The Linear Complexity and Autocorrelation of Quaternary Whiteman's Sequences

Vladimir.Edemskiy*<sup>a</sup>

Received 10<sup>th</sup> September 2013, Accepted 21<sup>st</sup> December 2013

Abstract: We found the linear complexity of quaternary sequences of period over the ring. The sequences are based on Whiteman's generalized cyclotomic classes of order four. Also we derived the maximum nontrivial autocorrelation magnitude of the constructed sequences.

Keywords: Linear complexity, Autocorrelation, Cyclotomic classes.

1. Introduction

The linear complexity of a sequence is an important characteristic of its quality. It is defined to be the length of the shortest linear feedback shift register that can generate the sequence. Sequences with high linear complexity and good autocorrelation properties are the useful tools in cryptography and other practical applications (see [2], [10], [12]).

The sequences of period \( pq \) (here \( p \) and \( q \) are distinct odd primes), constructed on Whiteman's generalized cyclotomic classes have been the subject of the research in series of works, take for example binary sequences ([13], [11], [8] and references therein) or \( m \)-phase over simple Galois field ([4]). A general approach to construction and determination of the linear complexity of sequences based on cosets was proposed in [3]; here the linear complexity also was derived over the finite field.

As noted in [7], an alternative approach is to adopt the algorithm described by Reeds and Sloane [11], which performs a similar task to the Berlekamp-Massey algorithm but operates directly with the integers modulo \( m \), i.e., over the finite ring \( \mathbb{Z}_m \). In this paper, we explore the linear complexity over the ring \( \mathbb{Z}_4 \) and periodic autocorrelation function of the quaternary sequences based on Whiteman's generalized cyclotomic classes of order four.

Let \( p \) and \( q \) be distinct odd primes and \( N = pq \). Suppose \( \gcd(p - 1, q - 1) = 4 \) and \( R = (p - 1)(q - 1)/4 \). By Chinese remainder theorem there exists a common primitive root \( g \) of both \( p \) and \( q \). The multiplicative order of \( g \) modulo \( N \) is equal \( R \).

* Novgorod State University /Str. B. St. Petersburgskaya, 41, 173003
Veliky Novgorod, Russia
* Corresponding Author Email: Vladimir.Edemsky@novsu.ru

We define Whiteman's generalized cyclotomic classes analogous to [17]:
\[
H_j = \{ g^l y^j : l = 0, \ldots, R - 1 \}, \quad j = 0, 1, 2, 3,
\]
where \( y = g(\text{mod } p), \quad y = 1(\text{mod } q) \). Define
\[
P = \{ p, 2p, \ldots, (q - 1)p \} \quad \text{and} \quad Q = \{ q, 2q, \ldots, (p - 1)q \}.
\]
Then we get
\[
Z_N^* = \bigcup_{k=0}^{3} H_k \quad \text{and} \quad Z_N = \bigcup_{k=0}^{3} H_k \cup P \cup Q \cup \{0\}.
\]
Let \( Q_0 = Q \cup \{0\} \). Define a quaternary sequence as follows:
\[
u_j = \begin{cases} 
  k, & \text{if } j \text{ mod } N \in H_k, \\
  1, & \text{if } j \text{ mod } N \in P, \\
  3, & \text{if } j \text{ mod } N \in Q_0.
\end{cases}
\]

Such sequences are also called coset sequences [3] or index sequences [6]. Our purpose is to examine the linear complexity and autocorrelation function of \( \{ u_j \} \). Unlike above mentioned studies ([4], [3]), we consider the linear complexity of sequence over the ring \( \mathbb{Z}_4 \), not over the finite field.

2. Linear Complexity

A polynomial \( C(x) = 1 + c_1 x + \ldots + c_m x^m \), \( C(x) \in \mathbb{Z}_4[x] \) is called an associated connection polynomial of periodic sequence \( \{u_j\} \) over \( \mathbb{Z}_4 \), if coefficients \( c_1, c_2, \ldots, c_m \) satisfy
\[
u_j = -c_1 u_{j-1} - c_2 u_{j-2} - \ldots - c_m u_{j-m}, \quad \forall r \geq m.
\]
The linear complexity of periodic sequence \( \{u_j\} \) over \( \mathbb{Z}_4 \) is equal to
\[
L = \min \{ \deg C(x) \} \quad \text{if } C(x) \text{ is an associated connection polynomial of } \{u_j\}.
\]
Also, we can define \( L \) as the degree of the minimal polynomial.

It shown in [16] that \( C(x) \) is an associated connection
polynomial of \( \{ u \} \) if and only if
\[ U(x) = (a^0 + a_1 x + \ldots + a_n x^{n-1}), \quad (2) \]
where \( U(x) = u_0 + u_1 x + \ldots + u_n x^{n-1} \).

Let \( r \) be the order of 2 modulo \( pq \), and let \( R = GF(2^r, 2^s) \) be a Galois ring of characteristic 4. The maximal ideal of the ring \( R \) is \( 2R \) [15]. The group of invertible elements \( R^* = R \setminus 2R \) of the ring \( R \) contains the cyclic subgroup of order \( 2^r-1 \) [15]. Hence, there exists an element \( \alpha \) of order \( pq \) in \( R^* \). Then, by Lemma 1, we have \( \alpha \in S \). And therefore, \( D_{HH} = 1 \).

From the last equalities we can easily deduce the following well-known (see [9] or [4]) assertions:

**Lemma 1** [4]

(i) If \( a \in \mathbb{Z}_N \), then \( \sum_{j \in \mathbb{Z}_N} a^j = 1 \) and \( \sum_{j \in \mathbb{Z}_N} a^j = -\sum_{j \in \mathbb{Z}_N} a^j = 1 \).

(ii) If \( a \in P \), then \( \sum_{j \in \mathbb{Z}_N} a^j = -\sum_{j \in \mathbb{Z}_N} a^j = -1 \).

(iii) If \( a \in Q \), then \( \sum_{j \in \mathbb{Z}_N} a^j = -\sum_{j \in \mathbb{Z}_N} a^j = -1 \).

Then \( T_{\alpha}(x) = S_{\alpha}(x) + S_{\alpha}(x) \) for \( l = 0, 1 \). By Lemma 1 we have
\[ S_{\alpha}(\alpha) + S_{\alpha}(\alpha) + S_{\alpha}(\alpha) = 1, \quad T_{\alpha}(\alpha) + T_{\alpha}(\alpha) = 1 \quad (3) \]

Put, by definition \( S(x) = \sum_{j \in \mathbb{Z}_N} S_{\alpha}(x) \). Then, by Lemma 1 we have \( U(\alpha^k) = S(\alpha^k) + 1 \), if \( a \in \mathbb{Z}_N \).

The next assertion is similar to Lemma 2 [8] for the simple field.

**Lemma 2** [7]

(i) If \( S(\alpha) = S_{\alpha}(\alpha) \), if \( a \in H_{\alpha} \), \( j = 0, 1, 2, 3 \), then \( k = 0, 1, 2, 3 \).

(ii) Indices are counted modulo 4.

(iii) If \( S(\alpha) = S_{\alpha}(\alpha) \), if \( a \in H_{\alpha} \), \( k = 0, 1, 2, 3 \).

*Proof.* (i) If \( a \in H_{\alpha} \), then \( aH_{\alpha} = y^j \), i.e., \( aH_{\alpha} = H_{\alpha+yj} \mod \subset 44 \).

This proves the first assertion.

(ii) By definition \( S(\alpha) = \sum_{j \in \mathbb{Z}_N} S_{\alpha}(\alpha) \), therefore
\[ S(\alpha) = \sum_{j \in \mathbb{Z}_N} S_{\alpha}(\alpha) \quad \text{Hence,} \quad S(\alpha) = S(\alpha) = \sum_{j \in \mathbb{Z}_N} S_{\alpha}(\alpha). \]

Now applying equality (3), we conclude the proof of Lemma 2. So, if \( S(\alpha) = S_{\alpha}(\alpha) \), then \( |S(\alpha) = 0 \) and \( v \in \mathbb{Z}_N \) \), and \( \{ v | U(\alpha) = 0 \text{ and } v \in \mathbb{Z}_N \} = (p-1)(q-1)/4 \) for \( S(\alpha) \in \mathbb{Z}/Z_4 \).

Further, here we have the natural epimorphism of the rings \( R \) and \( \overline{R} = R/2R \). Let \( \overline{b} \) denote the image of the element \( b \in R \) under this epimorphism.

As we already mentioned in the introduction, the linear complexity of these sequences over the simple field was examined in [4]. Since under the epimorphism we have the sequence over the field \( GF(2) \), and by [4] we obtain \( S(\alpha) = T_{\alpha}(\alpha) \in \mathbb{Z}_N \), if and only if \( 2 \in H_{\alpha} \cup H_{\alpha} \). In [8] it was shown that \( 2 \in H_{\alpha} \cup H_{\alpha} \), and if and only if \( p = q = 5 \mod 8 \).

Suppose \( D_{\alpha} = H_{\alpha} \cup H_{\alpha} \), \( l = 0, 1 \). The following statement is a generalization of Theorem 1 from [5].

**Lemma 3** Let \( p = q = 5 \mod 8 \). Then
\[ T_{\alpha}(\alpha)^2 = (0, 0) \cup T_{\alpha}(\alpha) + (0, 1) \cup T_{\alpha}(\alpha), \]
where \( (0, 0) = (D_{\alpha} \cap D_{\alpha}) \) and \( (0, 1) = (D_{\alpha} \cap D_{\alpha}) \) are generalized cyclotomic numbers of order 2.

*Proof.* By the definition of auxiliary polynomial we have
\[ (D_{\alpha}(\alpha))^2 = \sum_{\alpha \in \mathbb{Z}_N} \alpha^{(r-1)/2}, \]
and, to put it another way,
\[ (D_{\alpha}(\alpha))^2 = \sum_{\alpha \in \mathbb{Z}_N} \alpha^{(r-1)/2}. \]

As it is shown in [8], if \( p = q = 5 \mod 8 \) then \( -1 \in D_{\alpha} \). By definition \( D_{\alpha} \) contains \( (q-1)/2 - 1 \) elements \( t \) such that \( t+1 = 0 \mod p \) and \( t \neq -1 \). For every \( t \in \mathbb{Z}_N \), \( \sum_{\alpha \in \mathbb{Z}_N} \alpha^{(r-1)/2} = (q-1)/2 \). Continuing this line of reasoning for \( q \), we get
\[ \sum_{\alpha \in \mathbb{Z}_N} \alpha^{(r-1)/2} = \frac{p-1}{2} - \frac{q-1}{2} \frac{p-1}{2} \]
\[ = \frac{p-1}{2} (q-1) - \frac{p-1}{2} (q-1) = 0. \]

Thus, by (4) we have
\[ T_{\alpha}(\alpha)^2 = (D_{\alpha} \cap D_{\alpha}) + (D_{\alpha} \cap D_{\alpha}) \]

The assertion of Lemma 3 follows from the last equation.

**Lemma 4** [4]

(i) If \( T_{\alpha}(\alpha) = \mathbb{Z}_N \), \( l = 0, 1 \), then \( T_{\alpha}(\alpha) \in \mathbb{Z}_N \). In this case, as we already noted, \( 2 \in H_{\alpha} \cup H_{\alpha} \).

Conversely, let \( 2 \in H_{\alpha} \), then \( p = q = 5 \mod 8 \) [8]. Denote \( T_{\alpha}(\alpha) \) by \( z \). By Lemma 3 and (3) we obtain \( z^2 = (0, 0, 0) \) or \( z^2 = (0, 0, 0) = 0 \).

In the given case \( (0, 0) = (0, 0) \), \( a = (0, 0) \), \( b = (0, 0) \), \( 0 \) [17] and \( p = 5 + 8q \), \( q = 5 + 8q \), \( a, b \in \mathbb{Z}_N \).

Now, we generalize Lemma 3 by using Lemma 4.

**Lemma 5** [10]

Let \( a \in \mathbb{Z}_N \) if and only if \( 2 \in H_{\alpha} \).

*Proof.* First, we note that
\[ S(x) = T_{\alpha}(x) + 2S_{\alpha}(x) + S_{\alpha}(x). \quad (5) \]

Let \( S(x) = \mathbb{Z}_N \). Then \( 2 \in H_{\alpha} \cup H_{\alpha} \) and by Lemma 4 \( T_{\alpha}(\alpha) \in \mathbb{Z}_N \).

Suppose \( 2 \in H_{\alpha} \cup H_{\alpha} \). In this case by Lemma 1 we have
\[ S_{\alpha}(\alpha) + S_{\alpha}(\alpha) = S_{\alpha}(\alpha) + S_{\alpha}(\alpha). \]

Hence, by (3) we obtain in \( \mathbb{R} : \)
\[ S_{\alpha}(\alpha) + S_{\alpha}(\alpha) = S_{\alpha}(\alpha) + S_{\alpha}(\alpha) + 1. \]

Thus, \( S_{\alpha}(\alpha) + S_{\alpha}(\alpha) \in \mathbb{Z}_N \), we get a contradiction.

Let \( 2 \in H_{\alpha} \). Then by Lemma 4 \( T_{\alpha}(\alpha) \in \mathbb{Z}_N \) and by Lemma 5 \( S_{\alpha}(\alpha) + S_{\alpha}(\alpha) \in \mathbb{Z}_N \).

**Remark.** Employing the procedure proposed in [5] and generalized for Whitman’s cyclotomic classes in [8], and using cyclotomic numbers of order four, we can derive the equations for \( S_{\alpha}(\alpha), j = 0, 1, 2, 3 \) and prove Lemma 5 by direct computation.
By the choice of $\alpha$ we have an expansion
\[(x^n - 1)/(x - 1) = \sum_{i=0}^{n-1} x^{-i} \] where $x = e^{2\pi i/n}$ is an imaginary unit. The autocorrelation measures the amount of similarity between the sequence $\{u_j\}$ and a shift of $\{u_j\}$ by $w$ positions. Here we derive the

autocorrelation function by well-known procedure, which is based on cyclotomic numbers (see for example [2]). Consider the complex sequence constructed from sequence of $u_j$, i.e., wherein $a_i = i^n$. Then, the periodic autocorrelation function at shift $w$ of $\{u_j\}$ is given by

$$R(w) = \sum_{j=0}^{q-1} a_{j+w}^\ast,$$  

(6)

where $a_j^\ast$ is the complex conjugate of $a_j$.

Let the difference function be defined as $d_{qj}(C,B) = |C \cap (B + w)|$, where $B + w$ denotes the set $\{w + b : b \in B\}$ and $\ast$ denotes addition modulo $N$.

Let $c_j$ and $b_j$ be the characteristic sequences of $C$ and $B$, respectively, i.e.,

$$c_j = \begin{cases} 1, & \text{if } j \mod N \in C, \\ 0, & \text{otherwise} \end{cases} \quad b_j = \begin{cases} 1, & \text{if } j \mod N \in B, \\ 0, & \text{otherwise} \end{cases}.$$

Then,

$$\sum_{j=0}^{q-1} d_{qj}(C,B) = d_q(C,B).$$  

(7)

Hence, by (6) and (7), we can deduce the autocorrelation function from the difference functions $d_{qj}(H_s,H_t), d_{qj}(H_s,H_t)$ and so on.

To derive difference functions we will need cyclotomic numbers. Recall that the cyclotomic numbers of order 4 in this case are defined as [17] $(i,j) = (l+1) \mod l \mod l$ for all $i, j = 0, 1, 2, 3$.

**Lemma 6.7** If $w \in H_s$, $k = 0, 1, 2, 3$, then $d_{qj}(H_s,H_t) = (k-1) \mod l$ for all $j, l = 0, 1, 2, 3$.

**Proof.** Since $|H_s \cap (H_s + w)| = |w^4 H_s \cap (w^4 H_s + 1)|$ and $w^4 H_s \cap (w^4 H_s + 1)$, then $d_{qj}(H_s,H_t) = (l-k) \mod l$. By [17] $(m,n) = (m-n,m)$ and Lemma 6 is proved.

**Lemma 7.8** If $w \in H_s$, $k = 0, 1, 2, 3$, and $j = 0, 1, 2, 3$, then

1) $d_{qj}(P,H_s) = \begin{cases} (q-5)/4, & \text{if } j = k \text{ and } p = q = 5 \mod 8 \\ (q-1)/4, & \text{otherwise} \end{cases}$

2) $d_{qj}(H_s,P) = \begin{cases} (q-5)/4, & \text{if } j = k, \\ (q-1)/4, & \text{otherwise} \end{cases}$

3) $d_{qj}(Q_s,H_t) = d_{qj}(H_s,Q_t) = (q-1)/4.$

4) $d_{qj}(Q_s,P) = d_{qj}(P,Q_t) = 1.$

**Proof.** Note that $-1 \in H_s$ for $p = q = 5 \mod 8$ and $-1 \in H_s$ for $p = q = 4 \mod 8$ (see [8], Lemma 3.3). Then $-w \in H_s$ if $p = q = 5 \mod 8$ and $-w \in H_s$, if $p = q = 4 \mod 8$.

Therefore, $0 \in (H_s + w)$, if $k = j$ and $p = q = 5 \mod 8$ or $j = k + 2 \mod 4$ and $p = q = 4 \mod 8$.

Now, if $u \in H_s$ and $w \in H_s$, then $u = g^w \cdot w = g^{w+1}$, $0 \leq a, b \leq K-1$. Hence, we have $u + w = g^w + g^{w+1}$ (mod $p$). Consequently, $u + w = 0$ (mod $p$) if

**3. Autocorrelation**

The autocorrelation of an $N$-periodic sequence $\{u_j\}$ over $\mathbb{Z}_N$ is the complex-valued function defined by $R(w) = \sum_{j=0}^{N-1} u_{j+w}^\ast u_j$, where $i = \sqrt{-1}$ is an imaginary unit. The autocorrelation measures the amount of similarity between the sequence $\{u_j\}$ and a shift of $\{u_j\}$ by $w$ positions. Here we derive the
and only if \( a + j - b - k = (p - 1)/2 \pmod{(p - 1)} \). Whence \( 0 \leq a \leq \beta - 1 \), then the last congruence has \((q - 1)/4\) solutions. The case \( u + v = 0 \) was investigated in the beginning of the proof. The first assertion of Lemma 7 is proved. The proof of the rest is similar.

The following Lemma was proved in [17].

**Lemma 8.9** [17] If \( w \in P \cup Q \) then
\[
\begin{align*}
\delta_w(H_n,H_n) = & \begin{cases}
(p-1)(q-1)/16, & \text{if } j \neq l, \\
(p-1)(q-5)/16, & \text{if } j = l \text{ and } w \in P, \\
(p-5)(q-5)/16, & \text{if } j = l \text{ and } w \in Q.
\end{cases}
\end{align*}
\]

Lemmas 9 and 10 are proved similar to Lemma 8.

**Lemma 8.10**[f] \( w \in P \) then
1) \( \delta_w(H,P) = \delta_w(H,P) = 0 \) for all \( j = 0,1,2,3 \),
2) \( \delta_w(H,Q) = \delta_w(H,Q) = (p-1)/4 \),
3) \( \delta_w(P,P) = q - 2 \),
4) \( \delta_w(Q,P) = \delta_w(Q,P) = 1 \).

**Lemma 8.11**[f] \( w \in P \) then
1) \( \delta_w(Q,H) = \delta_w(Q,H) = 0 \) for all \( j = 0,1,2,3 \),
2) \( \delta_w(Q,P) = \delta_w(Q,P) = (q-1)/4 \),
3) \( \delta_w(Q,Q) = q \),
4) \( \delta_w(Q,P) = \delta_w(Q,P) = 0 \).

Now we will prove the main theorem of this section.

**Theorem 2.21**Let the sequence \( \{u_j\} \) be defined by (1). (i) if \( p = q + 4 \pmod{8} \) then
\[
R(w) = \begin{cases}
pq, & \text{if } w = 0, \\
-1+2i, & \text{if } w \in H_0, \\
-1, & \text{if } w \in H_1, \\
-p+q-3, & \text{if } w \in P, \\
p+q+1, & \text{if } w \in Q.
\end{cases}
\]
(ii) if \( p = q + 5 \pmod{8} \) then
\[
R(w) = \begin{cases}
pq, & \text{if } w = 0, \\
-1, & \text{if } w \in H_0 \cup H_1, \\
-3, & \text{if } w \in H_2, \\
1, & \text{if } w \in H_3, \\
p+q+3, & \text{if } w \in P, \\
p+q-3, & \text{if } w \in Q.
\end{cases}
\]

**Proof.** By (6) and (7) from (1) we have the following equations for real \( \text{Re}(R(w)) \) and imaginary \( \text{Im}(R(w)) \) parts of the autocorrelation function \( R(w) \):
\[
\begin{align*}
\text{Re}(R(w)) = & \delta_w(H_0,H_0) + \delta_w(H_1 \cup P,H_1 \cup P) + \delta_w(H_2,H_2) \\
& + \delta_w(H_3,\cup Q_0,H_3 \cup Q_0) - \delta_w(H_0,H_0) - \delta_w(H_2,H_2) \\
& - \delta_w(H_3, \cup Q_0,H_3 \cup Q_0) - \delta_w(H_1,\cup Q_0,H_1 \cup P),
\end{align*}
\]
and
\[
\begin{align*}
\text{Im}(R(w)) = & \delta_w(H_0,H_0) + \delta_w(H_1 \cup P,H_1 \cup Q_0) + \delta_w(H_2,H_2) \\
& + \delta_w(H_3,\cup P,H_3 \cup Q_0) - \delta_w(H_0,H_0) - \delta_w(H_2,H_2) \\
& - \delta_w(H_3, \cup P,H_3 \cup Q_0) - \delta_w(H_1,\cup P,H_1 \cup Q_0).
\end{align*}
\]
We consider few cases.

1) Let \( w \in H_0, k = 0,1,2,3 \). By Lemma 7 in this variant we obtain \( \delta_w(H_0,Q_0) + \delta_w(Q_0,H_0) - \delta_w(H_0,Q_0) - \delta_w(Q_0,H_0) = 0 \) and
\[
\begin{align*}
\delta_w(H_0,P) + \delta_w(Q_0,P) - & \delta_w(H_0,P) - \delta_w(Q_0,P) = \\
0, & \text{if } p = q + 4 \pmod{8}, \\
& \text{or } k = 0,2 \text{ and } p = q = 5 \pmod{8}, \\
-2, & \text{if } k = 1 \text{ and } p = q = 5 \pmod{8}, \\
2, & \text{if } k = 3 \text{ and } p = q = 5 \pmod{8}.
\end{align*}
\]
Hence, by Lemma 6 we have from (8)
\[
\text{Im}(R(w)) = \begin{cases}
0, & \text{if } p = q + 4 \pmod{8} \\
& \text{or } k = 0,2 \text{ and } p = q = 5 \pmod{8}, \\
-3, & \text{if } k = 1 \text{ and } p = q = 5 \pmod{8}, \\
1, & \text{if } k = 3 \text{ and } p = q = 5 \pmod{8}.
\end{cases}
\]
Similarly we obtain from (9) that the imaginary part of \( R(w) \) is equal
\[
\text{Im}(R(w)) = \begin{cases}
2, & \text{if } w \in H_0, \\
-2, & \text{if } w \in H_2, \\
0, & \text{if } w \in H_1 \cup H_3.
\end{cases}
\]

2) Let \( w \in P \). As above, by Lemmas 8, 9 and 10 we have
\[
\text{Im}(R(w)) = \begin{cases}
4(\frac{(p-1)(q-5)}{16} - \frac{(p-1)(q-1)}{16}), & \text{if } q - 2 - 2 = p + q - 3 \\
0, & \text{if } w \in H_0 \cup H_1 \cup H_2.
\end{cases}
\]
3) Let \( w \in Q \). Here \( R(w) = p - q + 1 \). Theorem 2 is proved.

**Conclusion**

In this paper we showed that the quaternary sequences based on Whitman’s generalized cyclotomic classes of order four have high linear complexity over \( Z_4 \). We derived the periodic autocorrelation function of these sequences. The examined sequences have satisfactory autocorrelation properties if \( p \) and \( q \) are close. Large linear complexity and small autocorrelation are desirable features for sequences used in applications like cryptology and other.
References


