Des. Codes Cryptogr. (2013) 67:19–35
DOI 10.1007/s10623-011-9583-0

A family of quadriphase sequences of period $4(2^n - 1)$ with low correlation and large linear span

Jie Li · Xiangyong Zeng · Xiaohu Tang · Chunlei Li

Received: 3 March 2011 / Revised: 26 September 2011 / Accepted: 30 October 2011 /
Published online: 19 November 2011

Abstract In this paper, a new family of quadriphase sequences with period $4(2^n - 1)$ is proposed for $n = me$, where m is an odd integer. The correlation values of the family, their distribution, and the linear spans of the proposed sequences are completely determined under two situations.

Keywords Galois ring · Quadriphase sequence · $\mathbf{Z}_4$-valued quadratic form · Low correlation · Linear span

Mathematics Subject Classification (2000) 94A05 · 94A55

1 Introduction

Families of pseudorandom sequences have wide applications in code-division multiple-access (CDMA) communications. In these applications, sequence families are preferred to have desired properties such as large family size, long period, low out-of-phase autocorrelation, low cross-correlation, large linear span, balance property and ease of implementation [6].

Communicated by P. Charpin.

J. Li · X. Zeng (✉)
Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China
e-mail: xzeng@hubu.edu.cn

J. Li
e-mail: jie.li2011@yahoo.com.cn

X. Tang
Provincial Key Lab of Information Coding and Transmission,
Institute of Mobile Communications, Southwest Jiaotong University, Chengdu 610031, China
e-mail: xhutang@ieee.org

C. Li
Department of Informatics, University of Bergen, 5020 Bergen, Norway
e-mail: chunlei.li@ii.uib.no

Since 1960s, many families of binary sequences with good properties have been found, and most of them are constructed by using m-sequences and their decimations. For example, the Gold sequences [2,4] and Kasami sequences [9,12,19].

In the late 1980s, the optimal family $\mathcal{A}$ of quadriphase sequences with period $2^n - 1$ and family size $2^n + 1$ was found [1,14]. The sequences in the family $\mathcal{A}$ are analogous to the m-sequences over Galois fields due to the similarity between Galois rings and Galois fields. By interleaving two sequences in $\mathcal{A}$, two optimal families $\mathcal{B}$ [1] and $\mathcal{C}$ [18] of quadriphase sequences can be obtained, and the corresponding period and family size of both $\mathcal{B}$ and $\mathcal{C}$ are $2(2^n - 1)$ and 2^{n-1}, respectively. Using a generalized quadratic form, Tang, Udaya and Fan generalized the family $\mathcal{A}$ and proposed a new family of quadriphase sequences with low correlation [15]. Based on a modification of the families $\mathcal{B}$ and $\mathcal{C}$, Tang and Udaya proposed the optimal family $\mathcal{D}$ of quadriphase sequences having the same period and maximal nontrivial correlation magnitude as the families $\mathcal{B}$ and $\mathcal{C}$ but a double family size [16]. By applying the orthogonal transformation to the families $\mathcal{B}$ and $\mathcal{C}$, another optimal family $\mathcal{E}$ of quadriphase sequences with period $2(2^n - 1)$ was also obtained in [17]. Recently, two new optimal families $\mathcal{S}$ and $\mathcal{U}$ of quadriphase sequences were presented in [8], which have the same correlation properties as the families $\mathcal{A}$ and $\mathcal{D}$ but larger linear span, respectively. And the correlation distribution of the family $\mathcal{U}$ was further studied in [10].

In this paper, we present a new construction of quadriphase sequence family $\mathcal{F}$ with period $4(2^n - 1)$ for $n = me$, where m is an odd integer. The key idea of the proposed construction is to interleave four sequences in the family $\mathcal{S}$ [8] and a perfect quadriphase sequence of period 4. By applying the theory of generalized quadratic forms to measure a related exponential sum, we determine the correlation property of the proposed family $\mathcal{F}$ under two situations. Further, the linear spans of those sequences are also completely determined. Every sequence in the family $\mathcal{F}_1$ (i.e., the family $\mathcal{F}$ under the first situation) can exactly be decomposed as the sum of a sequence in the family proposed in [11] and another quadriphase sequence. This leads to the sequences in the family $\mathcal{F}_1$ can achieve larger linear spans, although $\mathcal{F}_1$ and the family proposed in [11] have the same correlation distributions.

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries and notations. Section 3 proposes the quadriphase sequence family $\mathcal{F}$, and discusses the properties of an exponential sum. Under two situations, the correlation property and linear span of the proposed family are determined in Sects. 4 and 5. Section 6 concludes the study.

2 Preliminaries

2.1 Galois rings

Let $\mathbf{Z}_4[x]$ denote the ring of all polynomials over $\mathbf{Z}_4$, and $\bar{\cdot}$ denote the modulo 2 projection mapping from $\mathbf{Z}_4$ to $\mathbf{Z}_2$, i.e., $\overline{1} = \overline{3} = 1$ and $\overline{0} = \overline{2} = 0$. A monic polynomial $f(x) = \sum_{i=0}^{n} f_i x^i \in \mathbf{Z}_4[x]$ of degree n is said to be a *primitive basic irreducible polynomial* if $\overline{f}(x) = \sum_{i=0}^{n} \overline{f_i} x^i$ is a primitive polynomial over $\mathbf{Z}_2$. As in the case of finite fields, the Galois ring $\mathbf{R}$ may be constructed as quotients of the associated polynomial ring. In other words, the quotient ring $\mathbf{Z}_4[x]/(f(x))$, denoted by $\mathbf{R} = \mathrm{GR}(4, n)$, is called a Galois ring with 4^n elements and characteristic 4. Then naturally, the projection mapping $\bar{\cdot}$ induces a homomorphism from $\mathbf{R}$ to the finite field $\mathbf{F}_{2^n}$.

The element $x \in \mathbf{R}$ is a *unit* if there is an element $y \in \mathbf{R}$ such that $xy = 1$. Let $\mathbf{R}^*$ denote the set consisting of all units in $\mathbf{R}$. As a multiplicative group, $\mathbf{R}^*$ contains a cyclic subgroup of order $2^n - 1$. Let β be a generator of the cyclic group, then $\alpha = \overline{\beta}$ is a primitive element of $\mathbf{F}_{2^n}$. The Teichmüller set of $\mathbf{R}$ is defined as $\mathcal{T} = \left\{0, 1, \beta, \beta^2, \ldots, \beta^{2^n-2}\right\}$. Then, each $x \in \mathbf{R}$ has a 2-adic expansion of the following form

$$x = x_0 + 2x_1, \quad x_0,\ x_1 \in \mathcal{T}. \tag{1}$$

By (1), we have $x^2 = x_0^2$, then x is a unit if and only if $x_0 \neq 0$.

The *Frobenius automorphism* σ on $\mathbf{R}$ is given by

$$\sigma(x_0 + 2x_1) = x_0^2 + 2x_1^2, \quad \text{for all } x_0, x_1 \in \mathcal{T}.$$

Then the *trace function* $\mathrm{Tr}_1^n(\cdot)$ from $\mathbf{R}$ to $\mathbf{Z}_4$ is defined as

$$\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} \sigma^i(x).$$

Let $\mathrm{tr}_1^n(\cdot)$ denote the *trace function* from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$, i.e.,

$$\mathrm{tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}.$$

The following properties hold for arbitrary elements $x,\ y \in \mathbf{R}$:

P1) $\overline{\mathrm{Tr}_1^n(x)} = \mathrm{tr}_1^n(\overline{x})$;
P2) $\mathrm{Tr}_1^n(x + y) = \mathrm{Tr}_1^n(x) + \mathrm{Tr}_1^n(y)$.

2.2 $\mathbf{Z}_4$-valued quadratic forms

Since the addition operation in the Teichmüller set $\mathcal{T}$ is not closed, for $x,\ y \in \mathcal{T}$, we define an operation $\oplus$ on $\mathcal{T}$ by

$$x \oplus y = x + y + 2(xy)^{2^{n-1}}.$$

Then we have

$$2(x \oplus y) = 2(x + y) \ \text{ for } x, y \in \mathcal{T}. \tag{2}$$

Obviously, $(\mathcal{T}, \oplus, \cdot)$ is a Galois field isomorphic to $(\mathbf{F}_{2^n}, +, \cdot)$.

Let $K = \{0, 1\}$ be the Teichmüller set of $\mathbf{Z}_4$, then $(K, \oplus, \cdot)$ is the finite field of size 2, and it is the prime subfield of $\mathcal{T}$.

A *symmetric bilinear form* on $\mathcal{T}$ is a mapping $B : \mathcal{T} \times \mathcal{T} \longrightarrow K$ satisfying the symmetry

$$B(x, y) = B(y, x)$$

and the bilinearity

$$B(ax \oplus by, z) = aB(x, z) \oplus bB(y, z), \quad \text{for } a,\ b \in K.$$

In addition, if $B(x, x) = 0$ holds for all $x \in \mathcal{T}$, then B is called *alternating*. Otherwise, it is called *nonalternating*. The *rank* of B is defined as

$$\mathrm{rank}(B) = n - \dim_K(\mathrm{rad}(B)) \tag{3}$$

where $\mathrm{rad}(B) = \{x \in \mathcal{T} : B(x, y) = 0,\ \forall\, y \in \mathcal{T}\}$.

Definition 1 ([3]) A $\mathbf{Z}_4$-valued quadratic form is a mapping $Q : \mathcal{T} \longrightarrow \mathbf{Z}_4$ that satisfies

$$Q(x \oplus y) = Q(x) + Q(y) + 2B(x, y)$$

where $B : \mathcal{T} \times \mathcal{T} \longrightarrow K$ is a symmetric bilinear form.

The $\mathbf{Z}_4$-valued quadratic form Q is similarly called *alternating* if its associated bilinear form B is alternating. Otherwise, Q is called *nonalternating*. Moreover, Q is said to have *rank r* if its associated bilinear form B has rank r.

For a $\mathbf{Z}_4$-valued quadratic form Q: $\mathcal{T} \longrightarrow \mathbf{Z}_4$, define an exponential sum

$$\chi_Q(u) = \sum_{x \in \mathcal{T}} \omega^{Q(x)+2\mathrm{Tr}_1^n(ux)}, \quad u \in \mathcal{T} \tag{4}$$

where $\omega = \sqrt{-1}$ is a primitive fourth complex root of unity. Then the value distribution of the multi-set

$$\{\chi_Q(u) : u \in \mathcal{T}\}$$

depends only on the rank of Q and on whether Q is alternating or nonalternating (see [13]).

Lemma 1 *([13]) Let Q be a nonalternating $\mathbf{Z}_4$-valued quadratic form of rank r, then the value distribution of the multi-set $\{\chi_Q(u) : u \in \mathcal{T}\}$ is given by*

$$\chi_Q(u) = \begin{cases} 0, & 2^n - 2^r \text{ times}, \\ \pm(1+\omega)2^{n-\frac{r+1}{2}}, & 2^{r-2} \pm 2^{\frac{r-3}{2}} \text{ times}, \\ \pm(1-\omega)2^{n-\frac{r+1}{2}}, & 2^{r-2} \pm 2^{\frac{r-3}{2}} \text{ times} \end{cases}$$

for odd r, and

$$\chi_Q(u) = \begin{cases} 0, & 2^n - 2^r \text{ times}, \\ \pm 2^{n-\frac{r}{2}}, & 2^{r-2} \pm 2^{\frac{r}{2}-1} \text{ times}, \\ \pm 2^{n-\frac{r}{2}}\omega, & 2^{r-2} \text{ times (each)} \end{cases}$$

for even r.

2.3 Basic concepts of sequences

Two periodic sequences $\{s_i(t)\}$ and $\{s_j(t)\}$ are called *cyclically equivalent* if there exists a positive integer k such that

$$s_i(t) = s_j(t+k) \text{ for all } t \geq 0.$$

Otherwise, they are called to be *cyclically inequivalent*.

A sequence $\{s(t)\}$ is called a quadriphase (respectively, binary) sequence if $s(t) \in \mathbf{Z}_4$ (respectively, $\mathbf{Z}_2$) for all $t \geq 0$.

For a quadriphase (respectively, binary) sequence $s = \{s(t)\}$, we say that the sequence s *can be decomposed as the sum* of the quadriphase (respectively, binary) sequences $s^0 = \{s^0(t)\}, s^1 = \{s^1(t)\}, \cdots, s^k = \{s^k(t)\}$, i.e., $s = s^0 + s^1 + \cdots + s^k$, if

$$s(t) = s^0(t) + s^1(t) + \cdots + s^k(t) \text{ for all } t \geq 0, \tag{5}$$

where "+" in (5) denotes addition modulo 4 (respectively, 2).

Let $\mathcal{F}$ be a family of M cyclically inequivalent quadriphase sequences of period N given by

$$\mathcal{F} = \left\{ s_i = \{s_i(t)\}_{t=0}^{N-1} : 0 \leq i < M \right\}.$$

The *correlation function* of the sequences s_i and s_j in $\mathcal{F}$ is defined as

$$R_{s_i,s_j}(\tau) = \sum_{t=0}^{N-1} \omega^{s_i(t)-s_j(t+\tau)}$$

where $0 \le \tau < N$ and $t+\tau$ is taken modulo N. When $s_i = s_j$, $R_{s_i,s_j}(\tau)$ can be simplified as $R_{s_i}(\tau)$.

A quadriphase sequence s of period N is *perfect* if $R_s(\tau) = 0$ for all $0 < \tau < N-1$.

The *correlation distribution* of the family $\mathcal{F}$ is the value distribution of the following multi-set

$$\{R_{s_i,s_j}(\tau) : 0 \le i, j < M \text{ and } 0 \le \tau < N\}.$$

The *maximum nontrivial correlation magnitude* $R_{\max}$ of $\mathcal{F}$ is

$$R_{\max} = \max\Big\{|R_{s_i,s_j}(\tau)| : 0 \le i, j < M \text{ and } (i \ne j \text{ or } \tau \ne 0)\Big\}.$$

The *linear span* of a sequence s is the length of the shortest linear feedback shift register (LFSR) that generates s. More precisely, let

$$f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0 \in \mathbf{Z}_4[x] \text{ (respectively, } \mathbf{F}_2[x]),$$

if a quadriphase (respectively, binary) sequence $s = \{s(t)\}$ satisfies the linear recursive relation:

$$s(n+k) = c_{n-1}s(n+k-1) + \cdots + c_1 s(k+1) + c_0 s(k), \quad k \ge 0, \tag{6}$$

then $f(x)$ is called a *characteristic polynomial* of s. A monic polynomial with the lowest degree among all characteristic polynomials of the quadriphase (respectively, binary) sequence s is called a (respectively, the) *minimal polynomial* of s. The linear span of s is equal to the degree of a (respectively, the) minimal polynomial of s. Notice that a binary sequence has a unique minimal polynomial, while for a quadriphase sequence, its minimal polynomials may not be unique but they have the same degree [8].

For a sequence $s = (s(0), s(1), s(2), \cdots)$, define the left shift operator L as follows:

$$L^i(s) = (s(i), s(i+1), s(i+2), \cdots) \quad \text{for all } i \ge 1.$$

By convention, we write $L^0(s) = s$. Then the formula (6) can be written as

$$f(L)s = (L^n - c_{n-1}L^{n-1} - \cdots - c_1 L - c_0 L^0)s = \mathbf{0}$$

where $\mathbf{0}$ denotes the zero sequence of which all elements are 0. Thus a monic polynomial $f(x)$ is a characteristic polynomial of s if and only if $f(L)s = \mathbf{0}$. For more details, please refer to [6,5].

The following lemma will be used to study the linear span of the proposed sequences.

Lemma 2 *Let s be a quadriphase sequence and s' a binary sequence. Let $f(x) \in \mathbf{Z}_4[x]$ be a minimal polynomial of s and $g(x) \in \mathbf{F}_2[x]$ be the minimal polynomial of s'. Assume $\overline{f}$ is the minimal polynomial of $\overline{s}$, and let $gcd\left(\overline{f}(x), g(x)\right) = d_1(x)$, $gcd\left(g(x)/d_1(x), d_1(x)\right) = d_2(x)$. Then we have the following results.*

(1) ([8]) If $d_1(x) = 1$, then we have that the product $f(x)g(x) \in \mathbf{Z}_4[x]$ is a minimal polynomial of the sum $a = s + 2s'$.

(2) If $d_1(x) \neq 1$, then the linear span $LS(a)$ of $a = s + 2s'$ satisfies

$$LS(a) \geq deg\,(f(x)) + deg(g(x)) - deg(d_1(x)) - deg(d_2(x)).$$

Proof Since (1) has been proved in [8], we only give the proof of (2) here.

If $d_1(x) \neq 1$, let $k(x)$ be a minimal polynomial of the sequence a. Then we have $\overline{k}(L)(\overline{a}) = \mathbf{0}$, which implies $\overline{f}(x)$ divides $\overline{k}(x)$. By division with a remainder, $k(x)$ can be written as

$$k(x) = f(x)t(x) + 2\sigma(x)$$

with $\sigma(x) = 0$ or $\deg(\sigma(x)) < \deg(f(x))$.

From

$$(f(L)t(L) + 2\sigma(L))(s + 2s') = \mathbf{0}$$

we have

$$\overline{\sigma}(L)(\overline{s}) + \overline{f}(L)\overline{t}(L)(s') = \mathbf{0}. \tag{7}$$

Multiplying the both sides of (7) by $\overline{f}(L)$, we have

$$\overline{f}(L)\overline{\sigma}(L)(\overline{s}) + \overline{f}^2(L)\overline{t}(L)(s') = \mathbf{0},$$

by which we have

$$\overline{f}^2(L)\overline{t}(L)(s') = \mathbf{0}.$$

Thus $g(x)|\overline{f}^2(x)\overline{t}(x)$. Let $\overline{f}(x) = f_1(x)d_1(x)$ and $g(x) = g_1(x)d_1(x)$, we have $g_1|f_1^2 d_1\overline{t}$, which implies $g_1|d_1\overline{t}$ by $\gcd(f_1, g_1) = 1$. Let $g_1(x) = g_1'(x)d_2(x)$, $d_1(x) = d_1'(x)d_2(x)$, and then we have $g_1'|d_1'\overline{t}$. Thus $g_1'|\overline{t}$ by $\gcd(g_1'(x), d_1'(x)) = 1$. This implies $\deg(t(x)) \geq \deg(g_1'(x))$. Consequently, we have $\deg(k(x)) \geq \deg(f(x)) + \deg(g_1'(x))$. Since $g(x) = g_1'(x)d_2(x)d_1(x)$, we have $\deg(k(x)) \geq \deg(f(x)) + \deg(g(x)) - \deg(d_1(x)) - \deg(d_2(x))$. This finishes the proof. □

Notations

The following notations are used throughout this paper:

- The positive integers n, k, e, m satisfy $e = \gcd(n, k)$ and $n = me$ with an odd integer $m \geq 3$;
- $\{\eta_0, \eta_1, \ldots, \eta_{2^n-1}\}$ is an enumeration of the elements in $\mathcal{T}$, and β is a generator of $\mathcal{T}\backslash\{0\}$;
- $\alpha = \overline{\beta}$ is a primitive element of $\mathbf{F}_{2^n}$;
- λ is an element in $\mathbf{R}$ with $\overline{\lambda} \in \mathbf{F}_{2^e}\backslash\{0, 1\}$;
- v is an element in $\mathcal{T}$ with $\overline{v} \in \mathbf{F}_{2^e}$ and $\mathrm{tr}_1^e(\overline{v}) = 1$;
- $\beta^{l/4}$ denotes $\beta^{2^{n-2}\cdot l}$ for $0 \leq l < 4$;
- $\omega = \sqrt{-1}$ is a primitive fourth complex root of unity;
- $\mathrm{Re}(z)$ denotes the real part for a complex number z.

3 Results on the exponential sum $\xi(\gamma_1, \gamma_2, \delta)$ and a construction of quadriphase sequences

Given $x \in \mathbf{R}$, we define a function $P(x)$ via

$$P(x) = \sum_{j=1}^{(m-1)/2} \mathrm{Tr}_1^n\left(x^{2^{kj}+1}\right). \tag{8}$$

For all $\gamma_1, \gamma_2 \in \mathbf{R}$, and $\delta \in \mathcal{T}$, define an exponential sum

$$\xi(\gamma_1, \gamma_2, \delta) = \sum_{x \in \mathcal{T}} \omega^{\mathrm{Tr}_1^n([(1+2\gamma_1-(1+2\gamma_2)\delta)]x)+2(P(\lambda x)+P(\lambda\delta x))}. \tag{9}$$

This exponential sum has been extensively studied in [8,10]. In what follows, we will use the results in these two references to discuss some other properties of $\xi(\gamma_1, \gamma_2, \delta)$.

Let $1+2\gamma_1-(1+2\gamma_2)\delta = c+2u$ where $c, u \in \mathcal{T}$, and let $\lambda^{2^{kj}+1}+(\lambda\delta)^{2^{kj}+1} = a_j+2b_j$ for $1 \le j \le \frac{m-1}{2}$, where $a_j, b_j \in \mathcal{T}$. Then by (4), the exponential sum $\xi(\gamma_1, \gamma_2, \delta)$ can be rewritten as

$$\xi(\gamma_1, \gamma_2, \delta) = \sum_{x \in \mathcal{T}} \omega^{Q(x)+2\mathrm{Tr}_1^n(ux)}, \tag{10}$$

where

$$Q(x) = \mathrm{Tr}_1^n(cx) + 2\sum_{j=1}^{\frac{m-1}{2}} \mathrm{Tr}_1^n\left(a_j x^{2^{kj}+1}\right) \tag{11}$$

is a $\mathbf{Z}_4$-valued quadratic form and the associated bilinear form is

$$B(x, y) = \overline{\mathrm{Tr}_1^n\left(c^2xy\right)} \oplus \bigoplus_{j=1}^{\frac{m-1}{2}} \overline{\mathrm{Tr}_1^n\left[a_j\left(x^{2^{kj}}y + y^{2^{kj}}x\right)\right]}.$$

Then $Q(x)$ is alternating if and only if $c = 0$, i.e., $\delta = 1$. In this case,

$$\xi(\gamma_1, \gamma_2, 1) = \sum_{x \in \mathcal{T}} \omega^{\mathrm{Tr}_1^n[2(\gamma_1-\gamma_2)x]} = \begin{cases} 2^n, & \text{if } \overline{\gamma_1} = \overline{\gamma_2}, \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

When $\delta \neq 1$, by Lemma 1, the values of $\xi(\gamma_1, \gamma_2, \delta)$ are mainly dependent on the rank r of $Q(x)$.

Lemma 3 *([10]) For all $\gamma_1, \gamma_2 \in \mathbf{R}$ and $\delta \in \mathcal{T}\backslash\{0, 1\}$, the rank of $Q(x)$ defined in (11) is n.*

Lemma 4 *For all $v_0, v_1 \in \mathcal{T}$, and for each fixed $j \in \{0, 1, 2, \cdots, 2^n-1\}$, when $\delta \in \mathcal{T}\backslash\{0, 1\}$ and n is odd, the value distribution of sums $\xi(\eta_i + v_0, \eta_j + v_1, \delta)$ is given by*

$$\xi(\eta_i + v_0, \eta_j + v_1, \delta) = \begin{cases} (1 \pm \omega)2^{\frac{n-1}{2}}, & 2^{n-2} + 2^{\frac{n-3}{2}} \text{ times (each),} \\ (-1 \pm \omega)2^{\frac{n-1}{2}}, & 2^{n-2} - 2^{\frac{n-3}{2}} \text{ times (each)} \end{cases}$$

as i ranges from 0 to $2^n - 1$.

Proof Let $1 - \delta = c + 2u'$ where $c, u' \in \mathcal{T}$. It follows from (10) that

$$\xi(\eta_i + v_0, \eta_j + v_1, \delta) = \sum_{x \in \mathcal{T}} \omega^{Q(x)+2\mathrm{Tr}_1^n(ux)}$$

where $u = u' \oplus \eta_i \oplus v_0 \oplus \eta_j\delta \oplus v_1\delta$.

Given $v_0, v_1 \in \mathcal{T}$, $j \in \{0, 1, 2, \cdots, 2^n - 1\}$, and $\delta \in \mathcal{T}\backslash\{0, 1\}$, when i ranges from 0 to $2^n - 1$, u runs through $\mathcal{T}$. Notice that $Q(x)$ is nonalternating. Then by Lemmas 1 and 3 we get the desired result. □

For all $\gamma_1, \gamma_2 \in \mathbf{R}$, and $\delta \in \mathcal{T}$, define

$$\varsigma(\gamma_1, \gamma_2, \delta) = \xi(\gamma_1, \gamma_2, \delta) + \xi(\gamma_1 + v, \gamma_2 + v, \delta) \tag{13}$$

and

$$\kappa(\gamma_1, \gamma_2, \delta) = \xi(\gamma_1, \gamma_2, \delta) - \xi(\gamma_1 + v, \gamma_2 + v, \delta). \tag{14}$$

Then we have the following result.

Lemma 5 *For each fixed $\delta \notin \{0, 1\}$, as γ_1, γ_2 run through $\mathcal{T}$, $\varsigma(\gamma_1, \gamma_2, \delta)$ and $\kappa(\gamma_1, \gamma_2, \delta)$ have the following distribution.*

(1) When $v = 1$ and n is odd,

$$\varsigma(\gamma_1, \gamma_2, \delta) = \pm 2^{\frac{n+1}{2}},\ 2^{2n-1} \pm 2^{\frac{3n-1}{2}}\ times.$$

(2) When $v \neq 1$ and n is odd,

$$\varsigma(\gamma_1, \gamma_2, \delta) = \begin{cases} \pm 2^{\frac{n+1}{2}}, & 2^{2n-2} \pm 2^{\frac{3n-1}{2}}\ times, \\ \pm 2^{\frac{n+1}{2}}\omega, & 2^{2n-2}\ times\ (each). \end{cases}$$

(3) When $v \neq 1$ and n is even,

$$\varsigma(\gamma_1, \gamma_2, \delta) = \begin{cases} 2^{\frac{n}{2}} \pm 2^{\frac{n}{2}}\omega, & 2^{2n-2} + 2^{\frac{3n-2}{2}}\ times\ (each), \\ -2^{\frac{n}{2}} \pm 2^{\frac{n}{2}}\omega, & 2^{2n-2} - 2^{\frac{3n-2}{2}}\ times\ (each). \end{cases}$$

(4) When $v = 1$ and n is odd,

$$\kappa(\gamma_1, \gamma_2, \delta) = \pm 2^{\frac{n+1}{2}}\omega,\ 2^{2n-1}\ \text{times (each)}.$$

(5) When $v \neq 1$ and n is odd,

$$\kappa(\gamma_1, \gamma_2, \delta) = \begin{cases} \pm 2^{\frac{n+1}{2}}, & 2^{2n-2}\ times\ (each), \\ \pm 2^{\frac{n+1}{2}}\omega, & 2^{2n-2}\ times\ (each). \end{cases}$$

(6) When $v \neq 1$ and n is even,

$$\kappa(\gamma_1, \gamma_2, \delta) = \begin{cases} 2^{\frac{n}{2}} \pm 2^{\frac{n}{2}}\omega, & 2^{2n-2}\ times\ (each), \\ -2^{\frac{n}{2}} \pm 2^{\frac{n}{2}}\omega, & 2^{2n-2}\ times\ (each). \end{cases}$$

The proof is similar to those of Lemmas 7 and 8 in [8], so we omit it here.

To end this section, we give the construction for a family of quadriphase sequences with period $4(2^n - 1)$ as follows.

Definition 2 Let $v_0, v_1, v_2, v_3 \in \mathcal{T}$, we define a family $\mathcal{F} = \{s_0, s_1, \cdots, s_{2^n-1}\}$ of quadriphase sequences, where $s_i = \{s_i(t)\}_{t=0}^{4(2^n-1)-1}$ is given by

$$s_i(t) = \begin{cases} \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_0)]\beta^{t_0}\right) + 2P\left(\lambda\beta^{t_0}\right) + 2, & t = 4t_0, \\ \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_1)]\beta^{t_0+1/4}\right) + 2P\left(\lambda\beta^{t_0+1/4}\right), & t = 4t_0 + 1, \\ \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_2)]\beta^{t_0+2/4}\right) + 2P\left(\lambda\beta^{t_0+2/4}\right), & t = 4t_0 + 2, \\ \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_3)]\beta^{t_0+3/4}\right) + 2P\left(\lambda\beta^{t_0+3/4}\right), & t = 4t_0 + 3 \end{cases}$$

and $P(x)$ is defined by (8).

In Sects. 4 and 5, we will analyze the correlation distribution and the linear span of $\mathcal{F}$ for two special cases as below.

(1) Let $v_0 = v_3 = 0, v_1 = v_2 = 1$ and e be an odd integer ≥ 3 which forces n to be odd since m is odd, and in this case we call the family $\mathcal{F}$ as $\mathcal{F}_1$;
(2) Let $v_0 = v_2 = 0$ and $v_1 = v_3 = v$, and in this case we call the family $\mathcal{F}$ as $\mathcal{F}_2$.

Remark 1 The Ref. [11] introduced a family $\mathcal{S} = \left\{s'_0, s'_1, \ldots, s'_{2^n-1}\right\}$ of quaternary sequences $s'_i = \left\{s'_i(t)\right\}_{t=0}^{4(2^n-1)-1}$ defined by

$$s'_i(t) = \begin{cases} \mathrm{Tr}_1^n\left((1+2\eta_i)(1+2v_0)\beta^{t_0}\right) + 2, & t = 4t_0, \\ \mathrm{Tr}_1^n\left((1+2\eta_i)(1+2v_1)\beta^{t_0+1/4}\right), & t = 4t_0+1, \\ \mathrm{Tr}_1^n\left((1+2\eta_i)(1+2v_2)\beta^{t_0+2/4}\right), & t = 4t_0+2, \\ \mathrm{Tr}_1^n\left((1+2\eta_i)(1+2v_3)\beta^{t_0+3/4}\right), & t = 4t_0+3 \end{cases} \tag{15}$$

with $v_0 = v_3 = 0$ and $v_1 = v_2 = 1$. Thus, each sequence s_i in $\mathcal{F}_1$ can exactly be decomposed as the sum of the sequence s'_i in $\mathcal{S}$ and the quadriphase sequence $\left\{2P\left(\lambda\beta^{t/4}\right)\right\}_{t=0}^{4(2^n-1)-1}$.

4 The correlation distribution and linear span of $\mathcal{F}_1$

In this section, we study the correlation distribution and linear span of $\mathcal{F}_1$.

4.1 Correlation distribution of the family $\mathcal{F}_1$

The correlation distribution of $\mathcal{F}_1$ and that of $\mathcal{S}$ (for odd n) in [11] are closely related to two different exponential sums. Further, these two exponential sums have very similar properties. Indeed, they have the same value distribution by Lemma 4, and a similar result as Lemma 5 (4) also holds for the corresponding exponential sum in [11] although hasn't been proved mathematically (by the property 4 listed in Lemma 5, the proof of the following Theorem 1 is more simple than that in [11]). This is the reason why the families $\mathcal{F}_1$ and $\mathcal{S}$ have the same correlation distribution.

Theorem 1 *The family $\mathcal{F}_1$ has correlation distribution as*

$$R_{s_i,s_j}(\tau) = \begin{cases} 4(2^n-1), & 2^n \text{ times}, \\ -4, & 2^n(2^n-1) \text{ times}, \\ 0, & 2^{2n}(2^{n+1}-1) \text{ times}, \\ -4 \pm 2^{\frac{n+3}{2}}, & 2^n(2^n-2)(2^{n-1} \pm 2^{\frac{n-1}{2}}) \text{ times}, \\ \pm 2^{\frac{n+3}{2}}\omega, & 2^{2n}(2^{n-1}-1) \text{ times (each)}. \end{cases} \tag{16}$$

Proof For each τ with $0 \leq \tau < 4(2^n-1)$, we write $\tau = 4\tau_0 + l$ where $0 \leq \tau_0 < 2^n - 1$ and $0 \leq l < 4$.

A direct calculation shows that the correlation function between the sequences s_i and s_j in $\mathcal{F}_1$ is given by

$$R_{s_i,s_j}(\tau) = \begin{cases} \xi(\eta_i,\eta_j,\delta) + \xi(\eta_i+1,\eta_j+1,\delta) + \xi(\eta_i+1,\eta_j+1,\delta) + \xi(\eta_i,\eta_j,\delta) - 4, & l = 0, \\ \xi(\eta_i,\eta_j+1,\delta) + \xi(\eta_i+1,\eta_j+1,\delta) + \xi(\eta_i+1,\eta_j,\delta) - \xi(\eta_i,\eta_j,\delta), & l = 1, \\ \xi(\eta_i,\eta_j+1,\delta) + \xi(\eta_i+1,\eta_j,\delta) - \xi(\eta_i+1,\eta_j,\delta) + \xi(\eta_i,\eta_j+1,\delta), & l = 2, \\ -\xi(\eta_i,\eta_j,\delta) - \xi(\eta_i+1,\eta_j,\delta) + \xi(\eta_i+1,\eta_j+1,\delta) + \xi(\eta_i,\eta_j+1,\delta), & l = 3 \end{cases} \tag{17}$$

where $\delta = \beta^{\tau_0+l/4}$.

The analysis of the value distribution of $R_{s_i,s_j}(\tau)$ in $\mathcal{F}_1$ can be divided into two cases: **Case 1**: $l \in \{1, 3\}$ and $\delta = 1$, or $l \in \{0, 2\}$; **Case 2**: $l \in \{1, 3\}$ and $\delta \neq 1$.

The analysis of Case 1 is similar as that of cases i-iv in the proof of Theorem 1 in [11]. Further, for Case 1, the value distribution of $R_{s_i,s_j}(\tau)$ is the same as that of $R_{s_i',s_j'}(\tau)$ for cases i-iv in the proof of Theorem 1 in [11], so we omit it here.

The value distribution of $R_{s_i,s_j}(\tau)$ for Case 2 is investigated in what follows.

When $l \in \{1, 3\}$ and $\delta \neq 1$, by (17) and (14), one has

$$R_{s_i,s_j}(\tau) = \begin{cases} -\kappa(\eta_i, \eta_j, \delta) - \kappa(\eta_i, \eta_j + 1, \delta), & \text{if } l = 1, \\ \kappa(\eta_i, \eta_j, \delta) + \kappa(\eta_i, \eta_j + 1, \delta), & \text{if } l = 3. \end{cases} \tag{18}$$

In the following, for $l \in \{1, 3\}$, the distribution of the pair $(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$ is discussed when $i,\ j$ vary from 0 to $2^n - 1$ and δ runs through $\mathcal{T}\backslash\{0, 1\}$.

In the case of $l = 1$, by Lemma 5 (4) the pair $(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$ may take at most 4 values as in Table 1.

In the case of $l = 3$, we have that the pair $(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$ has the same distribution with $(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$ as in the case of $l = 1$, whose distribution is given by Table 2.

By Lemma 5 (4) and Table 1, one has $x_1 + x_3 = x_2 + x_4 = 2^{2n-1}(2^n - 2)$.

From Tables 1, 2 and (18), we have the value distribution of the multi-set

$$\left\{R_{s_i,s_j}(\tau) : 0 \leq i, j < 2^n, l \in \{1, 3\}, \delta \in \mathcal{T}\backslash\{0, 1\}\right\}$$

as

$$R_{s_i,s_j}(\tau) = \begin{cases} 0, & 2^{2n}(2^n - 2) \text{ times}, \\ \pm 2^{\frac{n+3}{2}}\omega, & 2^{2n-1}(2^n - 2) \text{ times (each)}. \end{cases}$$

Thus, the correlation distribution of $\mathcal{F}_1$ is completely determined as (16). This finishes the proof. □

Table 1 The distribution of $(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$ when $l = 1$

$(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$	$-\kappa(\eta_i, \eta_j, \delta) - \kappa(\eta_i, \eta_j + 1, \delta)$	Frequency
$(2^{\frac{n+1}{2}}\omega, 2^{\frac{n+1}{2}}\omega)$	$-2^{\frac{n+3}{2}}\omega$	x_1
$(-2^{\frac{n+1}{2}}\omega, -2^{\frac{n+1}{2}}\omega)$	$2^{\frac{n+3}{2}}\omega$	x_2
$(2^{\frac{n+1}{2}}\omega, -2^{\frac{n+1}{2}}\omega)$	0	x_3
$(-2^{\frac{n+1}{2}}\omega, 2^{\frac{n+1}{2}}\omega)$	0	x_4

Table 2 The distribution of $(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$ when $l = 3$

$(\kappa(\eta_i, \eta_j, \delta), \kappa(\eta_i, \eta_j + 1, \delta))$	$-\kappa(\eta_i, \eta_j, \delta) + \kappa(\eta_i, \eta_j + 1, \delta)$	Frequency
$(2^{\frac{n+1}{2}}\omega, 2^{\frac{n+1}{2}}\omega)$	0	x_1
$(-2^{\frac{n+1}{2}}\omega, -2^{\frac{n+1}{2}}\omega)$	0	x_2
$(2^{\frac{n+1}{2}}\omega, -2^{\frac{n+1}{2}}\omega)$	$-2^{\frac{n+3}{2}}\omega$	x_3
$(-2^{\frac{n+1}{2}}\omega, 2^{\frac{n+1}{2}}\omega)$	$2^{\frac{n+3}{2}}\omega$	x_4

4.2 Linear spans of the sequences in $\mathcal{F}_1$

By Definition 2, for each i with $0 \le i \le 2^n-1$, the sequence s_i in $\mathcal{F}_1$ can be written as

$$
\begin{aligned}
s_i(t) &= \begin{cases} \mathrm{Tr}_1^n\left((1+2\eta_i)\beta^{t_0}\right)+2P\left(\lambda\beta^{t_0}\right)+2, & t=4t_0,\\ \mathrm{Tr}_1^n\left([1+2(\eta_i+1)]\beta^{t_0+1/4}\right)+2P\left(\lambda\beta^{t_0+1/4}\right), & t=4t_0+1,\\ \mathrm{Tr}_1^n\left([1+2(\eta_i+1)]\beta^{t_0+2/4}\right)+2P\left(\lambda\beta^{t_0+2/4}\right), & t=4t_0+2,\\ \mathrm{Tr}_1^n\left((1+2\eta_i)\beta^{t_0+3/4}\right)+2P\left(\lambda\beta^{t_0+3/4}\right), & t=4t_0+3 \end{cases}\\
&= \begin{cases} \mathrm{Tr}_1^n\left(\beta^{t_0}\right)+2\mathrm{Tr}_1^n\left(\eta_i\beta^{t_0}\right)+2P\left(\lambda\beta^{t_0}\right)+2, & t=4t_0,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+1/4}\right)+2\mathrm{Tr}_1^n\left(\left(\eta_i+1\right)\beta^{t_0+1/4}\right)+2P\left(\lambda\beta^{t_0+1/4}\right), & t=4t_0+1,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+2/4}\right)+2\mathrm{Tr}_1^n\left(\left(\eta_i+1\right)\beta^{t_0+2/4}\right)+2P\left(\lambda\beta^{t_0+2/4}\right), & t=4t_0+2,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+3/4}\right)+2\mathrm{Tr}_1^n\left(\eta_i\beta^{t_0+3/4}\right)+2P\left(\lambda\beta^{t_0+3/4}\right), & t=4t_0+3 \end{cases}\\
&= \begin{cases} \mathrm{Tr}_1^n\left(\beta^{t_0}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0}\right)+2\overline{P\left(\lambda\beta^{t_0}\right)}+2, & t=4t_0,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+1/4}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0+1/4}\right)+2\mathrm{tr}_1^n\left(\alpha^{t_0+1/4}\right)+2\overline{P\left(\lambda\beta^{t_0+1/4}\right)}, & t=4t_0+1,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+2/4}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0+2/4}\right)+2\mathrm{tr}_1^n\left(\alpha^{t_0+2/4}\right)+2\overline{P\left(\lambda\beta^{t_0+2/4}\right)}, & t=4t_0+2,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+3/4}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0+3/4}\right)+2\overline{P\left(\lambda\beta^{t_0+3/4}\right)}, & t=4t_0+3 \end{cases}
\end{aligned}
$$

by properties P1, P2 of Sect. 2.1 and the equality $2\mathrm{Tr}_1^n(x)=2\mathrm{tr}_1^n(\overline{x})$ holds in $\mathbf{Z}_4$ for $x\in\mathbf{R}$.

Let $u_i=\{u_i(t)\}_{t=0}^{4(2^n-1)-1}$ be given by

$$
\begin{aligned}
u_i(t) &= \begin{cases} \mathrm{Tr}_1^n\left(\beta^{t_0}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0}\right), & t=4t_0,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+1/4}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0+1/4}\right), & t=4t_0+1,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+2/4}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0+2/4}\right), & t=4t_0+2,\\ \mathrm{Tr}_1^n\left(\beta^{t_0+3/4}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t_0+3/4}\right), & t=4t_0+3 \end{cases}\\
&= \mathrm{Tr}_1^n\left(\beta^{\frac{t}{4}}\right)+2\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{\frac{t}{4}}\right),
\end{aligned}
\tag{19}
$$

$q_1=\{q_1(t)\}_{t=0}^{4(2^n-1)-1}$ be given by

$$
\begin{aligned}
q_1(t) &= \begin{cases} \overline{P\left(\lambda\beta^{t_0}\right)}, & t=4t_0,\\ \overline{P\left(\lambda\beta^{t_0+1/4}\right)}, & t=4t_0+1,\\ \overline{P\left(\lambda\beta^{t_0+2/4}\right)}, & t=4t_0+2,\\ \overline{P\left(\lambda\beta^{t_0+3/4}\right)}, & t=4t_0+3 \end{cases}\\
&= \overline{P\left(\lambda\beta^{\frac{t}{4}}\right)},
\end{aligned}
\tag{20}
$$

$q_2=\{q_2(t)\}_{t=0}^{4(2^n-1)-1}$ be given by

$$
q_2(t)=\begin{cases} 1, & t\equiv 0 \bmod 4,\\ 0, & \text{otherwise} \end{cases}
\tag{21}
$$

and $r=\{r(t)\}_{t=0}^{4(2^n-1)-1}$ be given by

$$
r(t)=\begin{cases} 0, & t=4t_0,\\ \mathrm{tr}_1^n\left(\alpha^{t_0+1/4}\right), & t=4t_0+1,\\ \mathrm{tr}_1^n\left(\alpha^{t_0+2/4}\right), & t=4t_0+2,\\ 0, & t=4t_0+3. \end{cases}
\tag{22}
$$

Then for each i with $0\le i\le 2^n-1$, the sequence s_i in the family $\mathcal{F}_1$ can be decomposed as

$$
s_i=u_i+2q_1+2q_2+2r. \tag{23}
$$

Let $H(x)$ be a minimal polynomial of β over $\mathbf{Z}_4$, then $H(\beta) = 0$. Let $h(x) = \overline{H}(x)$ and then $h(\alpha) = 0$. Thus $h(x)$ is the minimal polynomial of α over $\mathbf{F}_2$. We have that $H(x)$ is a minimal polynomial of the sequence $\left\{\mathrm{Tr}_1^n\left(\beta^{t/4}\right)\right\}_{t=0}^{4(2^n-1)-1} = \left\{\mathrm{Tr}_1^n\left(\beta^{t}\right)\right\}_{t=0}^{4(2^n-1)-1}$ due to the fact $\mathrm{Tr}_1^n(\beta) = \mathrm{Tr}_1^n(\beta^2)$, and $h(x)$ is the minimal polynomial of the sequence $\left\{\mathrm{tr}_1^n\left(\overline{\eta_i}\alpha^{t/4}\right)\right\}_{t=0}^{4(2^n-1)-1}$. Thus, $H(L)(u_i) = \mathbf{0}$, which implies $H(x)$ is a characteristic polynomial of u_i. Let $H'(x)$ be a minimal polynomial of u_i, then $H'(L)(u_i) = \mathbf{0}$, and $\overline{H'}(L)(\overline{u_i}) = \mathbf{0}$. Since $h(x)$ is the minimal polynomial of $\overline{u_i}$, we have $h(x)|\overline{H'}(x)$. This implies $\deg(H'(x)) \geq n$. Therefore $H(x)$ is a minimal polynomial of the sequence u_i. Further, it can be verified that the minimal polynomial of q_2 is $x^4 - 1$.

Lemma 6 *The minimal polynomial of the sequence r defined by (22) is $h(x)^3$.*

Proof Set $\delta_{4j} = \delta_{4j+3} = 0$ and $\delta_{4j+1} = \delta_{4j+2} = 1$ for integers j. Then the sequence $r = \{r(t)\}_{t=0}^{4(2^n-1)-1}$ can be written as $r(t) = \mathrm{tr}_1^n\left(\delta_t\alpha^{t/4}\right) = \mathrm{tr}_1^n\left(\delta_t\alpha^{t}\right)$. Decompose the sequence r as $r = r^0 + r^1 + \cdots + r^{n-1}$, where $r^j = \left\{\delta_t\alpha^{t2^j}\right\}_{t=0}^{4(2^n-1)-1}$. For the first subsequence r^0, $(x-\alpha)^3 = x^3 + \alpha x^2 + \alpha^2 x + \alpha^3$ is its characteristic polynomial since the action of $L^3 + \alpha L^2 + \alpha^2 L + \alpha^3$ on r^0 is the sequence $\{s(t)\}_{t=0}^{4(2^n-1)-1}$, where

$$s(t) = \left(\delta_{t+3} + \delta_{t+2} + \delta_{t+1} + \delta_t\right)\alpha^{t+3} = 2\alpha^{t+3} = 0.$$

On the other hand, $(x-\alpha)^2 = x^2+\alpha^2$ is not a characteristic polynomial of r^0 since the action of $L^2 + \alpha^2$ on r^0 is the sequence $\left\{\left(\delta_{t+2} + \delta_t\right)\alpha^{t+2}\right\}_{t=0}^{4(2^n-1)-1} = \left\{\alpha^{t+2}\right\}_{t=0}^{4(2^n-1)-1}$, which is not the zero sequence. Therefore, $(x-\alpha)^3$ is the minimal polynomial of the sequence r^0. Similarly, $\left(x-\alpha^{2^j}\right)^3$ is the minimal polynomial of the sequence r^j. Since the $\left(x-\alpha^{2^j}\right)^3$ are coprime for each pair of different j, $h(x)^3 = \prod_{j=0}^{n-1}\left(x-\alpha^{2^j}\right)^3$ is the minimal polynomial of the sequence $r = r^0 + r^1 + \cdots + r^{n-1}$. This finishes the proof. □

By property P1 of Sect. 2.1 and (20), we have

$$q_1(t) = \overline{P(\lambda\beta^{\frac{t}{4}})} = \sum_{j=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left(\left(\overline{\lambda}\alpha^{t/4}\right)^{2^{kj}+1}\right) = \sum_{j=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left(\left(\overline{\lambda}^4\alpha^{t}\right)^{2^{kj}+1}\right) = \sum_{j=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left(\overline{\lambda}^8\alpha^{(2^{kj}+1)t}\right).$$

Then by a similar analysis as in Theorem 7 of [8], we have the following result.

Lemma 7 *The minimal polynomial $m(x)$ of q_1 is $m(x) = m_1(x)m_2(x)\cdots m_{(m-1)/2}(x)$, where $m_i(x)$ is the minimal polynomial of $\alpha^{2^{ki}+1}$ and $\deg(m_i(x)) = n$ for $1 \leq i \leq (m-1)/2$.*

Lemma 8 *The linear span $LS(s_i)$ of each sequence s_i in the family $\mathcal{F}_1$ satisfies $LS(s_i) \leq \frac{n(n+3e)}{2e} + 4$.*

Proof Notice that $h^3(x)$ is the minimal polynomial of r, which implies $h(x)$ is the minimal polynomial of $h(L)^2(r)$. Since $h(x)$ is also the minimal polynomial of $\overline{u_i}$, we have that $h(L)^2(r)$ is a shift of $\overline{u_i}$, i.e., $h(L)^2 r = L^s(\overline{u_i})$ for some nonnegative integer s.

There exists a polynomial $\varphi(x) \in \mathbf{F}_2[x]$ with $\deg(\varphi(x)) < n$, such that $x^s \equiv \varphi(x) \bmod h(x)$, thus $\alpha^s = \varphi(\alpha)$, $L^s(\overline{u_i}) = \left\{\mathrm{tr}_1^n(\alpha^{t+s})\right\}_{t=0}^{4(2^n-1)-1} = \varphi(L)(\overline{u_i})$. Then a direct verification shows that $(H(L)^2 + 2\varphi(L))(u_i + 2r) = \mathbf{0}$, which implies $H(x)^2 + 2\varphi(x)$ is a characteristic polynomial of $u_i + 2r$.

By Lemmas 6, 7 and (23), we have that $(H(x)^2 + 2\varphi(x))m(x)(x^4 - 1)$ is a characteristic polynomial of s_i. Then $\mathrm{LS}(s_i) \le \frac{n(n+3e)}{2e} + 4$. This finishes the proof. □

Theorem 2 *The linear span of each sequence s_i in the family $\mathcal{F}_1$ is equal to $\frac{n(n+3e)}{2e} + 4$.*

Proof By Lemmas 6 and 7, we have $h^3(x)$ and $m(x)$ are the minimal polynomial of r and q_1, respectively. For $0 \le j \le (m-1)/2$, each $2^{kj} + 1$ lies in different cyclotomic cosets mod $2^n - 1$, so $\gcd(h(x), m(x)) = 1$. Since the minimal polynomial of q_2 is $x^4 - 1$, $\gcd(m(x), x^4 - 1) = 1$ and $\gcd(h^3(x), x^4 - 1) = 1$, we have $h^3(x)m(x)(x^4 - 1)$ is the minimal polynomial of $q_1 + q_2 + r$. Recall that $H(x)$ is a minimal polynomial of u_i, and let

$$\begin{aligned} d_1 &= \gcd(\overline{H}(x), h^3(x)m(x)(x^4 - 1)) = h(x), \\ d_2 &= \gcd(d_1, h^3(x)m(x)(x^4 - 1)/d_1(x)) = h(x). \end{aligned}$$

By Lemma 2 and (23), we have

$$\begin{aligned} \mathrm{LS}(s_i) &\ge \deg(H(x)) + \deg(h^3(x)m(x)(x^4 - 1)) - \deg(h(x)) - \deg(h(x)) \\ &= \frac{n(n+3e)}{2e} + 4. \end{aligned} \tag{24}$$

By Lemma 8 and (24) we get the desired result. This finishes the proof. □

4.3 An example

For $m = e = 3$, $k = 6$ and $n = 9$, we use the primitive basic irreducible polynomial $f(x) = x^9 + 3x^8 + 2x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 3$ in $\mathbf{Z}_4[x]$ to generate the Galois ring $\mathbf{R} = \mathrm{GR}(4, 9)$, and choose the generator β of the cyclic group $\mathcal{T}\backslash\{0\}$ in $\mathbf{R}$ such that $f(\beta) = 0$. With the help of a computer, the family $\mathcal{F}_1$ can be verified to have the correlation distribution as

$$R_{s_i,s_j}(\tau) = \begin{cases} 2044, & 512 \text{ times}, \\ -4, & 261632 \text{ times}, \\ 0, & 268173312 \text{ times}, \\ -68, & 62668800 \text{ times}, \\ 60, & 71024640 \text{ times}, \\ \pm 64\omega, & 66846720 \text{ times (each)} \end{cases}$$

when $v_0 = v_3 = 0$, $v_1 = v_2 = 1$ and $\lambda = \beta^{73}$, which is consistent with Theorem 1.

It can also be verified that the linear span of each sequence in $\mathcal{F}_1$ is equal to 31, which is consistent with Theorem 2.

5 The correlation distribution and linear span of $\mathcal{F}_2$

In this section, the correlation distribution and linear span of $\mathcal{F}_2$ are studied.

5.1 Correlation distribution of the family $\mathcal{F}_2$

Theorem 3 *The family $\mathcal{F}_2$ has the following correlation distribution.*

(1) When n is odd and $v = 1$, the correlation function of $\mathcal{F}_2$ takes values

$$R_{s_i,s_j}(\tau) = \begin{cases} 4(2^n-1), & 2^n \text{ times,} \\ -4, & 2^n(2^n-1) \text{ times,} \\ 0, & 2^{2n}(2^{n+1}-1) \text{ times,} \\ -4 \pm 2^{\frac{n+3}{2}}, & 2^n(2^n-2)(2^{n-1} \pm 2^{\frac{n-1}{2}}) \text{ times,} \\ \pm 2^{\frac{n+3}{2}}\omega, & 2^{2n-1}(2^n-2) \text{ times (each).} \end{cases}$$

(2) When n is odd and $v \neq 1$, the correlation function of $\mathcal{F}_2$ takes values

$$R_{s_i,s_j}(\tau) = \begin{cases} 4(2^n-1), & 2^n \text{ times,} \\ -4, & 2^n(2^n-1) \text{ times,} \\ 0, & 2^{2n}(2^{n+1}-1) \text{ times,} \\ -4 \pm 2^{\frac{n+3}{2}}, & 2^n(2^n-2)(2^{n-2} \pm 2^{\frac{n-1}{2}}) \text{ times,} \\ -4 \pm 2^{\frac{n+3}{2}}\omega, & 2^{2n-2}(2^n-2) \text{ times (each),} \\ \pm 2^{\frac{n+3}{2}}, & 2^{2n-2}(2^n-2) \text{ times (each),} \\ \pm 2^{\frac{n+3}{2}}\omega, & 2^{2n-2}(2^n-2) \text{ times (each).} \end{cases}$$

(3) When n is even and $v \neq 1$, the correlation function of $\mathcal{F}_2$ takes values

$$R_{s_i,s_j}(\tau) = \begin{cases} 4(2^n-1), & 2^n \text{ times,} \\ -4, & 2^n(2^n-1) \text{ times,} \\ 0, & 2^{2n}(2^{n+1}-1) \text{ times,} \\ -4 + 2^{\frac{n}{2}+1} \pm 2^{\frac{n}{2}+1}\omega, & 2^n(2^n-2)(2^{n-2} + 2^{\frac{n-2}{2}}) \text{ times (each),} \\ -4 - 2^{\frac{n}{2}+1} \pm 2^{\frac{n}{2}+1}\omega, & 2^n(2^n-2)(2^{n-2} - 2^{\frac{n-2}{2}}) \text{ times (each),} \\ 2^{\frac{n}{2}+1} \pm 2^{\frac{n}{2}+1}\omega, & 2^{2n-2}(2^n-2) \text{ times (each),} \\ -2^{\frac{n}{2}+1} \pm 2^{\frac{n}{2}+1}\omega, & 2^{2n-2}(2^n-2) \text{ times (each).} \end{cases}$$

Proof The correlation function between the sequences s_i and s_j in $\mathcal{F}_2$ is given by

$$R_{s_i,s_j}(\tau) = \begin{cases} \xi(\eta_i,\eta_j,\delta) + \xi(\eta_i+v,\eta_j+v,\delta) + \xi(\eta_i,\eta_j,\delta) + \xi(\eta_i+v,\eta_j+v,\delta) - 4, & l = 0, \\ \xi(\eta_i,\eta_j+v,\delta) + \xi(\eta_i+v,\eta_j,\delta) + \xi(\eta_i,\eta_j+v,\delta) - \xi(\eta_i+v,\eta_j,\delta), & l = 1, \\ \xi(\eta_i,\eta_j,\delta) + \xi(\eta_i+v,\eta_j+v,\delta) - \xi(\eta_i,\eta_j,\delta) + \xi(\eta_i+v,\eta_j+v,\delta), & l = 2, \\ -\xi(\eta_i,\eta_j+v,\delta) - \xi(\eta_i+v,\eta_j,\delta) + \xi(\eta_i,\eta_j+v,\delta) + \xi(\eta_i+v,\eta_j,\delta), & l = 3. \end{cases} \tag{25}$$

By considering the following five cases, the correlation distribution of $\mathcal{F}_2$ will be determined.

Case 1: When $l = 0$ and $\delta = 1$, we have $\tau_0 = 0$.
By (12) and (25), we have

$$R_{s_i,s_j}(\tau) = \begin{cases} 4(2^n-1), & 2^n \text{ times,} \\ -4, & 2^n(2^n-1) \text{ times} \end{cases}$$

as i and j vary from 0 to $2^n - 1$.

Case 2: When $l = 2$ and $\delta = 1$, $R_{s_i,s_j}(\tau) = 2[-\xi(\eta_i,\eta_j,1) + \xi(\eta_i+v,\eta_j+v,1)] = 0$ occurs 2^{2n} times as i, j vary from 0 to $2^n - 1$.

Case 3: When $l \in \{1,3\}$, by (25), $R_{s_i,s_j}(\tau) = 0$ occurs $2^{2n}(2^n-1)$ times as i, j vary from 0 to $2^n - 1$, and τ_0 varies from 0 to $2^n - 2$.

Case 4: When $l = 0$ and $\delta \neq 1$, by (25) we have

$$R_{s_i,s_j}(\tau) = 2[\xi(\eta_i, \eta_j, \delta) + \xi(\eta_i + v, \eta_j + v, \delta)] - 4 = 2\varsigma(\eta_i, \eta_j, \delta) - 4.$$

Case 5: When $l = 2$ and $\delta \neq 1$, by (25) we have

$$R_{s_i,s_j}(\tau) = 2[-\xi(\eta_i, \eta_j, \delta) + \xi(\eta_i + v, \eta_j + v, \delta)] = -2\kappa(\eta_i, \eta_j, \delta).$$

Combining the above five cases, and by Lemma 5, we can get the desired result. This finishes the proof. □

5.2 Linear spans of the sequences in $\mathcal{F}_2$

We will determine the linear spans of the sequences in $\mathcal{F}_2$.

Let $u'_i = \{u'_i(t)\}_{t=0}^{4(2^n-1)-1}$ be given by

$$u'_i(t) = \begin{cases} \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_0)]\beta^{t_0}\right), & t = 4t_0, \\ \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_1)]\beta^{t_0+1/4}\right), & t = 4t_0 + 1, \\ \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_2)]\beta^{t_0+2/4}\right), & t = 4t_0 + 2, \\ \mathrm{Tr}_1^n\left([1 + 2(\eta_i + v_3)]\beta^{t_0+3/4}\right), & t = 4t_0 + 3 \end{cases} \tag{26}$$

for $0 \leq i \leq 2^n - 1$.

Then for each i with $0 \leq i \leq 2^n - 1$, the sequence s_i can be written as

$$s_i = u'_i + 2q_1 + 2q_2$$

where q_1 and q_2 are defined by (20) and (21), respectively.

Theorem 4 *The linear span $LS(s_i)$ of s_i in $\mathcal{F}_2$ is equal to $\frac{n(n+e)}{2e} + 4$ for each i with $0 \leq i \leq 2^n - 1$.*

Proof Let $\gamma = (1 + 2v)\beta^{1/4}$, then one can verify that u'_i can be rewritten as

$$u'_i = \mathrm{Tr}_1^n\left((1 + 2\eta_i)\,\gamma^t\right)$$

due to the fact that $v_0 = v_2 = 0$ and $v_0 = v_2 = v$.

Suppose that $f(x) \in \mathbf{Z}_4[x]$ is a minimal polynomial of u'_i. By a similar analysis as in Theorem 7 of [8], we have that $\deg(f) = n$ and $g(x) = \overline{f}(x)$ is the minimal polynomial of $\overline{u'}_i$. Lemma 7 shows that $m(x)$ is the minimal polynomial of q_1. Notice that $x^4 - 1$ is the minimal polynomial of q_2. The above analysis together with $\gcd(g(x), x^4 - 1) = 1$, $\gcd(g(x), m(x)) = 1$ and Lemma 2 imply that $f(x)m(x)(x^4 - 1)$ is a minimal polynomial of s_i. Therefore the linear span of s_i is equal to $\frac{n(n+e)}{2e} + 4$. This finishes the proof. □

5.3 An example

For $e = k = 2$, $m = 3$ and $n = 6$, we use the primitive basic irreducible polynomial $f(x) = x^6 + 3x^5 + 2x^3 + 1$ in $\mathbf{Z}_4[x]$ to generate the Galois ring $\mathbf{R} = \mathrm{GR}(4, 6)$, and choose the generator β of the cyclic group $\mathcal{T}\backslash\{0\}$ in $\mathbf{R}$ such that $f(\beta) = 0$. With the help of a

computer, $\mathcal{F}_2$ can be verified to have the correlation distribution as

$$R_{s_i,s_j}(\tau) = \begin{cases} 252, & 64 \text{ times}, \\ -4, & 4032 \text{ times}, \\ 0, & 520192 \text{ times}, \\ 12 \pm 16\omega, & 79360 \text{ times (each)}, \\ -20 \pm 16\omega, & 47616 \text{ times (each)}, \\ \pm 16 \pm 16\omega, & 63488 \text{ times (each)} \end{cases}$$

when $v_0 = v_2 = 0$, $v_1 = v_3 = v = \beta^{21}$ and $\lambda = \beta^{42}$, which is consistent with Theorem 3. And it can also be verified that the linear span of each sequence in $\mathcal{F}_2$ is equal to 16, which is consistent with Theorem 4.

6 Conclusion

In this paper, based on the constructions of a quadriphase sequence family in [8] and a binary sequence family in [7], a new family of quadriphase sequences of period $4(2^n - 1)$ has been presented for $n = me$, where m is an odd integer. The correlation distribution and linear span of the new family are determined under two situations. The maximum nontrivial correlation magnitude $R_{\max}$ is upper bounded by $4 + 2^{\frac{n+3}{2}}$.

Acknowledgments The authors would like to thank the two anonymous reviewers for their helpful comments, which have improved the presentation of this paper. The work of X. Zeng was supported by the National Science Foundation of China (NSFC) under Grant 61170257. The work of X. Tang was supported in part by NSFC under Grant 61171095.

References

1. Boztas S., Hammons R., Kumar P.V.: 4-phase sequences with near-optimum correlation properties. IEEE Trans. Inf. Theory **38**(3), 1103–1113 (1992).
2. Boztas S., Kumar P.V.: Binary sequences with Gold-like correlation but larger linear span. IEEE Trans. Inf. Theory **40**(2), 532–537 (1994).
3. Brown E.H.: Generalizations of the Kervaire invariant. Ann. Math. **95**(2), 368–383 (1972).
4. Gold R.: Maximal recursive sequences with 3-valued cross-correlation functions. IEEE Trans. Inf. Theory **14**(1), 154–156 (1968).
5. Golomb S.W., Gong G.: Signal Design for Good Correlation—for Wireless Communication, Cryptography and Radar. Cambridge University Press, Cambridge (2005).
6. Helleseth T., Kumar P.V.: Sequences with low correlation. In: Pless V., Huffman C. (eds.) Handbook of Coding Theory. Elsevier, Amsterdam (1998).
7. Jiang W.F., Hu L., Tang X.H., Zeng X.Y.: New family of binary sequences of period $4(2^n - 1)$ with low correlation. Appl. Algebr. Eng. Commun. Comput. **19**(5), 429–439 (2008).
8. Jiang W.F., Hu L., Tang X.H., Zeng X.Y.: New optimal quadriphase sequences with larger linear span. IEEE Trans. Inf. Theory **55**(1), 458–470 (2009).
9. Kasami T.: Weight distribution of Bose-Chaudhuri-Hocquenghem codes. In: Bose R.C., Dowling T.A. (eds.) Combinatorial Mathematics and Its Applications, pp. 335–357. University of North Carolina Press, Chapel Hill (1969).
10. Li N., Tang X.H., Zeng X.Y., Hu L.: On the correlation distributions of the optimal quaternary sequence family $\mathcal{U}$ and the optimal binary sequence family $\mathcal{V}$. IEEE Trans. Inf. Theory **57**(6), 3815–3824 (2011).
11. Li J., Zeng X.Y., Hu L.: A new family of quadriphase sequences with low correlation. In: Lecture Notes in Computer Science, vol. 6639, pp. 246–262 (2011).
12. Sarwate D.V., Pursley M.B.: Crosscorrelation properties of pseudorandom and related sequences. Proc. IEEE **68**, 593–619 (1980).

13. Schmidt K.-U.: $\mathbf{Z}_4$-valued quadratic forms and quaternary sequences families. IEEE Trans. Inf. Theory **42**(2), 579–592 (2009).
14. Solé P.: A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties. In: Lecture Notes in Computer Science, vol. 388, pp. 193–201 (1989).
15. Tang X.H., Udaya P., Fan P.Z.: Quadriphase sequences obtained from binary quadratic form sequences. In: Lecture Notes in Computer Science vol. 3486, pp. 243–254 (2005).
16. Tang X.H., Udaya, P.: A note on the optimal quadriphase sequences families. IEEE Trans. Inform. Theory **53**(1), 433–436 (2007).
17. Tang X.H., Helleseth T., Fan P.Z.: A new optimal quaternary sequence family of length $2(2^n - 1)$ obtained from the orthogonal transformation of families $\mathcal{B}$ and $\mathcal{C}$. Des. Codes Cryptogr. **53**(3), 137–148 (2009).
18. Udaya P., Siddiqi M.U.: Optimal and suboptimal quadriphase sequences derived from maximal length sequences over $\mathbf{Z}_4$. Appl. Algebr. Eng. Commun. Comput. **9**(2), 161–191 (1998).
19. Zeng X.Y., Liu J.Q., Hu L.: Generalized Kasami sequences: the large set. IEEE Trans. Inf. Theory **53**(7), 2587–2598 (2007).