), (1, 2, 0), (1, 3, 0)\)

Lemma 7. Let \( \{u_i\} \) be defined by (1). Then \( 21(p - 1)/16 + 1 \leq L_{(p - 1)/4}(u) \leq 3(p - 1)/2 + 2 \) and \( p + 1 \leq L_{(p - 1)/4+1}(u) \leq 3(p - 1)/2 + 2 \) for \( p > 5 \).

The statement of this lemma follows from Lemmas 4, 5 and (7), (8).

Theorem 8. Let \( \{u_i\} \) be defined by (1) for \((m, j, l) = (0, 1, 3), (0, 2, 3), (1, 2, 0), (1, 3, 0)\) and \((p - 1)/4 + 2 \leq k < (p - 1)/3 \). Then \( L_k(u) = p + 1 \).
Proof. We consider the case when \((m, j, l) = (0, 1, 3)\). Let \(f(x) = x^p/2 - (\rho + 3)/4 - (\rho + 1)x^pS_0(x)\) where \(\rho = \theta^{(p-1)/4}\) is a primitive 4-th root of unity modulo \(p\). Then \(w(f) = 2 + (p - 1)/4\). Denote \(S_u(x) + f(x)\) by \(h(x)\). Under the conditions of this theorem we have

\[
h(x) = (x^p + 1)S_1(x) + x^pS_0(x) + S_3(x) + 1 + x^p/2 - (\rho + 3)/4 - (\rho + 1)x^pS_0(x).
\]

Hence \(h(1) = 0\). Let \(h^{(n)}(x)\) be a formal derivative of order \(n\) of the polynomial \(h(x)\). By Lemmas \(2\) and \(3\) from \([6]\) we have that \(h^{(n)}(1) = 0\) if \(1 \leq n < (p - 1)/4\) and by Lemma \(3\) from \([6]\) \(h^{(p-1)/4}(1) = (2p + 1 + \rho^3 - (\rho + 1)) (p - 1)/4 = 0\). Hence, by Lemma \(2\) \(h^{(n)}(1) = 0\) if \((p - 1)/4 < n < (p - 1)/2\) and \(h(x) \equiv 0 (\mod (x - 1)^{(p-1)/2})\).

Further, \(h(-1) = -1/4 + 1/4 + 1 - 1/2 - (\rho + 3)/4 + (\rho + 1)/4 = 0\) and \(h^{(p-1)/4}(-1) = (-1 + \rho^3 + (\rho + 1)) (p - 1)/4 = 0\). So, by Lemma \(2\) \(h^{(n)}(1) = 0\) if \(1 < n < (p - 1)/2\) and \(h(x) \equiv 0 (\mod (x + 1)^{(p-1)/2})\). Therefore, by \(2\) we see that \(L_{(p-1)/4+2} \leq p + 1\). On the other hand, by Lemma \(1\) \(L_k(u) \geq L_k(v) + L_k(q)\). To conclude the proof, it remains to note that \(L_k(v) + L_k(q) = p + 1\) for \((p - 1)/4 + 2 < k < (p - 1)/3\) by \([7]\), \([8]\). The other cases may be considered similarly.

Farther, if \((p - 1)/3 \leq k < (p - 1)/2\) then by Lemmas \(1\) Theorem \(8\) and \([7]\), \([8]\) we have that \((p - 1)/2 + 1 \leq L_k(u) \leq p + 1\). It is simple to prove that \(L_{(p-1)/2+2}(u) \leq (p - 1)/2 + 2\).

### 4.2 Let \((m, j, l) = (0, 1, 2), (0, 3, 2), (1, 0, 3), (1, 2, 3)\)

Similarly as in subsection \(1.1\) we have that \(21(p - 1)/16 + 1 \leq L_{(p-1)/4}(u) \leq 3(p - 1)/2 + 2\).

**Theorem 9.** Let \(\{u_i\}\) be defined by \(1\) for \((m, j, l) = (0, 1, 2), (0, 3, 2), (1, 0, 3), (1, 2, 3)\) and \((p - 1)/4 + 1 \leq k < (p - 1)/3\) then \(L_k(u) = 5(p - 1)/4 + 2\).

**Proof.** We consider the case when \((m, j, l) = (0, 1, 2)\). Let here \(f(x) = -1/2 - 2S_2(x)\) and \(h(x) = S_u(x) + f(x)\). Since \((m, j, l) = (0, 1, 2)\) it follows that

\[
h(x) = (x^p + 1)S_1(x) + x^pS_0(x) + S_2(x) + 1 - 1/2 - 2S_2(x).
\]

Hence \(h(1) = 0\). By Lemma \(2\) from \([6]\) we have that \(h^{(n)}(1) = 0\) if \(1 \leq n < (p - 1)/4\). Hence \(h(x) \equiv 0 (\mod (x - 1)^{(p-1)/4})\).
Further, \( h(-1) = 0 \) and \( h^{(p-1)/4}(-1) = (-1 + \rho^2 - 2\rho^2)(p - 1)/4 = 0 \). So, \( h^{(n)}(-1) = 0 \) if \( 1 < n < (p - 1)/2 \) and \( h(x) \equiv 0 \pmod{(x + 1)^{(p-1)/2}} \). Therefore, by (2) we see that \( L_{(p-1)/4+2} \leq 2p - 3(p - 1)/4 \).

Suppose \( L_{(p-1)/4+2} < 2p - 3(p - 1)/4 \); then by (2) there exist \( m_0, m_1 \) such that \( m_0 + m_1 > 3(p - 1)/4 \) and \( S_u(x) + f(x) \equiv 0 \pmod{(x - 1)^{m_0}(x + 1)^{m_1}} \), \( w(f) \leq k < (p - 1)/3 \).

We consider two cases.

(i) Let \( m_0 \leq (p - 1)/4 \) or \( m_1 \leq (p - 1)/4 \). Then \( m_1 > (p - 1)/2 \) or \( m_0 > (p - 1)/2 \) and by (1) and (3) we obtain \( L_k(q) < (p + 1)/2 \) or \( L_k(v) < (p + 1)/2 \). This is impossible for \( k < (p - 1)/3 \) by (7) or (8).

(ii) Let \( \min(m_0,m_1) > (p - 1)/4 \). We can write that \( f(x) = f_0(x^2) + x f_1(x^2) \). Therefore, since \( 2S_1(x) + S_0(x) + S_2(x) + 1 + f(x) \equiv 0 \pmod{(x - 1)^{m_0}} \) and \( S_2(x) - S_0(x) + 1 + f(x) \equiv 0 \pmod{(x + 1)^{m_1}} \) or \( -S_2(x) + S_0(x) + 1 + f_0(x^2) - x f_1(x^2) \equiv 0 \pmod{(x - 1)^{m_1}} \) we see that \( S_1(x) + S_0(x) + 1 + f_0(x^2) \equiv 0 \pmod{(x - 1)^{\min(m_0,m_1)}} \). Hence, \( w(f_0) \geq (p - 1)/4 \) by Lemma (1).

Similarly, \( -2S_1(x) - S_0(x) - S_2(x) + 1 + f_0(x^2) - x f_1(x^2) \equiv 0 \pmod{(x + 1)^{m_1}} \) and \( S_2(x) - S_0(x) + 1 + f_0(x^2) + x f_1(x^2) \equiv 0 \pmod{(x + 1)^{m_1}} \) so \( S_1(x) + S_2(x) + 1 + x f_1(x^2) \equiv 0 \pmod{(x - 1)^{\min(m_0,m_1)}} \). Hence, \( w(f_1) \geq (p - 1)/4 \) by Lemma (1). This contradicts the fact that \( w(f) < (p - 1)/3 \).

Similarly, if \( (p - 1)/3 \leq k < (p - 1)/2 \) then by Lemmas (4) Theorem (8) and (7), (8) we have that \( (p - 1)/2 + 1 \leq L_k(u) \leq 2p - 3(p - 1)/4 \). Here \( L_{(p-1)/2+2}(u) \leq 3(p - 1)/4 + 2 \).

In the conclusion of this section note that we can improve the estimate of Lemma (5) for \( k \geq (p - 1)/2 + 1 \). With similar arguments as above we obtain the following results for \( u \).

**Lemma 10.** Let \( \{u_i\} \) be defined by (11) and \( k = (p - 1)/2 + f, f \geq 0 \). Then \( L_k(u) \leq L_{\lfloor f/2 \rfloor}(v) + 1 \) where \( \lfloor f/2 \rfloor \) is the integral part of number \( f/2 \).

## 5 Conclusion

We investigated the \( k \)-error linear complexity over \( \mathbb{F}_p \) of sequences of length \( 2p \) with optimal three-level autocorrelation. These balanced sequences are constructed by cyclotomic classes of order four using a method presented by Ding et al. We obtained the upper and lower bounds of \( k \)-error linear complexity and determine the exact values of the \( k \)-error linear complexity \( L_k(u) \) for \( 1 \leq k < (p - 1)/4 \) and \( (p - 1)/4 + 2 \leq k < (p - 1)/3 \).
References

[1] H. Aly, A. Winterhof, On the k-error linear complexity over $F_p$ of Legendre and Sidelnikov sequences, Des. Codes Crypt., 40 (2006), 369–374.

[2] H. Aly, W. Meidl and A. Winterhof, On the k-error linear complexity of cyclotomic sequences, J. Math. Crypt., 1 (2007), 1–14.

[3] T. Cusick, C. Ding and A. Renvall, Stream Ciphers and Number Theory, North-Holland Publishing Co., Amsterdam, 1998.

[4] C. Ding, T. Helleseth and H. Martinsen, New families of binary sequences with optimal three-level autocorrelation, IEEE Trans. Info. Theory, 47 (2001), 428 – 433.

[5] C. Ding, G. Xiao and W. Shan, The Stability Theory of Stream Ciphers, in Lecture Notes in Computer Science 561, Springer-Verlag, Berlin 1991.

[6] V.Edemskiy, A.Palvinskii, The linear complexity of binary sequences of length 2p with optimal three-level autocorrelation, Inf. Process. Lett., 116(2)(2015), 153-156

[7] S.W. Golomb, G. Gong, Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications, Cambridge University Press, 2005.

[8] M. Hall, Combinatorial Theory, Wiley, New York, 1975.

[9] Ireland, M.Rosen, A Classical Introduction to Modern Number Theory, Springer, Berlin,1982.

[10] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, 1983.

[11] J. Zhang, C. Zhao, The linear complexity of a class of binary sequences with period 2p, Appl. Algebra Eng. Commun. Comput., 26(5) (2015), 475–491.

[12] Stamp, C. F. Martin, An algorithm for the k-error linear complexity of binary sequences with period $2^n$, IEEE Trans. Inform. Theory, 39 (1993), 1398–1401.