IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024EAL2026

Publicized:2024/05/22

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

LETTER

Trace representation of balanced quaternary generalized cyclotomic sequences of period p^n

Feifei YAN[†a)], ***Student Member***, **Pinhui KE**[††b)], ***and*** **Zuling CHANG**[†††c)], ***Nonmembers***

SUMMARY Recently, trace representation of a class of balanced quaternary sequences of period p from the classical cyclotomic classes was given by Yang et al. (Cryptogr. Commun.,**15** (2023): 921–940). In this letter, based on the generalized cyclotomic classes, we define a class of balanced quaternary sequences of period p^n, where $p = ef + 1$ is an odd prime number and satisfies $e \equiv 0 \pmod 4$. Furthermore, we calculate the defining polynomial of these sequences and obtain the formula for determining their trace representations over $\mathbb{Z}_4$, by which the linear complexity of these sequences over $\mathbb{Z}_4$ can be determined.

key words: *Quaternary sequence, generalized cyclotomic classes, trace representation, defining polynomial, Galois ring*

1. Introduction

Pseudo-random sequences are widely used in various fields, such as code division multiple access, stream cryptography, coding theory etc. [1]–[3]. Quaternary sequences with high complexity, low correlation, and balancedness are the preferred sequences in practical applications.

Trace function over the Galois ring can effectively generate quaternary sequences. And the trace representation of quaternary sequences reveals some important properties of the sequences. In 2017, Chen [4] defined a family of quaternary sequences of period pq over $\mathbb{Z}_4$, and given their trace representation by using discrete Fourier transform, from which the linear complexity of the sequence is obtained. Recently, Yang et al. [5] constructed a class of balanced quaternary sequences of period p, and determined their trace representation and linear complexity over $\mathbb{Z}_4$. Except above mentioned results, limited works on the trace representation of quaternary sequences over Galois rings are known.

It is convenient to define quaternary sequences by using the classical and generalized cyclotomic classes [6]–[8]. Inspired by the works in [4], [5], we introduce a general construction of balanced quaternary sequences of period p^n by using generalized cyclotomic classes. And we calculate the trace representation of these sequences over $\mathbb{Z}_4$.

The rest of this letter is organized as follows. In Section 2, we provide some basic concepts and the required lemmas. In Section 3, we define a family of balanced quaternary sequences based on generalized cyclotomic classes, and derive the trace representation and linear complexity of these sequences over $\mathbb{Z}_4$. Section 4 draws the conclusions.

2. Preliminaries

Let $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, and $\mathbb{Z}_m^*$ denote the set of all elements in $\mathbb{Z}_m$ that are coprime with m.

The *Galois ring* of characteristic 4 and cardinality 4^r is denoted by $GR(4, 4^r)$. There exists a nonzero element ξ of order $2^r - 1$ in $GR(4, 4^r)$, which is a root of a basic primitive polynomial of degree r over $\mathbb{Z}_4$. Let $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^r-2}\}$, then any element $c \in GR(4, 4^r)$ can be written uniquely as $c = c_0 + 2c_1$, where $c_0, c_1 \in \mathcal{T}$.

Let d be a positive integer that satisfies $d|r$. Then $GR(4, 4^r)$ contains $GR(4, 4^d)$ as a subring. Define a map ϕ:

$$\phi : GR(4, 4^r) \to GR(4, 4^d)$$

$$c = c_0 + 2c_1 \mapsto c_0^{2^d} + 2c_1^{2^d}, \quad c_0, c_1 \in \mathcal{T}.$$

Then ϕ is an automorphisms of $GR(4, 4^r)$ leaving $GR(4, 4^d)$ fixed elementwise. And ϕ is called the *generailzed Frobenius automorphism* of $GR(4, 4^r)$ over $GR(4, 4^d)$ in [9]. For any $c \in GR(4, 4^r)$, define $Tr_d^r(c) = c + \phi(c) + \cdots + \phi^{\frac{r}{d}-1}(c)$ to be the generalized trace of $c \in GR(4, 4^r)$ relative to $GR(4, 4^d)$. Especially, if $c_0 \in \mathcal{T}$, we have

$$Tr_d^r(c_0) = c_0 + c_0^{2^d} + \cdots + c_0^{2^{d(\frac{r}{d}-1)}}. \tag{1}$$

For more detailed description of the theory of Galois rings, please refer to [9].

Let p be an odd prime and λ_n be the order of 2 modulo p^n, that is $2^{\lambda_n} \equiv 1 \pmod{p^n}$, then $p^n | (2^{\lambda_n} - 1)$, and there exists a nonzero element ξ_n of order $2^{\lambda_n} - 1$ in $GR(4, 4^{\lambda_n})$, then $\xi_n^{\frac{2^{\lambda_n}-1}{p^n}}$ denoted as β has order p^n. Thus, the quaternary sequence $\mathbf{s} = (s(0), s(1), \ldots)$ over $\mathbb{Z}_4$ of period p^n can be represented as

$$s(t) = \frac{1}{p^n} \sum_{k=0}^{p^n-1} \hat{s}(k)\beta^{kt}, \quad t = 0, 1, \ldots, p^n - 1, \tag{2}$$

[†]The author is with School of Mathematics and Statistics, Fujian Normal University, Fuzhou, Fujian, 350117, P.R. China.

[††]The author is with Key Laboratory of Analytical Mathematics and Applications (Ministry of Education), Fujian Normal University, Fuzhou, Fujian, 350117, P.R. China.

[†††]The author is with School of Mathematics and Statistics, Zhengzhou University, Zhengzhou, Henan, 450001, P. R. China.

[†]This work was supported by National Natural Science Foundation of China (No. 62272420), Natural Science Foundation of Fujian Province (No. 2023J01535).

a) E-mail: ffyfjnu@139.com

b) E-mail: keph@fjnu.edu.cn(corresponding author)

c) E-mail: zuling_chang@zzu.edu.cn

where

$$\hat{s}(k) = \sum_{t=0}^{p^n-1} s(t)\beta^{-kt}, \quad k = 0, 1, \ldots, p^n - 1. \tag{3}$$

Here $\hat{s}(k)$ is the *discrete Fourier transform* of $\mathbf{s}$ and $\hat{\mathbf{s}} = (\hat{s}(0), \hat{s}(1), \ldots)$ is called the *Fourier spectral sequence* of $\mathbf{s}$. The polynomial defined as

$$\hat{S}(x) = \frac{1}{p^n} \sum_{k=0}^{p^n-1} \hat{s}(k)x^k \in GR(4, 4^{\lambda_n})[x] \tag{4}$$

is called *Mattson-Solomon polynomial* in coding theory[10]. We have

$$s(t) = \hat{S}(\beta^t), \quad t \geq 0. \tag{5}$$

The polynomial satisfying (5) is also called the *defining polynomial* of $\mathbf{s}$ corresponding to β in[11]. Note that for a given β, since $\gcd(p^n, 4) = 1$, thus $\hat{S}(x)$ is uniquely determined modulo $x^{p^n} - 1$.

The following lemma provides a method for calculating the linear complexity of quaternary sequences over $\mathbb{Z}_4$.

Lemma 1: ([12]) Let $\mathbf{s} = (s(0), s(1), \ldots)$ be a quaternary sequence over $\mathbb{Z}_4$ of period p^n, and let $\hat{\mathbf{s}} = (\hat{s}(0), \hat{s}(1), \ldots)$ be its Fourier spectral sequence defined in (3). Then $LC(\mathbf{s})$, the linear complexity of $\mathbf{s}$ over $\mathbb{Z}_4$, is given by

$$LC(\mathbf{s}) = |\{k : \hat{s}(k) \neq 0, 0 \leq k \leq p^n - 1\}|.$$

That is, the linear complexity of the sequence $\mathbf{s}$ is equal to the number of nonzero coefficients in (4).

The following lemma contributes to understand the cyclotomic technique required in this letter.

Lemma 2: ([13]) Let p be a prime, then the following three assertions are equivalent:
(1) g is a primitive root of p and $g^{p-1} \not\equiv 1 \pmod{p^2}$.
(2) g is a primitive root of p^2.
(3) For every $m \geq 2$, g is a primitive root of p^m.

By Lemma 2, if g is a primitive root of p^2, then g is a primitive root of p^m, where $1 \leq m \leq n$. Moreover, the order of g in $\mathbb{Z}_{p^m}^*$ is $\varphi(p^m) = p^{m-1}(p-1)$, where $\varphi(\cdot)$ denotes the Euler function.

Let $p = ef + 1$ be an odd prime and g is a primitive root of p^2. For each $m (1 \leq m \leq n)$, $i \in \mathbb{Z}_e$, define

$$D_i^{(m)} = \left\{ g^{ek+i} \pmod{p^m} : k = 0, 1, \ldots, p^{m-1}f - 1 \right\}. \tag{6}$$

The division of $\mathbb{Z}_{p^m}^*$ can be obtained, that is

$$\mathbb{Z}_{p^m}^* = D_0^{(m)} \cup D_1^{(m)} \cup \cdots \cup D_{e-1}^{(m)}.$$

Due to $\mathbb{Z}_{p^m} = \mathbb{Z}_{p^m}^* \cup p\mathbb{Z}_{p^{m-1}}$, then $\mathbb{Z}_{p^n}$ can be denotes as

$$\mathbb{Z}_{p^n} = \left(\bigcup_{m=1}^{n} p^{n-m} D_0^{(m)}\right) \cup \cdots \cup \left(\bigcup_{m=1}^{n} p^{n-m} D_{e-1}^{(m)}\right) \cup \{0\}.$$

We denote

$$C_i = \bigcup_{m=1}^{n} p^{n-m} D_i^{(m)}, \quad 0 \leq i \leq e - 1. \tag{7}$$

Then $\mathbb{Z}_{p^n} = \bigcup_{i=0}^{e-1} C_i \cup \{0\}$.

The following lemma is the property of the cyclotomic classes.

Lemma 3: ([14]) Let $a \in \mathbb{Z}_{p^n}^*$, if $a \pmod{p^n} \in D_i^{(n)}$, then $aD_l^{(m)} \pmod{p^m} = D_{l+i \pmod e}^{(m)}$, $aC_l = C_{l+i \pmod e}$, where $0 \leq i \leq e-1, 0 \leq l \leq e-1, 1 \leq m \leq n$.

3. Trace representation of a family of balanced quaternary sequences

In this section, we will use the generalized cyclotomic classes to define a family of balanced quaternary sequences of period p^n, and calculate their trace representation over $\mathbb{Z}_4$.

Let $p = ef + 1$ be an odd prime, where $e \equiv 0 \pmod 4$, and C_i is defined in (7). Then a class of balanced quaternary sequences $\mathbf{s} = (s(0), s(1), \ldots)$ can be defined as:

$$s(t) = \begin{cases} a_i, & \text{if } t \pmod{p^n} \in C_i, \\ a_*, & \text{if } t \pmod{p^n} = 0, \end{cases} \tag{8}$$

where $a_*, a_0, \ldots, a_{e-1} \in \mathbb{Z}_4$, and the number of occurrences of 0, 1, 2 and 3 in $a_0, a_1, \ldots, a_{e-1}$ is the same. Obviously, $p^m (m < n)$ is not a period of $\mathbf{s}$, then it possesses the least period p^n.

Define a sequence $\mathbf{b}_i = (b_i(0), b_i(0), \ldots)$ of period p^n as follows:

$$b_i(t) = \begin{cases} 1, & \text{if } t \pmod{p^n} \in C_i; \\ 0, & \text{if } t \pmod{p^n} = 0. \end{cases} \tag{9}$$

Easy to verify the balanced quaternary sequence defined in (8) can be represented as

$$\mathbf{s} = a_*\boldsymbol{\delta} + \sum_{i=0}^{e-1} a_i \mathbf{b}_i, \tag{10}$$

where each $\mathbf{b}_i$ is defined in (9), and $\boldsymbol{\delta} = (\delta(0), \delta(1), \ldots)$ satisfies

$$\delta(t) = \begin{cases} 1, & \text{if } t \pmod{p^n} = 0; \\ 0, & \text{otherwise}. \end{cases} \tag{11}$$

Let g be a primitive root of p^2 and v be an integer for which $-1 \in D_v^{(n)}$. Let λ_n be the order of 2 modulo p^n, then β is a fixed element of order p^n in $GR(4, 4^{\lambda_n})$. Define polynomial $D_l^{(m)}(x) = \sum_{t \in D_l^{(m)}} x^t$, where $D_l^{(m)}$ is defined in (6), $0 \leq l \leq e-1$, $1 \leq m \leq n$. Also define polynomial $C_l(x) = \sum_{t \in C_l} x^t$, where C_l is defined in (7), $0 \leq l \leq e-1$.

The defining polynomial of the sequence $\mathbf{s}$ defined in (8) can be calculated by the following lemma.

Lemma 4: Let s be a sequence defined in (8). Then $\hat{S}(x)$,

the defining polynomial of $\mathbf{s}$ corresponding to β is given by

$$\hat{S}(x) = \rho_* + \sum_{l=0}^{e-1}\sum_{m=1}^{n} \rho_{l,m} D_l^{(m)}(x^{p^{n-m}}),$$

where $\rho_* = a_* + \dfrac{p^n-1}{e}\sum\limits_{i=0}^{e-1} a_i$, and for $0 \le l < e$, $1 \le m \le n$,

$$\rho_{l,m} = a_* + \sum_{i=0}^{e-1} a_i C_{i+l+v \pmod e}(\beta^{p^{n-m}}). \tag{12}$$

Proof 1: According to (5) and (10), we have

$$\begin{aligned}\hat{S}(\beta^t) = s(t) &= a_*\delta(t) + \sum_{i=0}^{e-1} a_i b_i(t)\\ &= a_*\hat{\triangle}(\beta^t) + \sum_{i=0}^{e-1} a_i \hat{B}_i(\beta^t),\end{aligned}$$

where $\hat{\triangle}(x)$ and $\hat{B}_i(x)$ denote the defining polynomials of $\boldsymbol{\delta}$ defined in (11) and $\mathbf{b}_i$ defined in (9) corresponding to β, respectively. Thus, we will calculate $\hat{\triangle}(x)$ and $\hat{B}_i(x)$, respectively.

We first calculate $\hat{B}_i(x)$. The Fourier spectral sequence of the sequence $\mathbf{b}_i$ defined in (9) write as $\hat{\mathbf{b}_i}$. By (3) and (9), we have $\hat{b}_i(0) = \sum_{t=0}^{p^n-1} b_i(t) = |C_i| = \dfrac{p^n-1}{e}$, and for $k = 1, 2, \ldots, p^n-1$, $\hat{b}_i(k) = \sum_{t=0}^{p^n-1} b_i(t)\beta^{-kt} = \sum_{t\in C_i}\beta^{-kt}$.

Since we assume that $-1 \in D_v^{(n)}$, for any $k \in \mathbb{Z}_{p^n}\setminus\{0\}$, there uniquely exitsts a pair (l,m) such that $k = p^{n-m}k'$, where $k' \in D_l^{(m)}$, $0 \le l \le e-1$ and $1 \le m \le n$. Then by Lemma 3, we have

$$\begin{aligned}-kC_i &= -p^{n-m}k'\left(\bigcup_{u=1}^{n} p^{n-u}D_i^{(u)}\right)\\ &= p^{n-m}\left(\bigcup_{u=1}^{n} p^{n-u}D_{i+l+v \pmod e}^{(u)}\right)\\ &= p^{n-m}C_{i+l+v \pmod e}.\end{aligned}$$

Therefore,

$$\begin{aligned}\hat{b}_i(k) = \sum_{t\in C_i}\beta^{-kt} &= \sum_{t\in C_{i+l+v \pmod e}}\beta^{p^{n-m}t}\\ &= C_{i+l+v \pmod e}(\beta^{p^{n-m}}),\end{aligned}$$

which implies that the value of $\hat{b}_i(k)$ depends on $p^{n-m}D_l^{(m)}$ to which k belongs. By (4), we get

$$\begin{aligned}\hat{B}_i(x) &= \sum_{k=0}^{p^n-1}\hat{b}_i(k)x^k = \hat{b}_i(0) + \sum_{k=1}^{p^n-1}\hat{b}_i(k)x^k\\ &= \frac{p^n-1}{e} + \sum_{l=0}^{e-1}\sum_{m=1}^{n}\sum_{k\in(p^{n-m}D_l^{(m)})}\hat{b}_i(k)x^k\\ &= \frac{p^n-1}{e} + \sum_{l=0}^{e-1}\sum_{m=1}^{n} C_{i+l+v \pmod e}(\beta^{p^{n-m}})D_l^{(m)}(x^{p^{n-m}}).\end{aligned} \tag{13}$$

Next, we calculate $\hat{\triangle}(x)$. According to (3), the Fourier spectral sequence of the sequence $\boldsymbol{\delta}$ defined in (11) write as $\hat{\boldsymbol{\delta}}$. For $k \in \mathbb{Z}_{p^n}$, $\hat{\boldsymbol{\delta}}$ satisfies

$$\hat{\delta}(k) = \sum_{t=0}^{p^n-1}\delta(t)\beta^{-kt} = \delta(0)\beta^0 + \sum_{t=1}^{p^n-1}\delta(t)\beta^{-kt} = 1.$$

Thus, by (4), we get

$$\begin{aligned}\hat{\triangle}(x) &= \sum_{k=0}^{p^n-1}\hat{\delta}(k)x^k = \sum_{k=0}^{p^n-1}x^k = 1 + \sum_{k=1}^{p^n-1}x^k\\ &= 1 + \sum_{l=0}^{e-1}\sum_{m=1}^{n}\sum_{k\in(p^{n-m}D_l^{(m)})}x^k\\ &= 1 + \sum_{l=0}^{e-1}\sum_{m=1}^{n} D_l^{(m)}(x^{p^{n-m}}).\end{aligned} \tag{14}$$

Therefore, by (5), (10), (13) and (14), we have

$$\begin{aligned}s(t) &= a_*\delta(t) + \sum_{i=0}^{e-1} a_i b_i(t) = a_*\hat{\triangle}(\beta^t) + \sum_{i=0}^{e-1} a_i\hat{B}_i(\beta^t)\\ &= a_* + \frac{p^n-1}{e}\sum_{i=0}^{e-1} a_i\\ &+ \sum_{l=0}^{e-1}\sum_{m=1}^{n}[a_* + \sum_{i=0}^{e-1} a_i C_{i+l+v \pmod e}(\beta^{p^{n-m}})]D_l^{(m)}(\beta^{p^{n-m}t}).\end{aligned}$$

From (5), it can be concluded that the conclusion is valid. □

Theorem 1: The trace representation of the sequence $\mathbf{s}$ defined in (8) over $\mathbb{Z}_4$ is given by

(1) If $2 \in D_0^{(m)}$ for any $m (1 \le m \le n)$, then

$$s(t) = \rho_* + \sum_{l=0}^{e-1}\sum_{m=1}^{n}\rho_{l,m}\sum_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} Tr_1^{\lambda_m}(\beta^{p^{n-m}tg^{ei+l}}),$$

(2) If $2 \in D_h^{(m)}$ for any $m (1 \le m \le n)$, $1 \le h \le e-1$, then

$$s(t) = \rho_* + \sum_{l=0}^{e-1}\sum_{m=1}^{n}\rho_{l,m}\sum_{i=0}^{\frac{p^{m-1}fd}{\lambda_m}-1} Tr_d^{\lambda_m}(\beta^{p^{n-m}tg^{ei+l}}),$$

where ρ_* and $\rho_{l,m}$ are defined in (12), and $d = \dfrac{e}{\gcd(e,h)}$.

Proof 2: According to Lemma 4 and (5), if we can use the trace functions over Galois rings to represent $D_l^{(m)}(\beta^{p^{n-m}t})$ with $0 \le l \le e-1$ and $1 \le m \le n$, then we can obtain the trace representation of the sequence $\mathbf{s}$.

For each $1 \le m \le n$, let λ_m is the order of 2 modulo p^m, and let A_m denote the cyclic group generated by 2. Then A_m can be represented as

$$A_m = \langle 2\rangle = \left\{1, 2^1, \ldots, 2^{\lambda_m-1}\right\},$$

where $\langle a\rangle$ denotes the cyclic group generated by a.

If $2 \in D_0^{(m)}$ for any $m(1 \le m \le n)$, then we have $\lambda_m | p^{m-1} f$ and A_m is a subgroup of $D_0^{(m)}$. And notice that the element $g^{\frac{p^{m-1}ef}{\lambda_m}} = g^{e \cdot \frac{p^{m-1}f}{\lambda_m}} \in D_0^{(m)}$ is also of order λ_m. This implies

$$A_m = \langle 2 \rangle = \left\langle g^{\frac{p^{m-1}ef}{\lambda_m}} \right\rangle = \left\{ g^{e \cdot \frac{p^{m-1}f}{\lambda_m} \cdot t} : 0 \le t < \lambda_m \right\},$$

hence we have

$$\begin{aligned} D_0^{(m)} &= \left\{ g^{ek} : 0 \le k < p^{m-1} f \right\} \\ &= \bigcup_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} g^{ei} \left\langle g^{\frac{p^{m-1}ef}{\lambda_m}} \right\rangle = \bigcup_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} g^{ei} A_m. \end{aligned}$$

Define polynomial $A_m(x) = \sum_{l \in A_m} x^l = x + x^2 + x^{2^2} + \cdots + x^{2^{\lambda_m - 1}}$, then

$$D_0^{(m)}(x) = \sum_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} \sum_{l \in A_m} x^{g^{ei} l} = \sum_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} A_m(x^{g^{ei}}).$$

Thus, according to (1), $D_0^{(m)}(\beta^{p^{n-m}t})$ can be described by the trace function from $GR(4, 4^{\lambda_m})$ to $\mathbb{Z}_4$ as

$$\begin{aligned} D_0^{(m)}(\beta^{p^{n-m}t}) &= \sum_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} A_m(\beta^{p^{n-m}tg^{ei}}) \\ &= \sum_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} Tr_1^{\lambda_m}(\beta^{p^{n-m}tg^{ei}}). \end{aligned}$$

For $D_l^{(m)}$ with $0 < l < e$, since $D_l^{(m)} = g^l D_0^{(m)}$, then

$$D_l^{(m)}(\beta^{p^{n-m}t}) = \sum_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} Tr_1^{\lambda_m}(\beta^{p^{n-m}tg^{ei+l}}).$$

Therefore, from Lemma 4 and (5), we obtain

$$s(t) = \hat{S}(\beta^t) = \rho_* + \sum_{l=0}^{e-1} \sum_{m=1}^{n} \rho_{l,m} \sum_{i=0}^{\frac{p^{m-1}f}{\lambda_m}-1} Tr_1^{\lambda_m}(\beta^{p^{n-m}tg^{ei+l}}).$$

The case of $2 \in D_h^{(m)}$ for any $m(1 \le m \le n, 0 < h < e)$ can be proven similarly, so the proof is omitted here.

The proof is completed. □

Corollary 1: Let $\mathbf{s}$ be a sequence defined in (8), ρ_* and $\rho_{l,m}(0 \le l \le e-1, 1 \le m \le n)$ be defined in (12). For $1 \le m \le n$, denote $\rho_m = (\rho_{0,m}, \rho_{1,m}, \ldots, \rho_{e-1,m})$. Then $LC(\mathbf{s})$, the complexity of $\mathbf{s}$ over $\mathbb{Z}_4$, is given by $LC(\mathbf{s}) = \varepsilon(\rho_*) + \sum_{m=1}^{n} \omega_H(\rho_m) p^{m-1} f$, where if $\rho_* = 0$, then $\varepsilon(\rho_*) = 0$; otherwise $\varepsilon(\rho_*) = 1$. And $\omega_H(\rho_m)$ denotes the number of non-zero terms $\rho_{l,m}(0 \le l \le e-1)$ in ρ_m.

4. Conclusions

In this letter, we defined a class of balanced quaternary sequences of period p^n based on the generalized cyclotomic classes. Started from their defining polynomial, we determined the trace representation of these sequences over $\mathbb{Z}_4$. And by determining the number of nonzero coefficients in the defining polynomial of these sequences, their linear complexity over $\mathbb{Z}_4$ is obtained. When the value of n in period p^n is equal to 1, the family of quaternary sequences constructed in this letter becomes the case in [5]. Thus, the results in this letter can be regarded as generalizations of the work in [5].

References

[1] F. Adachi, D. Garg, S. Takaoka, and K. Takeda, "Broadband CDMA techniques," IEEE Wirel. Commun., vol.12, no.2, pp.8–18, Apr. 2005.
[2] S.W. Golomb and G. Gong, Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar, Cambridge Univ. Press, Cambridge, U.K., 2005.
[3] J.L. Massey and T. Schaub, "Linear complexity in coding theory," Lect. notes Comput., vol.311, pp.19–32, 1988.
[4] Z.X. Chen, "Linear complexity and trace representation of quaternary sequences over $\mathbb{Z}_4$ based on generalized cyclotomic classes modulo pq," Cryptogr. Commun., vol.9, pp.445–458, Jul. 2017.
[5] Z.Y. Yang, Z.B. Xiao, and X.Y. Zeng, "Linear complexity and trace representation of balanced quaternary cyclotomic sequences of prime period p," Cryptogr. Commun., vol.15, pp.921–940, Sep. 2023.
[6] P.H. Ke and S.Y. Zhang, "New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity," Inform. Process. Lett., vol.112, no.16, pp.646–650, 2012.
[7] V. Edemskiy, "The linear complexity and autocorrelation of quaternary Whiteman's sequences," International Journal of Applied Mathematics Electronics and Computers, vol.1, no.4, pp.7–11, Dec. 2013.
[8] Z.X. Chen and V. Edemskiy, "Linear complexity of quaternary sequences over $\mathbb{Z}_4$ derived from generalized cyclotomic classes modulo $2p$," International Journal of Network Security, vol.19, pp.613–622, 2016.
[9] Z.X. Wan, "Lectures on finite fields and Galois rings," World Scientific Publisher, pp.309–333, 2003.
[10] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," Elsevier, 1977.
[11] Z. Dai, G. Gong, H.Y. Song, and D. Ye, "Trace representation and linear complexity of binary eth power residue sequences of period p," IEEE Trans. Inf. Theory, vol.57, no.3, pp.1530–1547, Mar. 2011.
[12] P. Udaya and M.U. Siddiqi, "Generalized GMW quadriphase sequences satisfying the Welch bound with equality," Appl. Algebra Eng. Commun. Comput., vol.10, no.3, pp.203–225, Mar. 2000.
[13] P. Ribenboim, "The Book of Prime Number Records," Mathematical Gazette, vol.73, 1988.
[14] C.H. Wu, Z.X. Chen, and X.N. Du, "The linear complexity of q-ary generalized cyclotomic sequences of period p^m," J. Wuhan Univ. (Nat. Sci. Ed.), vol.59, no.2, pp.129–136, Apr. 2013.