International Journal of
Applied Mathematics,
Electronics and Computers
ISSN:2147-8228 www.atscience.org/IJAMEC
Advanced Technology and Science
Original Research Paper

The Linear Complexity and Autocorrelation of Quaternary Whiteman's Sequences

Vladimir.Edemskiy[*,a]

Received 10th September 2013, Accepted 21th 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 reminder theorem there exists a common primitive root g of both p and q. The multiplicative order of g modulo N is equal R.

[a] *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]:

$$H_j = \{g^l y^j : l = 0,\dots,R-1\}, \quad j = 0,1,2,3,$$

where $y : y \equiv g \pmod p$, $y \equiv 1 \pmod q$. Define $P = \{p, 2p, \dots, (q-1)p\}$ and $Q = \{q, 2q, \dots, (p-1)q\}$. 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:

$$u_j = \begin{cases} k, & \text{if } j \bmod N \in H_k, \\ 1, & \text{if } j \bmod N \in P, \\ 3, & \text{if } j \bmod N \in Q_0. \end{cases} \tag{1}$$

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 $C(x) = 1 + c_1 x + \dots + c_m x^m$, $C(x) \in \mathbb{Z}_4[x]$ is called an associated connection polynomial of periodic sequence $\{u_j\}$ over $\mathbb{Z}_4$, if coefficients $c_1, c_2, \dots, c_m$ satisfy $u_t = -c_1 u_{t-1} - c_2 u_{t-2} - \dots - c_m u_{t-m}, \forall t \ge m$. The linear complexity of periodic sequence $\{u_i\}$ over $\mathbb{Z}_4$ is equal to $L = \min\{\deg C(x) \mid C(x)$ 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 $\{u_j\}$ if and only if

$$U(x)C(x) \equiv 0 \left(\mathrm{mod}(x^N - 1)\right), \quad (2)$$

where $U(x) = u_0 + u_1 x + ... + u_{N-1} x^{N-1}$.

Let r be the order of 2 modulo pq, and let $R = GF(2^{2r}, 2^2)$ 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 α of order pq in R^*. Then, $1 + \alpha + \alpha^2 + \ldots + \alpha^{pq-1} = 0$ and

$$1 + \alpha^q + \alpha^{2q} + \ldots + \alpha^{(p-1)q} = 0, \; 1 + \alpha^p + \alpha^{2p} + \ldots + \alpha^{(q-1)p} = 0.$$

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

Lemma 1.1[4]

(i) If $a \in \mathbb{Z}_N^*$, then $\sum_{j \in \mathbb{Z}_N^*} \alpha^{ja} = 1$ and $\sum_{j \in P} \alpha^{ja} = \sum_{j \in P} \alpha^{ja} = -1$,

(ii) If $a \in P$, then $\sum_{j \in H_k} \alpha^{ja} = -(p-1)/4$ and $\sum_{j \in P} \alpha^{ja} = -1$,

(iii) If $a \in Q$, then $\sum_{j \in H_k} \alpha^{ja} = -(q-1)/4$ and $\sum_{j \in Q} \alpha^{ja} = -1$.

Here we introduce auxiliary polynomials $S_j(x) = \sum_{f \in H_j} x^f$, $j = 0,1,2,3$ and $T_l = \sum_{h \in H_l \cup H_{l+2}} x^h$, $l = 0,1$.

Then $T_l(x) = S_l(x) + S_{l+2}(x)$ for $l = 0,1$. By Lemma 1 we have

$$S_0(\alpha) + S_1(\alpha) + S_2(\alpha) + S_3(\alpha) = 1, \; T_0(\alpha) + T_1(\alpha) = 1 \quad (3)$$

Put, by definition $S(x) = \sum_{j=0}^{3} j S_j(x)$. Then, by Lemma 1 we have $U(\alpha^a) = S(\alpha^a) + 1$, if $a \in \mathbb{Z}_{pq}^*$.

The next assertion is similar to Lemma 6 from [4] for the simple field.

Lemma 2.2

(i) $S_j(\alpha^a) = S_{j+k}(\alpha)$, if $a \in H_k$, $j = 0,1,2,3$; $k = 0,1,2,3$.

Indices are counted modulo 4.

(ii) $S(\alpha^a) = S(\alpha) - k$, if $a \in H_k$, $k = 0,1,2,3$.

Proof. (i) If $a \in H_k$, then $aH_k = y^k H_j$, i.e., $aH_k = H_{(j+k) \bmod 4}$.

This proves the first assertion.

(ii) By definition $S(\alpha^a) = \sum_{j=0}^{3} j S_j(\alpha^a)$, therefore $S(\alpha^a) = \sum_{j=0}^{3} j S_{j+k}(\alpha)$. Hence, $S(\alpha^a) = S(\alpha) - k \sum_{j=0}^{3} S_j(\alpha)$.

Now applying equality (3), we conclude the proof of Lemma 2.

So, if $S(\alpha) \notin \mathbb{Z}_4$ then $|\{v \mid U(\alpha^v) = 0 \text{ and } v \in \mathbb{Z}_{pq}^*\}| = 0$, and $|\{v \mid U(\alpha^v) = 0 \text{ and } v \in \mathbb{Z}_{pq}^*\}| = (p-1)(q-1)/4$ for $S(\alpha) \in \mathbb{Z}/4\mathbb{Z}$.

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 $\overline{S(\alpha)} = \overline{T_1(\alpha)} \in \mathbb{Z}_2$ if and only if $2 \in H_0 \cup H_2$. In [8] it was shown that $2 \in H_0 \cup H_2$ if and only if $p \equiv q \equiv 5 (\mathrm{mod}\, 8)$.

Suppose $D_l = H_l \cup H_{l+2}$, $l = 0,1$. The following statement is a generalization of Theorem 1 from [5].

Lemma 3.3 Let $p \equiv q \equiv 5 (\mathrm{mod}\, 8)$. Then

$$(T_0(\alpha))^2 = (0,0)_2 T_0(\alpha) + (0,1)_2 T_1(\alpha),$$

where $(0,0)_2 = |(D_0 + 1) \cap D_0|$ and $(0,1)_2 = |(D_0 + 1) \cap D_1|$ are generalized cyclotomic numbers of order 2.

Proof. By the definition of auxiliary polynomial we have $(T_0(\alpha))^2 = \sum_{w,u \in D_0} \alpha^{w+u}$ or, to put it another way,

$$(D_0(\alpha))^2 = \sum_{u,t \in D_0} \alpha^{u(t+1)}. \quad (4)$$

As it is shown in [8], if $p \equiv q \equiv 5 (\mathrm{mod}\, 8)$ then $-1 \in D_0$. By definition D_0 contains $(q-1)/2 - 1$ elements t such that $t + 1 \equiv 0 (\mathrm{mod}\, p)$ and $t \neq -1$. For every t by Lemma 1 $\sum_{u,t \in D_0} \alpha^{u(t+1)} = -(p-1)/2$. Continuing this line of reasoning for q, we get

$$\sum_{u,t \in D_0, (t+1) \notin \mathbb{Z}_{pq}^*} \alpha^{u(t+1)} = \frac{p-1}{2} \cdot \left(\frac{q-1}{2} - 1 \right) - \frac{q-1}{2} \cdot \left(\frac{p-1}{2} - 1 \right) + \frac{(p-1)(q-1)}{2} = 0.$$

Thus, by (4) we have

$$(T_0(\alpha))^2 = |(D_0 + 1) \cap D_0| \cdot T_0(\alpha) + |(D_0 + 1) \cap D_1| \cdot T_1(\alpha).$$

The assertion of Lemma 3 follows from the last equation.

Lemma 3 allows to determine $T_l(\alpha)$, $l = 0,1$ in R.

Lemma 4.4 $T_l(\alpha) \in \mathbb{Z}_4$, $l = 0,1$ if and only if $2 \in D_0$.

Proof. If $T_l(\alpha) \in \mathbb{Z}_4$, $l = 0,1$ then $\overline{T_l(\alpha)} \in \mathbb{Z}_2$, In this case, as we already noted, $2 \in D_0 = H_0 \cup H_2$ [8].

Conversely, let $2 \in D_0$, then $p \equiv q \equiv 5 (\mathrm{mod}\, 8)$ [8]. Denote $T_0(\alpha)$ by z. By Lemma 3 and (3) we obtain $z^2 = (0,0)_2 z + (0,1)_2 (1 - z)$ or $z^2 - z - (0,0)_2 + 1 = 0$. In the given case $(0,0)_2 = ((p-2)(q-2) + 3)/4$, $(0,1)_2 = (0,0)_2 - 1$ [17] and $p = 5 + 8a$, $q = 5 + 8b$, $a, b \in \mathbb{Z}$. So, $z^2 - z - 2(a + b - 1) = 0$, then $z \in \{0,1\}$, if $a + b \equiv 1 (\mathrm{mod}\, 2)$ or $z \in \{2,3\}$ for $a + b \equiv 0 (\mathrm{mod}\, 2)$.

Now, we generalize Lemma 3 by using Lemma 4.

Lemma 5.5 $S(\alpha) \in \mathbb{Z}_4$ if and only if $2 \in H_0$.

Proof. First, we note that

$$S(x) = T_1(x) + 2(S_2(x) + S_3(x)). \quad (5)$$

Let $S(\alpha) \in \mathbb{Z}_4$. Then $2 \in H_0 \cup H_2$ and by Lemma 4 $T_1(\alpha) \in \mathbb{Z}_4$, consequently $2(S_2(\alpha) + S_3(\alpha)) \in 2\mathbb{Z}_4$.

Suppose $2 \in H_2$. In this case by Lemma 1 we have $S_2(\alpha^2) + S_3(\alpha^2) = S_0(\alpha) + S_1(\alpha)$. Hence, by (3) we obtain in $\overline{R}$:

$$\overline{S_2(\alpha) + S_3(\alpha)}^2 = \overline{S_2(\alpha) + S_3(\alpha)} + 1.$$

Thus, $\overline{S_2(\alpha) + S_3(\alpha)} \notin \mathbb{Z}_2$, we get a contradiction.

Let $2 \in H_0$. Then by Lemma 4 $T_1(\alpha) \in \mathbb{Z}_4$ and by Lemma 1 $\overline{S_2(\alpha) + S_3(\alpha)} \in \mathbb{Z}_2$. Then, by (5) we obtain $S(\alpha) \in \mathbb{Z}_4$.

Remark. Employing the procedure proposed in [5] and generalized for Whiteman's cyclotomic classes in [8], and using cyclotomic numbers of order four, we can derive the equations for $S_j(\alpha)$, $j = 0,1,2,3$ and prove Lemma 5 by direct computation.

By the choice of α we have an expansion $(x^{pq}-1)/(x-1)=\prod_{i=1}^{pq-1}(x-\alpha^i)$ then $pq=\prod_{i=1}^{pq-1}(1-\alpha^i)$. So, $\alpha^j-\alpha^l\in R^*$ when $j,l=0,...,pq-1, j\neq l$. Therefore, if $\alpha^j, j\in J$ are the roots of the polynomial then this polynomial is divisible in R by $\prod_{j\in J}(x-\alpha^j)$.

Theorem 1.6 Let the sequence $\{u_t\}$ be defined by (1). Then

(1) $L=pq-q+1$ if $p\equiv q\equiv 5(\mathrm{mod}\,8)$ and $2\notin H_0$,

(2) $L=pq-(p+3)(q-1)/4$ if $p\equiv q\equiv 5(\mathrm{mod}\,8)$ and $2\in H_0$,

(3) $L=pq-p-q+2$ if $p\equiv 1(\mathrm{mod}\,8)$ and $q\equiv 5(\mathrm{mod}\,8)$,

(4) $L=pq$ if $p\equiv 5(\mathrm{mod}\,8)$ and $q\equiv 1(\mathrm{mod}\,8)$,

Proof. By definition of sequences $\{u_j\}$ and by Lemma 1, in $\mathbb{Z}_4$ we have $U(1)=3$, $U(\alpha^b)=(p-1)/2$, if $b\in P$ and $U(\alpha^b)=(q-1)/2+2$, if $b\in Q$.

Let $p\equiv q\equiv 5(\mathrm{mod}\,8)$ and $2\notin H_0$. Then by Lemma 2 and Lemma $5\,U(\alpha^c)\neq 0$, if $c\in\mathbb{Z}_{pq}^*\cup P\cup\{0\}$ and $U(\alpha^b)=0$, if $b\in Q$.

Suppose $Q(x)=\prod_{j\in Q}(x-\alpha^j)$ and choose $C(x)=\left(x^{pq}-1\right)/Q(x)$. Then all the roots of $x^{pq}-1$ are the roots of $U(x)C(x)$. Hence, by (2) $C(x)$ is an associated connection polynomial of $\{u_j\}$ and $L\le pq-p+1$. If $L\neq pq-p+1$, then there exists another associated connection polynomial $C_1(x)$ of sequence $\{u_j\}$ with degree less than $pq-p+1$. Hence, $C_1(\alpha^v)S(\alpha^v)=0$ for $v=0,1,\ldots,pq-1$. Since $U(\alpha^c)\neq 0$, if $c\in\mathbb{Z}_{pq}^*\cup P\cup\{0\}$, then we obtain that $2C_1(\alpha^v)=0$ for $v\in\mathbb{Z}_{pq}^*\cup P\cup\{0\}$ and $2C_1(x)\neq 0$ by definition of an associated connection polynomial. Thus, $2C_1(x)$ is divisible by $\prod_{j\in\mathbb{Z}_{pq}^*\cup P\cup\{0\}}\left(x-\alpha^j\right)$, which contradicts to the fact that the degree of $2C_1(x)$ is less than $pq-p+1$. Therefore, $L=pq-p+1$. This completes the proof of the first statement of the Theorem 1.

Let $p\equiv q\equiv 5(\mathrm{mod}\,8)$ and $2\in H_0$. Then by Lemma 2 and Lemma 5 there exist $k:\ 0\le k\le 3$ and $U(\alpha^b)=0$, if $b\in H_k\cup Q$ and $U(\alpha^c)\neq 0$, if $c\in(\mathbb{Z}_{pq}^*\setminus H_k)\cup P\cup\{0\}$. Here choose $C(x)=\left(x^{pq}-1\right)/(Q(x)H(x))$, where $H(x)=\prod_{j\in H_k}(x-\alpha^j)$. If $2\in H_0$ then $H(x)\in\mathbb{Z}_4[x]$. Continuing the line of argument as in the first case we obtain $L=pq-(p+3)(q-1)/4$.

The rest two statements of Theorem 1 we prove in the same way.

Theorem 1 shows that the sequences $\{u_j\}$ defined by (1) have high linear complexity over the ring $v\in\mathbb{Z}_4$. Changing the values of $\{u_j\}$ when $j\in P\cup Q_0$ does not substantially influence the process and the result of the analysis.

3. Autocorrelation

The autocorrelation of an N -periodic sequence $\{u_j\}$ over $\mathbb{Z}_4$ is the complex-valued function defined by $R(w)=\sum_{n=0}^{N-1} i^{u_n-u_{n+w}}$, 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 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 $a_j=i^{u_j}$. Then, the periodic autocorrelation function at shift w of $\{u_j\}$ is given by

$$R(w)=\sum_{j=0}^{N-1}a_j a_{j+w}^*, \tag{6}$$

where a_j^* is the complex conjugate of a_j .

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

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

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

Then,

$$\sum_{j=0}^{N-1}c_j b_{j+w}=d_w(C,B). \tag{7}$$

Hence, by (6) and (7), we can deduce the autocorrelation function from the difference functions $d_w(H_0,H_0), d_w(H_1,H_1)$ 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] $(i,j)=|(H_i+1)\cap H_j|$ for all $i,j=0,1,2,3$.

Lemma 6.7 If $w\in H_k, k=0,1,2,3,$ then $d_w(H_j,H_l)=(k-l,j-l)$ for all $j,l=0,1,2,3.$

Proof. Since $|H_j\cap(H_l+w)|=|w^{-1}H_j\cap(w^{-1}H_l+1)|$ and $w^{-1}H_l=H_{(l-k)\bmod 4}$, then $d_w(H_j,H_l)=(l-k,j-k)$. By [17] $(m,n)=(-m,n-m)$, and Lemma 6 is proved.

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

1)

$$d_w(P,H_j)=\begin{cases}(q-5)/4, & \text{if } j=k \text{ and } p\equiv q\equiv 5\,(\mathrm{mod}\,8)\\ & \text{or } j\equiv k+2\,(\mathrm{mod}\,4) \text{ and } p\equiv q+4\,(\mathrm{mod}\,8),\\ (q-1)/4, & \text{otherwise.}\end{cases}$$

2)

$$d_w(H_j,P)=\begin{cases}(q-5)/4, & \text{if } j=k,\\ (q-1)/4, & \text{otherwise.}\end{cases}$$

3) $d_w(Q_0,H_j)=d_w(H_j,Q_0)=(q-1)/4.$

4) $d_w(Q_0,P)=d_w(P,Q_0)=1.$

Proof. Note that $-1\in H_0$ for $p\equiv q\equiv 5\,(\mathrm{mod}\,8)$ and $-1\in H_2$ for $p\equiv q+4\,(\mathrm{mod}\,8)$ (see [8], Lemma 3.3). Then $-w\in H_k$ if $p\equiv q\equiv 5\,(\mathrm{mod}\,8)$ and $-w\in H_{k+2}$ if $p\equiv q+4\,(\mathrm{mod}\,8)$. Therefore, $0\in(H_j+w)$, if $k=j$ and $p\equiv q\equiv 5\,(\mathrm{mod}\,8)$ or $j\equiv k+2\,(\mathrm{mod}\,4)$ and $p\equiv q+4\,(\mathrm{mod}\,8)$.

Now, if $u\in H_j$ and $w\in H_k$, then $u=g^a y^j, w=g^b y^k, 0\le a,b\le R-1.$ Hence, we have $u+w\equiv g^{a+j}+g^{b+k}\,(\mathrm{mod}\,p)$. Consequently, $u+w\equiv 0\,(\mathrm{mod}\,p)$ if

and only if $a+j-b-k \equiv (p-1)/2 \pmod{(p-1)}$. Whence $0 \le a \le R-1$, then the last congruence has $(q-1)/4$ solutions. The case $u+w=0$ 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

$$d_w(H_j,H_l)=\begin{cases}(p-1)(q-1)/16, & \text{if } j \neq l,\\ (p-1)(q-5)/16, & \text{if } j=l \text{ and } w\in P,\\ (p-5)(q-5)/16, & \text{if } j=l \text{ and } w\in Q.\end{cases}$$

Lemmas 9 and 10 are proved similar to Lemma 8.

Lemma 9.10 If $w \in P$ then

1) $d_w(P,H_j)=d_w(H_j,P)=0$ for all $j=0,1,2,3$,

2) $d_w(H_j,Q_0)=d_w(Q_0,H_j)=(p-1)/4$,

3) $d_w(P,P)=q-2$,

4) $d_w(Q_0,P)=d_w(P,Q_0)=1$.

Lemma 10.11 If $w \in Q$ then

1) $d_w(Q_0,H_j)=d_w(H_j,Q_0)=0$ for all $j=0,1,2,3$,

2) $d_w(H_j,P)=d_w(P,H_j)=(q-1)/4$,

3) $d_w(Q_0,Q_0)=p$,

4) $d_w(Q_0,P)=d_w(P,Q_0)=0$.

Now we will prove the main theorem of this section.

Theorem 2.*12*Let the sequence $\{u_j\}$ be defined by (1).

(i) if $p \equiv q+4 \pmod 8$ then

$$R(w)=\begin{cases}pq, & \text{if } w=0,\\ -1+2i, & \text{if } w\in H_0,\\ -1-2i, & \text{if } w\in H_2,\\ -1, & \text{if } w\in H_1\cup H_3,\\ -p+q-3, & \text{if } w\in P,\\ p-q+1, & \text{if } w\in Q.\end{cases}$$

(ii) if $p \equiv q \equiv 5 \pmod 8$ then

$$R(w)=\begin{cases}pq, & \text{if } w=0,\\ -1, & \text{if } w\in H_0\cup H_2,\\ -3, & \text{if } w\in H_1,\\ 1, & \text{if } w\in H_3,\\ -p+q-3, & \text{if } w\in P,\\ p-q+1, & \text{if } w\in Q.\end{cases}$$

Proof. By (6) and (7) from (1) we have the following equations for real $(\mathrm{Re}R(w))$ and imaginary $(\mathrm{Im}R(w))$ parts of the autocorrelation function $R(w)$:

$$\begin{aligned}\mathrm{Re}R(w) &= d_w(H_0,H_0)+d_w(H_1\cup P,H_1\cup P)+d_w(H_2,H_2)\\ &+d_w(H_3\cup Q_0,H_3\cup Q_0)-d_w(H_0,H_2)-d_w(H_2,H_0)\\ &-d_w(H_1\cup P,H_3\cup Q_0)-d_w(H_3\cup Q_0,H_1\cup P),\end{aligned} \quad (8)$$

and

$$\begin{aligned}\mathrm{Im}R(w) &= d_w(H_1\cup P,H_0)+d_w(H_3\cup Q_0,H_2)+d_w(H_0,H_3\cup Q_0)\\ &+d_w(H_2,H_1\cup P)-d_w(H_1\cup P,H_2)-d_w(H_3\cup Q_0,H_0)\\ &-d_w(H_0,H_1\cup P)-d_w(H_2,H_3\cup Q_0)\end{aligned} \quad (9)$$

We consider few cases.

1) Let $w\in H_k, k=0,1,2,3$. By Lemma 7 in this variant we obtain $d_w(H_3,Q_0)+d_w(Q_0,H_3)-d_w(H_1,Q_0)-d_w(Q_0,H_1)=0$, $d_w(P,Q_0)+d_w(Q_0,P)=2$

and

$$d_w(H_1,P)+d_w(P,H_1)-d_w(H_3,P)-d_w(P,H_3)=\begin{cases}0, & \text{if } p\equiv q+4 \pmod 8\\ & \text{or } k=0,2 \text{ and } p\equiv q\equiv 5 \pmod 8,\\ -2, & \text{if } k=1 \text{ and } p\equiv q\equiv 5 \pmod 8,\\ 2, & \text{if } k=3 \text{ and } p\equiv q\equiv 5 \pmod 8.\end{cases}$$

Hence, by Lemma 6 we have from (8)

$$\begin{aligned}\mathrm{Re}R(w) &= (h,0)+(h-1,0)+(h-2,0)+(h-3,0)-(h,2)\\ &-(h-2,2)-(h-1,2)-(h-3,2)-2.\end{aligned}$$

It is shown [17] that

$$\sum_{k=0}^{3}(k,0)-(k,2)=1,$$

hence

$$\mathrm{Re}R(w)=\begin{cases}-1, & \text{if } p\equiv q+4 \pmod 8\\ & \text{or } k=0,2 \text{ and } p\equiv q\equiv 5 \pmod 8,\\ -3, & \text{if } k=1 \text{ and } p\equiv q\equiv 5 \pmod 8,\\ 1, & \text{if } k=3 \text{ and } p\equiv q\equiv 5 \pmod 8.\end{cases}$$

Similarly we obtain from (9) that the imaginary part of $R(w)$ is equal

$$\begin{aligned}\mathrm{Im}R(w) &= \sum_{k=0}^{3}(k,1)-(k,3)+d_w(P,H_0)+d_w(Q_0,H_2)+d_w(H_0,Q_0)\\ &+d_w(H_2,P)-d_w(P,H_2)-d_w(Q_0,H_0)-d_w(H_0,P)-d_w(H_2,Q_0).\end{aligned}$$

Here the difference of cyclotomic numbers equals zero. Therefore, by Lemma 7 we obtain the following: If $p\equiv q+4 \pmod 8$ then $\mathrm{Im}R(w)=\begin{cases}2, & \text{if } w\in H_0,\\ -2, & \text{if } w\in H_2,\\ 0, & \text{if } w\in H_1\cup H_3.\end{cases}$; If $p\equiv q\equiv 5 \pmod 8$ then $\mathrm{Im}R(w)=0$.

2) Let $w\in P$. As above, by Lemmas 8, 9 and 10 we have

$$\mathrm{Re}R(w)=4\left(\frac{(p-1)(q-5)}{16}-\frac{(p-1)(q-1)}{16}\right)+q-2-2=-p+q-3$$

and $\mathrm{Im}R(w)=0$.

3) Let $w\in Q$. Here $R(w)=p-q+1$. Theorem 2 is proved.

Corollary. If $q-p=4$, then $\max_{w\neq 0}|R(w)|=3$. Thus, the autocorrelation properties of examined quaternary sequences are the same as of quaternary sequences of period pq from [14] but our sequences are significantly more well-balanced.

4.Conclusion

In this paper we showed that the quaternary sequences based on Whiteman's generalized cyclotomic classes of order four have high linear complexity over Z4. 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

[1] E. Bai, X. Fu and G. Xiao, "On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}," *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88-A(1), pp. 392-395, 2005.

[2] T. W. Cusick, C. Ding and A. Renvall,*Stream Ciphers and Number Theory*, Elsevier, Amsterdam, 1998.

[3] A. Çeşmelioğluand W. Meidl, "A general approach to construction and determination of the linear complexity of sequences based on cosets. Sequences and Their Applications - SETA 2010", *LNCS*, vol. 6338, pp.125-138, 2010.

[4] Z. Chen and X. Du, "Linear complexity and autocorrelation values of a polyphase generalized cyclotomic sequence of length pq", *Frontiers of Computer Science in China*, vol. 4 (4), pp. 529-535, 2010.

[5] V. A. Edemskii, " On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes," *Discret. Math. Appl.*, vol. 20(1), pp. 75–84, 2010 (Diskretn. Mat. 22(1), 74–82 (2010)).

[6] D. H. Green and P. R. Green, "Polyphase power-residue sequences", *Proc. R. Soc. Lond. A.*, vol. 459, pp. 817—827, 2003.

[7] D. H. Green, "Linear complexity of modulo-m power residue sequences", *IEE Proc., Comput. Digit. Tech.*, vol. 151 (6), pp. 385—390, 2004.

[8] L. Hu, Q. Yue and M. Wang, "The Linear Complexity of Whiteman's Generalized Cyclotomic Sequences of Period $p^{m+1}q^{n+1}$", *IEEE Trans. Info. Theory*, vol. 58 (8), pp. 5534 – 5543, 2012.

[9] W. Meidl, "Remarks on a cyclotomic sequence",*Des. Codes Cryptography*, vol. 51(1), pp. 33-43, 2009.

[10] H. Niederreiter, "Linear complexity and related complexity measures for sequences",ed. T. Johansson, S. Maitra, INDOCRYPT 2003. *LNCS*,vol. 2904, pp. 1–17, 2003.

[11] J. A. Reeds and N. J. A. Sloane, "Shift-register synthesis (modulo m)", *SIAM J. Comput.*, vol. 14, pp. 505-513, 1968.

[12] A. Topuzoğlu and A. Winterhof, "Pseudorandom sequences", ed. A. Garcia, H. Stichtenoth,*Topics in Geometry, Coding Theory and Cryptography, Algebra and Applications*, vol. 6, pp. 135—166, 2007.

[13] T. Yan, X. Du, G. Xiao and X. Huang, "Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k",*Information Sciences*, vol. 179(7), pp.1019—1023, 2009.

[14] Z. Yang and P. Ke, "Construction of quaternary sequences of length *pq* with low autocorrelation", *Cryptography and Communications*, vol. 3 (2), pp. 55-64, 2011.

[15] W. Z. Wan, *Finite Fields and Galois Rings*, Singapore. World Scientific Publisher, 2003.

[16] W. Z. Wan, *Algebra and Coding Theory*, Beijing. Science Press, 1976.

[17] A. L. Whiteman, " A family of diference sets", *Illinois J. Math.*, vol. 6, pp. 107-121, 1962.