Linear complexity of quaternary sequences over $\mathbb{Z}_4$ based on Ding-Helleseth generalized cyclotomic classes

Xina Zhang[1], Xiaoni Du[1], Chenhuang Wu[2]

1. College of Mathematics and Statistics, Northwest Normal University,
Lanzhou, Gansu 730070, P.R. China
ymLdxn@126.com

2. School of Mathematics, Putian University,
Putian, Fujian 351100, P.R. China

August 21, 2018

Abstract

A family of quaternary sequences over $\mathbb{Z}_4$ is defined based on the Ding-Helleseth generalized cyclotomic classes modulo pq for two distinct odd primes p and q. The linear complexity is determined by computing the defining polynomial of the sequences, which is in fact connected with the discrete Fourier transform of the sequences. The results show that the sequences possess large linear complexity and are "good" sequences from the viewpoint of cryptography.

Keywords: Quaternary sequences; Ding-Helleseth generalized cyclotomic classes; defining polynomials: linear complexity; trace representation

1 Introduction

Pseudo-random sequences with sound pseudo-randomness properties have been widely used in modern communication systems and cryptography [12, 13]. Cyclotomic and generalized cyclotomic sequences over finite fields are important pseudorandom sequences in stream ciphers due to their sound pseudo-random cryptographic properties and large linear complexity, such as Legendre sequences, Jacobi sequences, etc. [3–6]. We should mention that most of the generalized cyclotomic sequences are defined over finite fields $\mathbb{F}_2$ or $\mathbb{F}_4$ or $\mathbb{F}_r$ with r an odd prime(see [3–6,8,16], for example). For the quaternary sequences over ring $\mathbb{Z}_4$, most of the studies are focused on the analysis

1

of their autocorrelation [15, 19, 22] and the analysis of the linear complexity [10] are rare, especially for the generalized cyclotomic sequences sequences over ring $\mathbb{Z}_4$.

Very recently, as a generalization of Jacobi sequences, a family of quaternary sequences over $\mathbb{Z}_4$ with period pq was proposed by Edemskiy [9] and Chen [1], respectively. They determined the linear complexity with different methods. In this paper, we will propose a similar kind of quaternary sequences over $\mathbb{Z}_4$ using the Ding-Helleseth generalized cyclotomic classes [7].

For cryptographic applications, the *linear complexity* $L((s_u))$ of a N period sequence (s_u) is an important merit factor [2, 11, 13, 18]. It may be defined as the length of the shortest linear feedback shift register which generates the sequence. The feedback function of this shift register can be deduced from the knowledge of just $2L((s_u))$ consecutive digits of the sequence. Thus, it is reasonable to suggest that "good" sequences have $L((s_u)) > N/2$ from the viewpoint of cryptography [2, 18].

Let p and q be two distinct primes with $\gcd(p-1, q-1) = 4$ and $e = (p-1)(q-1)/4$. By the Chinese Remainder Theorem there exists a common primitive root g of both p and q, and the multiplicative order of g modulo pq is e. There also exists an integer h satisfying $h \equiv g \pmod{p}$ and $h \equiv 1 \pmod{q}$. Define

$$D_i = \{g^{4s+i}h^j \pmod{pq} : 0 \le s < e/4,\ 0 \le j < 4\},\ 0 \le i < 4$$

and thus, the multiplication subgroup of the residue ring $\mathbb{Z}_{pq}$ is $\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{3} D_i$. We note that $h^4 \in D_0$, since otherwise, we write $h^4 \equiv g^{4s+i}h^j \pmod{pq}$ for some $0 \le s < e/4$ and $1 \le i < 4$ and get $g^{e-(4s+i)}h^{4-j} = 1 \in D_i$, a contradiction.

Let $P = \{p, 2p, \ldots, (q-1)p\}$, $Q = \{q, 2q, \ldots, (p-1)q\}$, $R = \{0\}$. Then a quaternary sequences (e_u) over $\mathbb{Z}_4$ of length pq are defined by

$$e_u = \begin{cases} 2, & \text{if } u \pmod{pq} \in Q \cup R, \\ 0, & \text{if } u \pmod{pq} \in P, \\ i, & \text{if } u \pmod{pq} \in D_i, i = 0, 1, 2, 3. \end{cases} \tag{1}$$

In Section 2, we will compute the defining polynomial of (e_u) in (1) first and then determine exact values of the linear complexity. The defining polynomial of (e_u) can also help us to give the trace representation of (e_u), which we mention in Section 3. In the rest of the paper, we always suppose that the subscript of D is performed modulo 4.

2   Main Results and Proof

First we introduce the defining pairs of the sequence (s_u) over $\mathbb{Z}_4$ with odd period T. The group of units of Galois ring $GR(4, 4^r)$ of characteristic 4 with 4^r many elements, is $GR^*(4, 4^r) = G_1 \times G_2$, where G_1 is a cyclic group of order $2^r - 1$ and G_2 is a group

of order 2^r. Note that any $\alpha \in GR(4, 4^r)$ can be uniquely represented as

$$\alpha := \alpha_1 + 2\alpha_2, \ \alpha_1, \alpha_2 \in \mathcal{T}. \tag{2}$$

where $\mathcal{T} = \{0\} \cup G_1$. See [21, Ch. 14] for details on the theory of Galois rings.

Let $T | (2^r - 1)$ and $\alpha \in GR(4, 4^r)$ be a primitive T-th root of unity. By [20], one can see that $s_u = \sum\limits_{0 \leq i < T} \rho_i \alpha^{iu}$, where $\rho_i = \sum\limits_{0 \leq u < T} s_u \alpha^{-iu} \ (0 \leq i < T)$ is the (discrete) Fourier transform (DFT) of (s_u). We call $s_u = G(\alpha^u), u \geq 0$ with $G(X) = \sum\limits_{0 \leq i < T} \rho_i X^i \in GR(4, 4^r)[X]$ the *defining polynomial* of (s_u) corresponding to α [3–5] and $(G(X), \alpha)$ a *defining pair* of (s_u).

Define

$$D_i(X) = \sum_{u \in D_i} X^u \in \mathbb{Z}_4[X]$$

for $i = 0, 1, 2, 3$.

From our construction, one can see that p and q satisfy one of $q \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$ or $q \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 4$ since $\gcd(p-1, q-1) = 4$. Now we present the defining polynomial of the sequences as following.

Theorem 1. *If $q \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$, the defining polynomial $G(X)$ of (e_u) is*

$$G(X) = 2 \sum_{j=0}^{q-1} X^{jp} + \sum_{i=0}^{3} (\rho - i) D_i(X),$$

where $\rho = \sum\limits_{i=1}^{3} i D_i(\beta)$.

Theorem 2. *If $q \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 4$, the defining polynomial $G(X)$ of (e_u) is*

$$G(X) = 2 \sum_{j=0}^{p-1} X^{jq} + 2 \sum_{j=1}^{q-1} X^{jp} + \sum_{i=0}^{3} (\rho + 2 - i) D_i(X),$$

where $\rho = \sum\limits_{i=1}^{3} i D_i(\beta)$.

To prove Theorems 1 and 2, we need some notations and auxiliary lemmas. It is easy to see that

$$u D_i := \{uv \pmod{pq} : v \in D_i\} = D_{i+j}$$

for $u \in D_j$. We note that most of the calculations are performed in the Galois ring $GR(4, 4^\ell)$ with characteristic four.

3

Lemma 1. *Let $\gamma \in GR(4, 4^\ell)$ be a primitive pq-th root of unity, then we have*

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

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

(3). $\displaystyle\sum_{z \in \mathbb{Z}_{pq}^*} \gamma^z = \sum_{i=0}^{3} D_i(\gamma) = 1$.

It is easy to check these results, thus we omit the proof.

Lemma 2. *Let $\gamma \in GR(4, 4^\ell)$ be a primitive pq-th root of unity. For $0 \le i < 4$, we have*

(1). $D_i(\gamma^{kp}) = 0, \ 0 \le k < q$.

(2). $D_i(\gamma^{kq}) = 3(q-1)/4, \ 1 \le k < p$.

Proof. (1). Rewrite $s = \frac{q-1}{4}s_1 + s_2$ with $0 \le s_1 < \frac{p-1}{4}$ and $0 \le s_2 < \frac{q-1}{4}$, so from the definitions of D_i, g and h, we have

$$D_i \pmod{q} = \{1, g^4, \ldots, g^{4((q-1)/4-1)}\} \pmod{q} := D',$$

and each element in D' appears $p - 1$ times. So for $0 \le k < q$ we get by Lemma 1(2)

$$D_i(\gamma^{kp}) = (p-1)\sum_{j \in D'} \gamma^{jkp} = 0.$$

(2) Similarly, we have

$$D_i \pmod{p} = \{1, \ldots, p-1\} = \mathbb{Z}_p^*,$$

and each element of $\mathbb{Z}_p^*$ appears $(q-1)/4$ times. So we can get the desired result by Lemma 1(2). $\qquad\square$

Lemma 3. *Let $0 \le a < 4$ and $w = g^{4x}h^j \in D_0$ for $0 \le x < e/4$ and $0 \le j < 4$.*

(1). *There are exactly $\frac{q-1}{4}$ many solutions w satisfying $g^a + w \equiv 0 \pmod{p}$.*

(2). *There are exactly $p - 1$ many solutions w satisfying $g^a + w \equiv 0 \pmod{q}$ if $4 \mid (a + \frac{q-1}{2})$, and no solution otherwise .*

(3). *There is a solution w satisfying both $g^a + w \equiv 0 \pmod{p}$ and $g^a + w \equiv 0 \pmod{q}$ iff $4 \mid (\frac{p-1}{2} - \frac{q-1}{2} - j)$ and $4 \mid (a + \frac{q-1}{2})$. Such solution is unique modulo $e/4$.*

Proof. (1) Since
$$g^{4x}h^j \equiv -g^a = g^{(p-1)/2+a} \pmod{p},$$

then we have $4x + j \equiv (p-1)/2 + a \pmod{p-1}$ and hence $4x + j = k(p-1) + (p-1)/2 + a$ for all $0 \le k < (q-1)/4$.

(2). Similarly, we have $4x \equiv (q-1)/2 + a \pmod{q-1}$ and hence $4x = k(q-1) + (q-1)/2 + a$ for all $0 \le k < (p-1)/4$ and $0 \le j < 4$.

For (3), we need to consider the equations

$$
\begin{cases}
4x \equiv (p-1)/2 + a - j & (\text{mod } p-1), \\
4x \equiv (q-1)/2 + a & (\text{mod } q-1).
\end{cases}
$$

By [6, Lemma 5] and (2) of this lemma, we get the desired result. $\qquad\square$

Below we will calculate the inner product $\mathcal{C}_i(X) \cdot \mathcal{C}_j(X)^{\mathrm{T}}$ for $0 \le i, j < 4$, here $\mathcal{C}_i(X)^{\mathrm{T}}$ is defined by the transpose of $\mathcal{C}_i(X)$ and

$$
\mathcal{C}_i(X) = (D_i(X), D_{i+1}(X), D_{i+2}(X), D_{i+3}(X)).
$$

Lemma 4. *Let $\beta \in GR(4, 4^\ell)$ be a primitive pq-th root of unity. For any $0 \le i, j < 4$, we have*

$$
\mathcal{C}_i(\beta) \cdot \mathcal{C}_j(\beta)^{\mathrm{T}} + (q-1)/4 = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise,} \end{cases}
$$

if $q \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$, and

$$
\mathcal{C}_i(\beta) \cdot \mathcal{C}_j(\beta)^{\mathrm{T}} + (q-1)/4 = \begin{cases} 1, & \text{if } i \equiv j+2 \pmod 4, \\ 0, & \text{otherwise,} \end{cases}
$$

if $q \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 4$.

Proof. Since $D_i = g^i D_0$ for all $0 \le i < 4$, we have

$$
\begin{aligned}
\mathcal{C}_i(\beta) \cdot \mathcal{C}_j(\beta)^{\mathrm{T}} &= \sum_{k=0}^{3} \sum_{u \in D_0} \beta^{u g^{i+k}} \sum_{v \in D_0} \beta^{v g^{j+k}} \\
&= \sum_{k=0}^{3} \sum_{u \in D_0} \sum_{w \in D_0} \beta^{u g^{j+k}(g^{i-j}+w)} \quad (\text{here } v = uw) \\
&= \sum_{w \in D_0} \sum_{k=0}^{3} \sum_{z \in D_{j+k}} \gamma_w^z = \sum_{w \in D_0} \sum_{k=0}^{3} D_k(\gamma_w),
\end{aligned}
$$

and in the above penultimate equation $z = u g^{j+k}, \gamma_w = \beta^{g^{i-j}+w}$. Now we need to determine $\mathrm{ord}(\gamma_w)$, and we find that the possible values of $\mathrm{ord}(\gamma_w)$ are $1, p, q, pq$. Thus,

$$
\mathcal{C}_i(\beta) \cdot \mathcal{C}_j(\beta)^{\mathrm{T}} = \left(\sum_{\substack{w \in D_0 \\ \mathrm{ord}(\gamma_w)=1}} + \sum_{\substack{w \in D_0 \\ \mathrm{ord}(\gamma_w)=p}} + \sum_{\substack{w \in D_0 \\ \mathrm{ord}(\gamma_w)=q}} + \sum_{\substack{w \in D_0 \\ \mathrm{ord}(\gamma_w)=pq}} \right) \cdot \sum_{k=0}^{3} D_k(\gamma_w)
$$

We first suppose that $q \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$. If $\mathrm{ord}(\gamma_w) = 1$, then $g^{i-j} + w \equiv 0 \pmod{pq}$. By Lemma 3(3), there is unique $w(= g^{4s} h^t) \in D_0$ satisfying it iff $4 | (\frac{p-1}{2} - \frac{q-1}{2} - t)$ and $4 \mid (\frac{q-1}{2} + i - j)$, that is, $t = 2$ and $i = j$.

5

If $\operatorname{ord}(\gamma_w) = p$, then $g^{i-j} + w \equiv 0 \pmod{q}$ but $g^{i-j} + w \not\equiv 0 \pmod{p}$. By Lemma 3(2), there are $p - 2$ many or not any $w \in D_0$ satisfying it depending on whether $i = j$ or not.

Similarly, if $\operatorname{ord}(\gamma_w) = q$, then by Lemma 3(1), there are $\frac{q-1}{4} - 1$ or $\frac{q-1}{4}$ many $w \in D_0$ satisfying it depending on whether $t = 2$ and $i = j$ hold or not.

So the number of $w \in D_0$ satisfying $\operatorname{ord}(\gamma_w) = pq$, is $\frac{(p-1)(q-1)}{4} - (\frac{q-1}{4} - 1) - (p-2) - 1$ or $\frac{(p-1)(q-1)}{4} - \frac{q-1}{4}$ depending on whether $i = j$ or not.

From all the discussion above, we derive

$$\mathcal{C}_i(\beta) \cdot \mathcal{C}_j(\beta)^{\mathrm{T}} + (q-1)/4 = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

For $q \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 4$, one can get the desired result by Lemma 3(3) in a similar way. $\qquad \square$

We are now ready to prove Theorems 1 and 2.

Proof of Theorem 1. If $q \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$, we can check that the defining polynomial $G(X)$ of (e_u) is

$$
\begin{aligned}
G(X) &= 2\sum_{j=0}^{q-1} X^{jp} + \sum_{i=1}^{3} i\left(\mathcal{C}_k(\beta) \cdot \mathcal{C}_0(X)^{\mathrm{T}} + \frac{q-1}{4}\right) \\
&= 2\sum_{j=0}^{q-1} X^{jp} + \sum_{i=1}^{3} i\mathcal{C}_i(\beta) \cdot \mathcal{C}_0(X)^{\mathrm{T}}.
\end{aligned}
$$

In fact, for $u = kp$ with $0 \le k < q$, it follows from Lemma 2 that $\mathcal{C}_0(\beta^{kp}) = (0, 0, 0, 0)$, thus $G(\beta^0) = 2 = e_0$ and $G(\beta^{kp}) = 0 = e_{kp}$ for $k \neq 0$.

Similarly for $u = kq$ with $1 \le k < p$, it follows from Lemma 1(2) that $\mathcal{C}_0(\beta^{kq}) = (\frac{3(q-1)}{4}, \frac{3(q-1)}{4}, \frac{3(q-1)}{4}, \frac{3(q-1)}{4})$, so we have $G(\beta^{kq}) = 2 = e_{kq}$.

For $u \in D_k$ with $0 \le k < 4$, Lemmas 1 and 4 leads to that $G(\beta^u) = k = e_u$.

Hence we get $e_u = G(\beta^u)$ for all $u \ge 0$.

With the above discussion and simple calculation, one can get the desired results from the definition of ρ and Lemma 1(3). $\qquad \square$

Proof of Theorem 2. If $q \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 4$, similar to the proof of Theorem 1, one can check that the defining polynomial $G(X)$ of (e_u) is

$$
\begin{aligned}
G(X) &= 2 + 2\sum_{j=0}^{p-1} X^{jq} + 2\sum_{j=0}^{q-1} X^{jp} + \mathcal{C}_2(\beta) \cdot \mathcal{C}_3(X)^{\mathrm{T}} \\
&\quad + 2\mathcal{C}_2(\beta) \cdot \mathcal{C}_2(X)^{\mathrm{T}} + 3\mathcal{C}_2(\beta) \cdot \mathcal{C}_1(X)^{\mathrm{T}},
\end{aligned}
$$

thus we can get the desired results after simple calculation. $\qquad \square$

Theorems 1 and 2 are essential to the presentation of linear complexity of the sequences. Thus we have

6

Theorem 3. *If* $q \equiv 1$ (mod 8) *and* $p \equiv 5$ (mod 8), *the linear complexity of* (e_u) *is*

$$L((e_u)) = \begin{cases} q + 3(p-1)(q-1)/4, & \text{if } 2 \in D_0, \\ pq - p + 1, & \text{if } 2 \in D_2. \end{cases}$$

Theorem 4. *If* $q \equiv 5$ (mod 8) *and* $p \equiv 1$ (mod 4), *the linear complexity of* (e_u) *is*

$$L((e_u)) = pq.$$

Proof of Theorem 3. According to the work of Udaya and Siddiqi [20, Theorem 4], we have that the linear complexity $L((e_u))$ equals the number of nonzero coefficients of the defining polynomial of (e_u). Then the result can be followed from Lemma 5. $\square$

Below, we let $\bar{b}$ denote the image of the element $b \in GR(4, 4^r)$ under the natural epimorphism of the rings $GR(4, 4^r)$ and $\overline{GR(4, 4^r)} = GR(4, 4^r)/2GR(4, 4^r)$.

Define

$$E(x) = \sum_{i=1}^{3} i D_i(x),$$

then it follows from Lemma 1 and the relations of $\overline{D_l}$ that $\overline{E(\beta^k)} = E(\beta) - l$ for $k \in D_l$ with $l = 0, 1, 2, 3$. Thus we have $\overline{E(\beta^k)} = \overline{D_1(\beta) + D_3(\beta)} \in \mathbb{Z}_2$ iff $2|l$, i.e., $2 \in D_0 \cup D_2$. Moreover, from our selection of p and q, we have that

$$2 \in D_0 \cup D_2 \text{ iff } q \equiv 1 \pmod 8 \text{ and } p \equiv 5 \pmod 8,$$

since 2 is a quadratic residue (non-residue) modulo prime q iff $q \equiv \pm 1$ (mod 8) ($q \equiv \pm 5$ (mod 8)).

Lemma 5. $\rho \in \mathbb{Z}_4$ *iff* $2 \in D_0$.

Proof. Let $H_i = D_i \cup D_{i+2}$ and $H_i(x) = \sum_{j \in H_i} x^j$ for $i = 0, 1$. We will prove the result with the following steps.

We first prove that if $q \equiv 1$ (mod 8), then $(H_0(\beta))^2 = (0,0)H_0(\beta) + (0,1)H_1(\beta)$ with $(0,0) = |(H_0+1) \cap H_0|$ and $(0,1) = |(H_0+1) \cap H_1|$ are the generalized cyclotomic numbers of order 2.

Note that

$$(H_0(\beta))^2 = \sum_{u \in H_0} \sum_{t \in H_0} \beta^{u(t+1)}.$$

We have [14, Proposition 9.8.6] that $-1 \in D_0$ iff $q \equiv 1$ (mod 8). One can see that H_0 contains $(q-1)/2 - 1$ elements such that $t + 1 \equiv 0$ (mod p), and $2(p-1) - 1$ elements such that $t + 1 \equiv 0$ (mod q), respectively, for $t \neq -1$. It follows from Lemma 2 that

$$\sum_{u \in H_0} \sum_{t \in H_0, (t+1, pq) > 1} \beta^{u(t+1)} = \left(\frac{q-3}{2}\right) \cdot 0 + (2p - 3)\frac{3(q-1)}{2} + \frac{(p-1)(q-1)}{2} = 0.$$

Thus, we have $(H_0(\beta))^2 = (0,0)H_0(\beta) + (0,1)H_1(\beta)$.

Second, we prove that $H_i(\beta) \in \mathbb{Z}_4$ for $i = 0, 1$ iff $2 \in D_0 \cup D_2$. If $H_i(\beta) \in \mathbb{Z}_4$, then $\overline{H_i(\beta)} \in \mathbb{Z}_2$ and the discussion immediately above the Lemma leads to $2 \in D_0 \cup D_2$. Meanwhile, if $2 \in D_0 \cup D_2$, then $q \equiv 1 \pmod 8$. Denote $z = H_0(\beta)$, then by Lemma 1 we have $z^2 = (0,2)z + (0,1)(1-z)$, thus we have $z^2 = z$, i.e., $z \in \mathbb{Z}_2$ since $(0,0) = (q-5)(p-2)/4$ and $(0,1) = (q-1)(p-2)/4$ [6].

Finally, rewrite $E(x) = H_1(x) + 2(D_2(x) + D_3(x))$, then if $E(\beta) \in \mathbb{Z}_4$, we have $H_1(\beta) \in \mathbb{Z}_4$ and $2(D_2(\beta) + D_3(\beta)) \in 2\mathbb{Z}_4$. If $2 \in D_2$, then we have $D_2(\beta^2) + D_3(\beta^2) = D_0(\beta) + D_1(\beta)$, thus we have $\overline{D_2(\beta) + D_3(\beta)}^2 = \overline{D_2(\beta) + D_3(\beta)} + 1$, hence $\overline{D_2(\beta) + D_3(\beta)} \notin \mathbb{Z}_2$. A contradiction.

If $2 \in D_0$, we have $H_1(\beta) \in \mathbb{Z}_4$ and $\overline{D_2(\beta) + D_3(\beta)} \in \mathbb{Z}_2$, thus $E(\beta) = \rho \in \mathbb{Z}_4$. $\square$

The proof of Theorem 4 is similar to that of Theorem 3, we omit it here.

Theorems 3 and 4 show that the sequence possess large linear complexity and they are "good" from the view point of cryptography.

3   Final Remarks

It is well known that the trace representation can be computed by applying the (discrete) Fourier transform [17]. Trace functions over Galois rings [19, 20] is extensively applied to producing pseudorandom sequences efficiently and analyzing their pseudorandom properties [13, 15, 20] (see also references therein). The *trace function* $\mathrm{TR}_s^r(-)$ from $GR(4, 4^r)$ to $GR(4, 4^s)$ ($s|r$) is defined by

$$\mathrm{TR}_s^r(\alpha) = \Phi_s^0(\alpha) + \Phi_s(\alpha) + \ldots + \Phi_s^{r/s-1}(\alpha),$$

where $\Phi_s(\alpha) = \alpha_1^{2^s} + 2\alpha_2^{2^s}$ is the *Frobenius automorphism* of $GR(4, 4^r)$ over $GR(4, 4^s)$ with order r/s. For more details on trace functions over Galois rings, we refer the reader to [21].

Below we present the trace representation of (e_u) without proof since the proof is in a similar way as in [1] with the fact that $2 \in D_0 \cup D_2$ iff $q \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$ and $2 \in D_1 \cup D_3$ iff $q \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 4$.

Theorem 5. *Let ℓ be the order of 2 modulo pq, ℓ_p the order of 2 modulo p and ℓ_q the order of 2 modulo q. The trace representation of (e_u) is*
(1) For $q \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$,

$$e_u = 2 + 2 \sum_{i=0}^{\frac{q-1}{\ell_q}-1} \mathrm{TR}_1^{\ell_q}(\beta^{ug^i p}) + \sum_{i=0}^{3}(\rho - i) \sum_{t=0}^{\frac{e}{4\ell/\epsilon}-1} \sum_{j=0}^{3} \mathrm{TR}_\epsilon^\ell(\beta^{ug^{4t+i}h^j}),$$

with $\epsilon = 1$ if $2 \in D_0$ and $\epsilon = 2$ if $2 \in D_2$.

(2) For $q \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 4$,

$$e_u = 2 + 2 \sum_{i=0}^{\frac{p-1}{\ell_p}-1} \mathrm{TR}_1^{\ell_p}(\beta^{ug^i q}) + 2 \sum_{i=0}^{\frac{q-1}{\ell_q}-1} \mathrm{TR}_1^{\ell_q}(\beta^{ug^i p}) + \sum_{i=0}^{3}(\rho + 2 - i) \sum_{t=0}^{\frac{4e}{\ell}-1} \sum_{j=0}^{3} \mathrm{TR}_4^{\ell}(\beta^{ug^{4t+i}h^j}).$$

Acknowledgements

References

[1] Z. Chen, "Linear complexity and trace representation of quaternary sequences over Z_4 based on generalized cyclotomic classes modulo pq," Cryptography and Communications, vol. 9, no. 4, pp. 445-458, 2017.

[2] T. W. Cusick, C. Ding, and A. R. Renvall, Stream Ciphers and Number Theory. Vol. 66, Elsevier, 2004.

[3] Z. Dai, G. Gong and H. Y. Song, "Trace representation and linear complexity of binary e-th residue sequences," Int'l Workshop on Coding and Cryptography-WCC, pp. 121-133, Versailles, France, 2003.

[4] Z. Dai, G. Gong and H. Y. Song, "A trace representation of binary Jacobi sequences," Discrete Mathematics, vol. 309, no. 6, pp. 1517-1527, 2009.

[5] Z. Dai, G. Gong, H. Y. Song and D. Ye, "Trace representation and linear complexity of binary e-th power residue sequences of period p," IEEE Transactions on Information Theory, vol. 57, no. 3, pp. 1530-1547, 2011.

[6] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," Finite Fields and Their Applications, vol. 3, no. 2, pp. 159-174, 1997.

[7] C. Ding, T. Helleseth, "New generalized cyclotomy and its applications," Finite Fields and Their Applications, vol. 4, no. 2, pp. 140-166, 1998.

[8] X. Du, Z. Chen, "Trace representations of generalized cyclotomic sequences of length pq with arbitrary order," Chinese Journal of Electronics, vol. 18, no. 3, pp. 460-464, 2009.

[9] V. Edemskiy, A. Ivanov, "Autocorrelation and linear complexity of quaternary sequences of period $2p$ based on cyclotomic classes of order four," IEEE International Symposium on Information Theory Proceedings (ISIT), pp. 3120-3124, 2013.

[10] V. Edemskiy, A. Ivanov, "Linear complexity of quaternary sequences of length pq with low autocorrelation," Journal of Computational and Applied Mathematics, vol. 259, pp. 555-560, 2014.

[11] J. Gao, Y. Hu, X. Li, "Linear span of the optimal frequency hopping sequences from irreducible cyclic codes," Chinese Journal of Electronics, vol. 24, no. 4, pp. 818-823, 2015.

[12] S. Golomb, Shift Register Sequences. Oakland, CA: Holden-Day, 1967. Revised edition: Laguna Hills, CA: Aegean Park Press, 1982.

[13] S. Golomb, G. Gong, Signal Design for Good Correlation. Cambridge: Cambridge University Press, 2005.

[14] K. Ireland, M. Rosen, An Introduction to Modern Nubmer Theory. Second Edition, Springer, 1990.

[15] Y. Kim, J. Jang, J. Kim, J. No, "New construction of quaternary sequences with ideal autocorrelation from legendre sequences," IEEE International Symposium on Information Theory (ISIT), pp. 282-285, 2009.

[16] D. Li, Q. Wen, J. Zhang, et al., "Linear complexity of generalized cyclotomic quaternary sequences with period pq," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 97, no. 5, pp. 1153-1158, 2014.

[17] J. Massey, "Codes and Ciphers: Fourier and Blahut. Codes, Curves, and Signals," Springer US, pp. 105-119, 1998.

[18] J. A. Reeds and N. J. A. Sloane, "Shift register synthesis (modulo m)," SIAM J. Comput., vol. 14, pp. 505-513, 1985.

[19] P. Udaya, M. U. Siddiqi, "Optimal biphase sequences with large linear complexity derived from sequences over $\mathbb{Z}_4$," IEEE Transactions on Information Theory, vol. 42, no. 1, pp. 206-216, 1996.

[20] P. Udaya, M. U. Siddiqi, "Generalized GMW quadriphase sequences satisfying the Welch bound with equality," Applicable Algebra in Engineering, Communication and Computing, vol. 10, no. 3, pp. 203-225, 2000.

[21] Z. Wan, Finite Fields and Galois Rings. Singapore: World Scientific Publisher, 2003.

[22] Y. Yang, X. H. Tang, "Balanced quaternary sequences pairs of odd period with (almost) optimal autocorrelation and cross-correlation," IEEE Communications Letters, vol. 18, no. 8, pp. 1327-1330, 2014.