Article
http://justc.ustc.edu.cn Received: November 11, 2021; Accepted: March 09, 2022

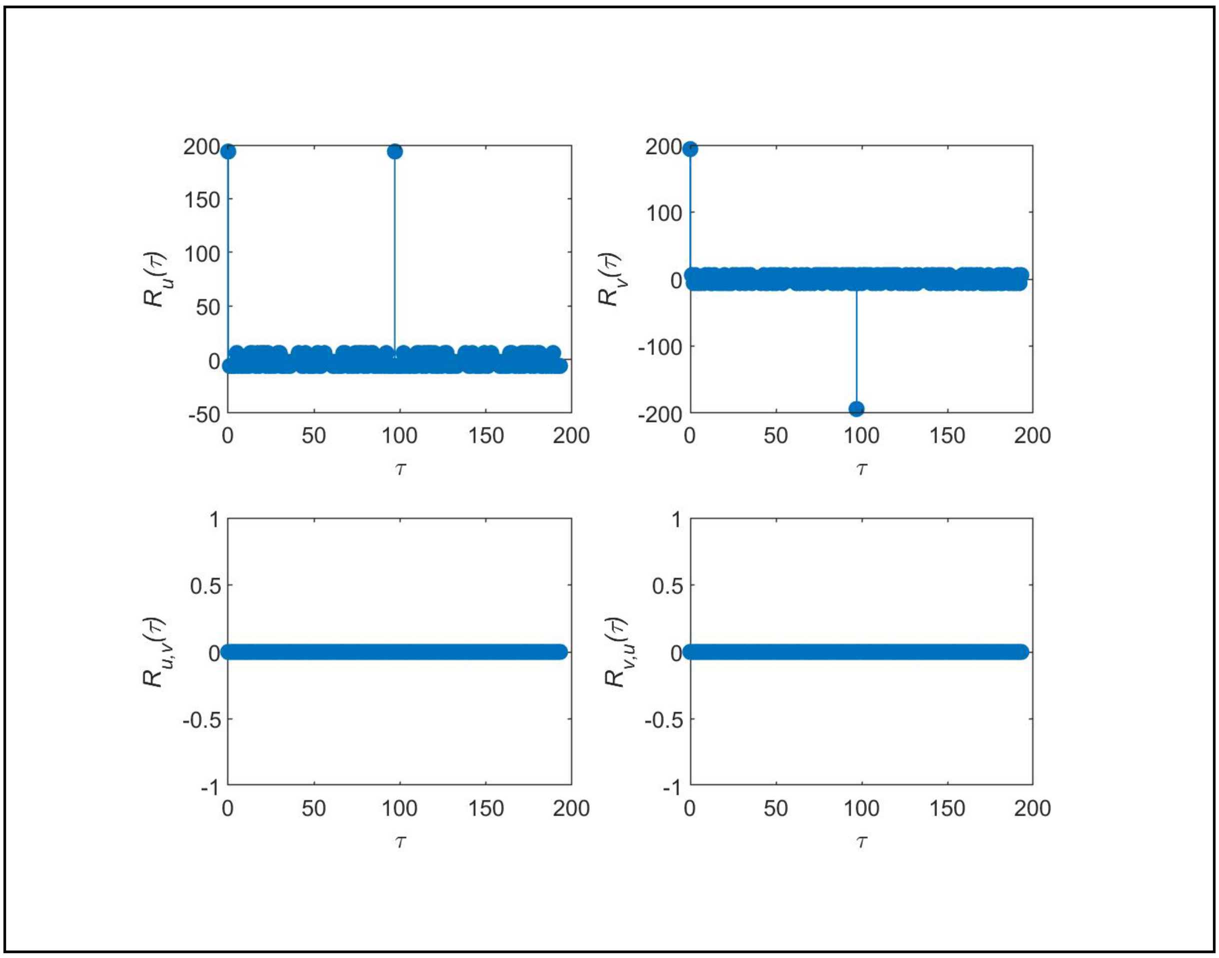
Almost balanced and uncorrelated quaternary sequence pairs of even length

Yi Ouyang[1], Sen Wang[1] ✉, and Xianhong Xie[2]

[1]Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China;
[2]Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei 230027, China

✉Correspondence: Sen Wang, E-mail: senwang11@163.com

Graphical abstract



The autocorrelation $R_u(\tau), R_v(\tau)$ and cross-correlation $R_{u,v}(\tau), R_{v,u}(\tau)$ of sequence pair (u, v).

Public summary

■ Given a partition of $\mathbb{Z}_N^*$ into four subsets, a generic construction of uncorrelated quaternary sequence pairs of length $2N$ was proposed.

■ Choose the partition of $\mathbb{Z}_N^*$ from cyclotomic classes of order 4 and 8. The sequence pairs obtained are uncorrelated, almost balanced and with low autocorrelation, except at a few positions.

Citation: Ouyang Y, Wang S, Xie X H. Almost balanced and uncorrelated quaternary sequence pairs of even length. *JUSTC*, **2022**, 52(3): 4. DOI: 10.52396/JUSTC-2021-0234

Article
http://justc.ustc.edu.cn
Received: November 11, 2021; Accepted: March 09, 2022

Almost balanced and uncorrelated quaternary sequence pairs of even length

Yi Ouyang[1], Sen Wang[1] ✉, and Xianhong Xie[2]

[1]Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China;
[2]Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei 230027, China

✉Correspondence: Sen Wang, E-mail: senwang11@163.com

Cite This: *JUSTC*, **2022**, 52(3): 4 (7pp)   Read Online

Abstract: Given a partition of $\mathbb{Z}_N^*$ into four subsets, we present a generic construction of uncorrelated quaternary sequence pairs of length $2N$ using the interleaved technique based on this partition. By choosing partitions arising from cyclotomic classes of order 4 and 8 over $\mathbb{Z}_p$, we construct uncorrelated quaternary sequence pairs of length $2p$, which are almost balanced and have low autocorrelation, except at a few positions.

Keywords: quaternary sequence pair; interleaved technique; cyclotomic class

CLC number: O236.2 **Document code:** A

2020 Mathematics Subject Classification: 94A55; 94A60

1 Introduction

Sequences and sequence pairs that are optimally autocorrelated, largely complex, and balanced are important in many applications, such as measurement, digital communication, and continuous-wave radar[1−3]. In recent years, owing to their simple implementation, they have an amount of attention. Sequences and sequence pairs with low correlation can be generalized to quasi-complementary sequence sets and a few weight codes. Luo et al. proposed three new constructions of asymptotically optimal periodic quasi-complementary sequence sets using new parameters and small alphabet sizes[4]. Shi et al. obtained a family of abelian binary five-weight codes using a Gray map[5]. Several studies have been conducted on binary sequence pairs[6−9]. In this study, we focus on quaternary sequence pairs.

Li et al. constructed quaternary sequences and sequence pairs using binary complete sequences and sequence pairs[10]. Peng et al. proposed quaternary sequence pairs with an even length and three-level correlation using inverse Gray mapping and two difference set pairs of the same modulus[11]. Yang et al. presented two lower bounds on the maximum cross-correlation magnitude of balanced quaternary sequence pairs with (almost) optimal autocorrelation, and constructed a balanced quaternary sequence pair whose autocorrelation and cross-correlation achieve the lower bound[12]. Zhou et al. presented two generic constructions of quaternary periodic complementary pairs[13]: first, using the known binary odd periodic complementary pairs and Gray mapping; and second, based on the product sequences of a known quaternary sequence and a perfect quaternary sequence.

The remainder of this paper is organized as follows. In Section 2, we introduce quaternary sequences and their correlations, partitions of $\mathbb{Z}_p$ by cyclotomic classes, and permutations of $\mathbb{Z}_4$. In Section 3, we describe the construction of an uncorrelated quaternary sequence pair. In Section 4, we present almost balanced and uncorrelated sequence pairs with low autocorrelation, except at a few positions, and provide some examples to illustrate this. Finally, we summarize this study in Section 5.

2 Preliminaries

2.1 Quaternary sequences and their correlations

Let $\mathbb{Z}_4=\{0,1,2,3\}$. A quaternary sequence is a sequence with the alphabet $\mathbb{Z}_4$. The periodic cross-correlation function between two quaternary sequences $a=(a(0), a(1), \cdots, a(N-1))$ and $b=(b(0), b(1), \cdots, b(N-1))$ of period N is the complex function:

$$R_{a,b}(\tau):=\sum_{t=0}^{N-1}\omega^{a(t)-b(t+\tau)}\quad(0\leqslant\tau<N) \tag{1}$$

where $\omega=\sqrt{-1}$, and after the addition, $t+\tau$ is taken as modulo N. We say that the sequence pair (a,b) is uncorrelated if $R_{a,b}(\tau)=0$ for $0\leqslant\tau<N$.

Suppose $G_i=\{i:a(t)=i\}, 0\leqslant i\leqslant 3$. For $i\neq j$, a is called balanced if $|G_i|-|G_j|=0$ and $4\mid N$, or $|G_i|-|G_j|=1$ and $4\nmid N$. a is called almost balanced if $|G_i|-|G_j|\leqslant 2$ for $i\neq j$.

Let $\{\alpha_0,\alpha_1,\cdots,\alpha_{M-1}\}$ be a sequence set that consists of M sequences of length N. An $N\times M$ matrix R is formed by placing the sequence α_i in the ith column, $0\leqslant i<M$, that is, $R=[\alpha_0,\alpha_1,\cdots,\alpha_{M-1}]$. The interleaved sequence u is the sequence concatenating the successive rows of matrix R, denoted as

$$u=I(\alpha_0, \alpha_1, \cdots, \alpha_{M-1}).$$

I is called the interleaving operator, and $\alpha_0, \alpha_1, \cdots, \alpha_{M-1}$ are called the column sequences of u.

Lemma 2.1. Suppose $u = I(\alpha_0, \alpha_1, \cdots, \alpha_{M-1})$ and $v = I(\beta_0, \beta_1, \cdots, \beta_{M-1})$. For $0 \leqslant \tau < MN$, we write $\tau = \tau' M + \tau''$, where $0 \leqslant \tau' < N$ and $0 \leqslant \tau'' < M$. The cross-correlation function between u and v is given by:

$$R_{u,v}(\tau) = \sum_{k=0}^{M-\tau''-1} R_{\alpha_k, \beta_{k+\tau''}}(\tau') + \sum_{k=M-\tau''}^{M-1} R_{\alpha_k, \beta_{k+\tau''-M}}(\tau'+1) \qquad (2)$$

2.2 Partitions of $\mathbb{Z}_p$ by cyclotomic classes

Recall that for a set X, a partition of X is a family of subsets $\{X_i\}_{i\in I}$ such that $\bigcup_i X_i = X$ and $X_i \cap X_j = \emptyset$ if $i \neq j$. Cyclotomic classes are typically used to obtain the partitions of $\mathbb{Z}_N$.

We first recall the definition[3] of cyclotomic classes over $\mathbb{Z}_p$.

Definition 2.1. Let p be an odd prime, $p-1 = ef$, and γ a generator of $\mathbb{Z}_p^*$. For $0 \leqslant l < e$, $D_l^{(e,p)} = \{\gamma^{l+ek} : 0 \leqslant k < f\}$ is the set of cyclotomic classes of order e over $\mathbb{Z}_p$. For $0 \leqslant l \neq l' < e$, the cyclotomic number

$$(l, l')_e^p = |(D_l^{(e,p)} + 1) \cap D_{l'}^{(e,p)}|.$$

We drop e and p from the notation when they are implied by the context. We let $D_e = D_e^{(e,p)} = \{0\}$.

Cyclotomic classes give partitions of $\mathbb{Z}_p^*$ and $\mathbb{Z}_p$:

$$\mathbb{Z}_p^* = \bigcup_{l=0}^{e-1} D_l^{(e,p)}, \quad \mathbb{Z}_p = \bigcup_{l=0}^{e} D_l^{(e,p)}.$$

Lemma 2.2. [3] Suppose $p-1 = ef$, $0 \leqslant l \neq l' < e$, then

$$(l, l') = \begin{cases} (l', l), & \text{if } f \text{ is even;} \\ \left(l' + \dfrac{e}{2}, l + \dfrac{e}{2}\right), & \text{if } f \text{ is odd.} \end{cases}$$

We need the following information about cyclotomic numbers[3]:

(i) If $e = 4$, then $p = 4f + 1 = x^2 + 4y^2$ where $x \equiv 1 \pmod 4$ is unique and y is unique up to a certain point depending on the choice of γ. Table 1 lists the cyclotomic numbers of order four.

(ii) If $e = 8$, then $p = 8f + 1 = x^2 + 4y^2 = a^2 + 2b^2$ with a unique $x \equiv a \equiv 1 \pmod 4$. Table 2 lists the cyclotomic numbers of order eight when $p \equiv 1 \bmod 16$ (equivalently f is even).

2.3 Permutations of $\mathbb{Z}_4$

A permutation of $\mathbb{Z}_4$ is written as $\sigma = (\sigma(0), \sigma(1), \sigma(2), \sigma(3))$. It is well-known that 24 permutations of $\mathbb{Z}_4$ exist, which are ordered as follows:

Table 1. Cyclotomic numbers of order 4.

	f is even	f is odd
$16\times(0,0)$	$p-11-6x$	$p-7+2x$
$16\times(0,1)$	$p-3+2x+8y$	$p+1+2x-8y$
$16\times(0,2)$	$p-3+2x$	$p+1-6x$
$16\times(0,3)$	$p-3+2x-8y$	$p+1+2x+8y$
$16\times(1,1)$	$p-3+2x-8y$	$p-3-2x$
$16\times(1,2)$	$p+1-2x$	$p+1+2x+8y$

Table 2. Cyclotomic numbers of order 8 for $p \equiv 1 \bmod 16$.

	If 2 is a quartic residue	If 2 is not a quartic residue
$64\times(0,0)$	$p-23-18x-24a$	$p-23+6x$
$64\times(0,1)$	$p-7+2x+4a+16y+16b$	$p-7+2x+4a$
$64\times(0,2)$	$p-7+6x+16y$	$p-7-2x-8a-16y$
$64\times(0,3)$	$p-7+2x+4a-16y+16b$	$p-7+2x+4a$
$64\times(0,4)$	$p-7-2x+8a$	$p-7-10x$
$64\times(0,5)$	$p-7+2x+4a+16y-16b$	$p-7+2x+4a$
$64\times(0,6)$	$p-7+6x-16y$	$p-7-2x-8a+16y$
$64\times(0,7)$	$p-7+2x+4a-16y-16b$	$p-7+2x+4a$
$64\times(1,2)$	$p+1+2x-4a$	$p+1-6x+4a$
$64\times(1,3)$	$p+1-6x+4a$	$p+1+2x-4a-16b$
$64\times(1,4)$	$p+1+2x-4a$	$p+1+2x-4a+16y$
$64\times(1,5)$	$p+1+2x-4a$	$p+1+2x-4a-16y$
$64\times(1,6)$	$p+1-6x+4a$	$p+1+2x-4a+16b$
$64\times(2,4)$	$p+1-2x$	$p+1+6x+8a$
$64\times(2,5)$	$p+1+2x-4a$	$p+1-6x+4a$

DOI: 10.52396/JUSTC-2021-0234
JUSTC, **2022**, 52(3): 4

$$\begin{aligned}&\sigma_1=(0,1,2,3),\ \sigma_2=(0,3,2,1),\\&\sigma_3=(1,0,3,2),\ \sigma_4=(1,2,3,0),\\&\sigma_5=(2,3,0,1),\ \sigma_6=(2,1,0,3),\\&\sigma_7=(3,2,1,0),\ \sigma_8=(3,0,1,2),\\&\sigma_9=(0,1,3,2),\ \sigma_{10}=(0,3,1,2),\\&\sigma_{11}=(1,0,2,3),\ \sigma_{12}=(1,2,0,3),\\&\sigma_{13}=(2,3,1,0),\ \sigma_{14}=(2,1,3,0),\\&\sigma_{15}=(3,2,0,1),\ \sigma_{16}=(3,0,2,1),\\&\sigma_{17}=(0,2,3,1),\ \sigma_{18}=(0,2,1,3),\\&\sigma_{19}=(1,3,0,2),\ \sigma_{20}=(1,3,2,0),\\&\sigma_{21}=(2,0,1,3),\ \sigma_{22}=(2,0,3,1),\\&\sigma_{23}=(3,1,2,0),\ \sigma_{24}=(3,1,0,2).\end{aligned}$$

3 New construction of perfect quaternary sequences pairs

In this section, we provide a generic construction of uncorrelated quaternary sequences pairs.

Suppose N is an odd integer. We need a special case for Lemma 2.1:

Lemma 3.1. Let a,b,c be quaternary sequences of length N. Let u *and* v be the interleaved sequences

$$u=I\left(a,L^{\frac{N+1}{2}}(a)\right)\text{ and }v=I\left(b,L^{\frac{N+1}{2}}(c)\right)$$

where L is the left shift operator. Subsequently, the auto- and cross-correlation functions of u and v are given by:

$$R_u(\tau)=\begin{cases}2R_a(\tau'), & \tau''=0;\\ 2R_a\left(\tau'+\dfrac{N+1}{2}\right), & \tau''=1\end{cases}\tag{3}$$

$$R_v(\tau)=\begin{cases}R_b(\tau')+R_c(\tau'), & \tau''=0;\\ R_{b,c}\left(\tau'+\dfrac{N+1}{2}\right)+R_{c,b}\left(\tau'+\dfrac{N+1}{2}\right), & \tau''=1\end{cases}\tag{4}$$

$$R_{u,v}(\tau)=\begin{cases}R_{a,b}(\tau')+R_{a,c}(\tau'), & \tau''=0;\\ R_{a,c}\left(\tau'+\dfrac{N+1}{2}\right)+R_{a,b}\left(\tau'+\dfrac{N+1}{2}\right), & \tau''=1\end{cases}\tag{5}$$

where $0\leqslant\tau<2N$, $\tau=2\tau'+\tau''$, $0\leqslant\tau'<N$ and $0\leqslant\tau''<2$.

Definition 3.1. Suppose $\pi=\{A_0,A_1,A_2,A_3\}$ is a partition of $\mathbb{Z}_N^*$, $\sigma=(\sigma(0),\sigma(1),\sigma(2),\sigma(3))$ is a permutation of $\mathbb{Z}_4$, and $s\in\{0,1,2,3\}$. The quaternary sequence $\beta=\beta_{\pi,\sigma,s}$ associated with π, σ, and s of length N is defined as

$$\beta(t)=\begin{cases}\sigma(s), & \text{if } t=0;\\ k, & \text{if } t\in A_{\sigma(k)},\ k=0,1,2,3\end{cases}\tag{6}$$

If π implied by context and $\sigma=\sigma_i$, then we write β_i^s for $\beta_{\pi,\sigma_i,s}$.

The first result of this study is the following:

Theorem 3.1. Suppose the permutations of $\mathbb{Z}_4$ are ordered as in Chapter 2.3. Subsequently, for any partition π of $\mathbb{Z}_N^*$ and any $s\in\{0,1,2,3\}$, if i, j, $j+4$ are in the same interval $[1,8]$, $[9,16]$, or $[17,24]$, then

$$R_{\beta_i^s,\beta_j^s}(\tau)+R_{\beta_i^s,\beta_{j+4}^s}(\tau)=0,\ 0\leqslant\tau<N.$$

Consequently, the interleaved sequence pair

$$u=I\left(\beta_i^s,L^{\frac{N+1}{2}}(\beta_i^s)\right),\quad v=I\left(\beta_j^s,L^{\frac{N+1}{2}}(\beta_{j+4}^s)\right)\tag{7}$$

is an uncorrelated pair, that is, $R_{u,v}(\tau)=0$.

Proof. We prove the case in which $i=j=1$ and $s=0$. The other cases can be proved in the same manner.

We write $\beta_i^0=\beta_i$, and we must show that $R_{\beta_1}(\tau)+R_{\beta_1,\beta_5}(\tau)=0$. For subsets X,Y of $\mathbb{Z}_N$, the difference function $d_\tau(X,Y)$ is the function

$$d_\tau(X,Y)=|X\cap(Y+\tau)|.$$

By definition, the real and imaginary parts of the autocorrelation function $R_{\beta_1}(\tau)$ and the cross-correlation function $R_{\beta_1,\beta_5}(\tau)$ are given as follows:

$$\begin{aligned}\mathrm{Re}R_{\beta_1}(\tau)=&|\{t:\beta_1(t)-\beta_1(t+\tau)=0\}|-|\{t:\beta_1(t)-\beta_1(t+\tau)=2\}|-|\{t:\beta_1(t)-\beta_1(t+\tau)=-2\}|=\\&d_\tau(\{0\}\cup A_0,\{0\}\cup A_0)+d_\tau(A_1,A_1)+d_\tau(A_2,A_2)+d_\tau(A_3,A_3)-d_\tau(\{0\}\cup A_0,A_2)-d_\tau(A_1,A_3)-d_\tau(A_2,\{0\}\cup A_0)-d_\tau(A_3,A_1),\\ \mathrm{Im}R_{\beta_1}(\tau)=&|\{t:\beta_1(t)-\beta_1(t+\tau)=1\}|+|\{t:\beta_1(t)-\beta_1(t+\tau)=-3\}|-|\{t:\beta_1(t)-\beta_1(t+\tau)=-1\}|-|\{t:\beta_1(t)-\beta_1(t+\tau)=3\}|=\\&d_\tau(\{0\}\cup A_0,A_1)+d_\tau(A_1,A_2)+d_\tau(A_2,A_3)+d_\tau(A_3,\{0\}\cup A_0)-d_\tau(A_1,\{0\}\cup A_0)-d_\tau(A_2,A_1)-d_\tau(A_3,A_2)-d_\tau(\{0\}\cup A_0,A_3),\\ \mathrm{Re}R_{\beta_1,\beta_5}(\tau)=&|\{t:\beta_1(t)-\beta_5(t+\tau)=0\}|-|\{t:\beta_1(t)-\beta_5(t+\tau)=2\}|-|\{t:\beta_1(t)-\beta_5(t+\tau)=-2\}|=\\&d_\tau(A_2,\{0\}\cup A_0)+d_\tau(A_3,A_1)+d_\tau(\{0\}\cup A_0,A_2)+d_\tau(A_1,A_3)-d_\tau(A_2,A_2)-d_\tau(A_3,A_3)-d_\tau(\{0\}\cup A_0,\{0\}\cup A_0)-d_\tau(A_1,A_1),\\ \mathrm{Im}R_{\beta_1,\beta_5}(\tau)=&|\{t:\beta_1(t)-\beta_5(t+\tau)=1\}|+|\{t:\beta_1(t)-\beta_5(t+\tau)=-3\}|-|\{t:\beta_1(t)-\beta_5(t+\tau)=-1\}|-|\{t:\beta_1(t)-\beta_5(t+\tau)=3\}|=\\&d_\tau(A_2,A_1)+d_\tau(A_3,A_2)+d_\tau(\{0\}\cup A_0,A_3)+d_\tau(A_1,\{0\}\cup A_0)-d_\tau(A_3,\{0\}\cup A_0)-d_\tau(\{0\}\cup A_0,A_1)-d_\tau(A_1,A_2)-d_\tau(A_2,A_3),\end{aligned}$$

where $0\leq t<N$. If the subsets $X_1\cap X_2=\emptyset$ and $Y_1\cap Y_2=\emptyset$, we verify that

$$d_\tau(X_1\cup X_2,Y_1\cup Y_2)=d_\tau(X_1,Y_1)+d_\tau(X_1,Y_2)+d_\tau(X_2,Y_1)+d_\tau(X_2,Y_2).$$

Therefore, $R_{\beta_1}(\tau)+R_{\beta_1,\beta_5}(\tau)=0$ for $0\leqslant\tau<N$.

In practice, the pair (u,v), given by Eq. (7), is preferrable as be an uncorrelated sequence pair, which is almost balanced and with low autocorrelation, except at a few positions. Note that

(i) If the partition components A_i are of the same size (that is, $N\equiv 1\bmod 4$), then β_i^s is balanced, that is, u and v are almost balanced.

(ii) By Lemma 3.1,

DOI: 10.52396/JUSTC-2021-0234
JUSTC, **2022**, 52(3): 4

$$R_u(\tau)=\begin{cases}2R_{\beta_i^s}(\tau'), & \tau''=0;\\ 2R_{\beta_i^s}\left(\tau'+\dfrac{N+1}{2}\right), & \tau''=1;\end{cases}$$

$$R_v(\tau)=\begin{cases}2R_{\beta_j^s}(\tau'), & \tau''=0;\\ -2R_{\beta_j^s}\left(\tau'+\dfrac{N+1}{2}\right), & \tau''=1.\end{cases}$$

Hence, the low autocorrelation of u and v at $\tau\neq 0, N$ is guaranteed by the low autocorrelation of β_i^s and β_j^s at $\tau\neq 0$, respectively. We also note that $R_u(0)=R_v(0)=R_u(N)=2N$, $R_v(N)=-2N$.

For a prime p, we choose appropriate partitions of $\mathbb{Z}_p^*$ by cyclotomic classes of orders 4 and 8 to obtain (u,v) with good properties. Here, we provide a toy example.

Suppose $N\equiv 1 \pmod 4$ with the partition given by:

$$A_0=\left\{1,\cdots,\frac{N-1}{4}\right\},\qquad A_1=\left\{\frac{N+3}{4},\cdots,\frac{N-1}{2}\right\},$$
$$A_2=\left\{\frac{N+1}{2},\cdots,\frac{3(N-1)}{4}\right\},\qquad A_3=\left\{\frac{3N+1}{4},\cdots,N-1\right\}.$$

This provides a perfect and almost balanced pair with high autocorrelation.

Example 3.1. Let $N=13$, $A_0=\{1,2,3\}$, $A_1=\{4,5,6\}$, $A_2=\{7,8,9\}$, and $A_3=\{10,11,12\}$. Let $(i,j)=(1,2)$ and $s=1$. Subsequently,

$$\beta_1^1=1000111222333,$$
$$\beta_2^1=3000333222111,$$
$$\beta_6^1=1222111000333.$$

The quaternary sequences pair (u,v) is

$$u=12020203131311202020313131,$$
$$v=30000003333331222222111111.$$

We can see that $R_{u,v}(\tau)=0$ for $0\leqslant\tau<26$; however, the sequences u,v have a large autocorrelation.

4 Construction of sequence pairs using cyclotomic classes of $\mathbb{Z}_p$

Let p be an odd prime. We choose the partition of $\mathbb{Z}_p^*$ from cyclotomic classes of orders 4 and 8. This makes the sequences β_i^s balanced such that the sequence pairs obtained are uncorrelated, almost balanced, and have low autocorrelation, except at a few positions.

Theorem 4.1. Suppose $p=4f+1=x^2+4y^2$ with $x\equiv 1 \bmod 4$. Let D_k be the cyclotomic class of order 4 and π the partition $A_k=D_k$. Subsequently, β_i^s is balanced and

① if f is even,

$$R_{\beta_i^s}(\tau)\in\{-1+\Delta_1,-1+y+\Delta_1,-1-y+\Delta_1\},$$

where $\Delta_1\in\{0,\pm 2\}$;

② if f is odd and $1\leqslant i\leqslant 8$,

$$R_{\beta_i^s}(\tau)\in\{-1+\Delta_1+\Delta_2\omega,-1+y+\Delta_1+\Delta_2\omega,-1-y+\Delta_1+\Delta_2\omega\},$$

where $\Delta_1\in\{0,\pm 1\}$, $\Delta_2\in\{0,\pm 1,\pm 2\}$.

Therefore, if y is small, then β_i^s has low autocorrelation, except at the in-phase position.

Proof. The real and imaginary parts of the autocorrelation function $R_{\beta_i^s}(\tau)$ are given as follows:

$$\begin{aligned}\mathrm{Re}R_{\beta_i^s}(\tau)=&d_\tau(D_{\sigma_i(0)},D_{\sigma_i(0)})+d_\tau(D_{\sigma_i(1)},D_{\sigma_i(1)})+d_\tau(D_{\sigma_i(2)},D_{\sigma_i(2)})+\\&d_\tau(D_{\sigma_i(3)},D_{\sigma_i(3)})-d_\tau(D_{\sigma_i(0)},D_{\sigma_i(2)})-d_\tau(D_{\sigma_i(1)},D_{\sigma_i(3)})-\\&d_\tau(D_{\sigma_i(2)},D_{\sigma_i(0)})-d_\tau(D_{\sigma_i(3)},D_{\sigma_i(1)})+\Delta_1,\\ \mathrm{Im}R_{\beta_i^s}(\tau)=&d_\tau(D_{\sigma_i(0)},D_{\sigma_i(1)})+d_\tau(D_{\sigma_i(1)},D_{\sigma_i(2)})+d_\tau(D_{\sigma_i(2)},D_{\sigma_i(3)})+\\&d_\tau(D_{\sigma_i(3)},D_{\sigma_i(0)})-d_\tau(D_{\sigma_i(1)},D_{\sigma_i(0)})-d_\tau(D_{\sigma_i(2)},D_{\sigma_i(1)})-\\&d_\tau(D_{\sigma_i(3)},D_{\sigma_i(2)})-d_\tau(D_{\sigma_i(0)},D_{\sigma_i(3)})+\Delta_2,\end{aligned}$$

where if $\sigma_i(s)=k$,

$$\begin{aligned}\Delta_1=&|D_{\sigma_i(k)}\cap\tau|+|\{0\}\cap(D_{\sigma_i(k)}+\tau)|-\\&|\{0\}\cap(D_{\sigma_i(k+2)}+\tau)|-|D_{\sigma_i(k+2)}\cap\tau|,\\ \Delta_2=&|D_{\sigma_i(k+3)}\cap\tau|+|\{0\}\cap(D_{\sigma_i(k+1)}+\tau)|-\\&|\{0\}\cap(D_{\sigma_i(k+3)}+\tau)|-|D_{\sigma_i(k+1)}\cap\tau|.\end{aligned}$$

If f is even, then $-1\in D_0$, and $\Delta_1\in\{0,\pm 2\},\Delta_2=0$, by calculation, for $\tau\in\mathbb{Z}_p^*$, $\mathrm{Re}R_{\beta_i^s}(\tau)\in\{-1+\Delta_1,-1+y+\Delta_1,-1-y+\Delta_1\}$, $\mathrm{Im}R_{\beta_i^s}(\tau)=0$, that is, $R_{\beta_i^s}(\tau)\in\{-1+\Delta_1,-1+y+\Delta_1,-1-y+\Delta_1\}$.

If f is odd, then $-1\in D_2$, and $\Delta_1\in\{0,\pm 1\},\Delta_2\in\{0,\pm 1,\pm 2\}$, by calculation, for $\tau\in\mathbb{Z}_p^*$, $\mathrm{Re}R_{\beta_i^s}(\tau)\in\{-1+\Delta_1,-1+y+\Delta_1,-1-y+\Delta_1\}$, we can verify that $\mathrm{Im}R_{\beta_i^s}(\tau)=\Delta_2$ if $1\leqslant i\leqslant 8$, that is, $R_{\beta_i^s}(\tau)\in\{-1+\Delta_1+\Delta_2\omega,-1+y+\Delta_1+\Delta_2\omega,-1-y+\Delta_1+\Delta_2\omega\}$.

Example 4.1. Suppose $p=37=4\times 9+1$, $\mathbb{F}_{37}^{\times}=\langle 2\rangle$. The cyclotomic classes of order 4 over $\mathbb{Z}_{37}$ are

$$D_0=\{1,7,9,10,12,16,26,33,34\},$$
$$D_1=\{2,14,15,18,20,24,29,31,32\},$$
$$D_2=\{3,4,11,21,25,27,28,30,36\},$$
$$D_3=\{5,6,8,13,17,19,22,23,35\}.$$

Let $A_k=D_k, 0\leqslant k\leqslant 3$, $i=2$, $j=3$ and $s=1$, then,

$$\beta_2^1=3032211010020133013132113202232330012,$$
$$\beta_3^1=0103322121131200120203220313303001123,$$
$$\beta_7^1=2321100303313022302021002131121223301.$$

The quaternary sequence pair (u,v) of length 74 is

$$u=31033221211312001202032203133030011233103322121131200120203220313303001123,$$
$$v=00120130302221132111123112220303102102230231212000331033330133000212132032.$$

By calculation, $R_{u,v}(\tau)=0$, and $R_u(\tau)$ and $R_v(\tau)$ are given by:

DOI: 10.52396/JUSTC-2021-0234
JUSTC, **2022**, 52(3): 4

$$\begin{aligned}R_u(\tau)_{\tau=0}^{73}=&\{74,-2,-2-4\omega,-2,-2,-2+4\omega,-2+4\omega,-2,-2+4\omega,-2,-2,-2,\\&-2,-2+4\omega,-2-4\omega,-2-4\omega,-2,-2+4\omega,-2-4\omega,-2+4\omega,\\&-2-4\omega,-2,-2+4\omega,-2+4\omega,-2-4\omega,-2,-2,-2,-2,-2-4\omega,\\&-2,-2-4\omega,-2-4\omega,-2,-2,-2+4\omega,-2,74,-2,-2-4\omega,-2,-2,\\&-2+4\omega,-2+4\omega,-2,-2+4\omega,-2,-2,-2,-2,-2+4\omega,-2-4\omega,\\&-2-4\omega,-2,-2+4\omega,-2-4\omega,-2+4\omega,-2-4\omega,-2,-2+4\omega,\\&-2+4\omega,-2-4\omega,-2,-2,-2,-2,-2-4\omega,-2,-2-4\omega,-2-4\omega,\\&-2,-2,-2+4\omega,-2\},\end{aligned}$$

$$\begin{aligned}R_v(\tau)_{\tau=0}^{73}=&\{74,2,-2-4\omega,2,-2,2-4\omega,-2+4\omega,2,-2+4\omega,2,-2,2,-2,2-4\omega,\\&-2-4\omega,2+4\omega,-2,2-4\omega,-2-4\omega,2-4\omega,-2-4\omega,2,-2+4\omega,\\&2-4\omega,-2-4\omega,2,-2,2,-2,2+4\omega,-2,2+4\omega,-2-4\omega,2,-2,2-4\omega,\\&-2,-74,-2,2+4\omega,-2,2,-2+4\omega,2-4\omega,-2,2-4\omega,-2,2,-2,2,\\&-2+4\omega,2+4\omega,-2-4\omega,2,-2+4\omega,2+4\omega,-2+4\omega,2+4\omega,-2,\\&2-4\omega,-2+4\omega,2+4\omega,-2,2,-2,2,-2-4\omega,2,-2-4\omega,2+4\omega,-2,\\&2,-2+4\omega,2\}.\end{aligned}$$

Theorem 4.2. Suppose $p=m^4+16$ is a prime. Let the partition π be given by $A_0=D_0\cup D_4, A_1=D_1\cup D_7, A_2=D_2\cup D_6$, $A_3=D_3\cup D_5$, where the D_ks are cyclotomic classes of order 8. Then, the sequence β_i^s is balanced and has low autocorrelation except at the in-phase position: $R_{\beta_i^s}(\tau)\in\{-7,\pm1,\pm3\}$ for $0<\tau<p$.

Proof. If f is even, $x=m^2, y=\pm2, a=m^2-4$. We prove this when $i=1, s=0$, and the other cases are provable in the same manner.

The real and imaginary parts of $R_{\beta_1^0}(\tau)$ are as follows:

$$\mathrm{Re}R_{\beta_1^0}(\tau)=d_\tau(\{0\}\cup A_0,\{0\}\cup A_0)+d_\tau(A_1,A_1)+d_\tau(A_2,A_2)+d_\tau(A_3,A_3)-d_\tau(\{0\}\cup A_0,A_2)-d_\tau(A_1,A_3)-d_\tau(A_2,\{0\}\cup A_0)-d_\tau(A_3,A_1),$$

$$\mathrm{Im}R_{\beta_1^0}(\tau)=d_\tau(\{0\}\cup A_0,A_1)+d_\tau(A_1,A_2)+d_\tau(A_2,A_3)+d_\tau(A_3,\{0\}\cup A_0)-d_\tau(A_1,\{0\}\cup A_0)-d_\tau(A_2,A_1)-d_\tau(A_3,A_2)-d_\tau(\{0\}\cup A_0,A_3).$$

For $\tau\in D_0$, we have

$$\begin{aligned}\mathrm{Re}R_{\beta_1^0}(\tau)=&d_\tau(A_0,A_0)+d_\tau(A_1,A_1)+d_\tau(A_2.A_2)+d_\tau(A_3,A_3)-\\&d_\tau(A_0,A_2)-d_\tau(A_1,A_3)-d_\tau(A_2,A_0)-d_\tau(A_3,A_1)+\\&|A_0\cap\tau|+|\{0\}\cap(A_0+\tau)|-|\{0\}\cap(A_2+\tau)|-|A_2\cap\tau|=\\&(0,0)+(0,1)-(0,2)+(0,3)+3(0,4)+(0,5)-(0,6)+(0,7)+\\&2(1,2)+2(2,5)-2(2,4)-2(1,3)-2(1,5)-2(1,4)-2(1,6)+2=\\&\begin{cases}1, & \text{if 2 is a quartic residue;}\\1-x+a, & \text{if 2 is not a quartic residue;}\end{cases}\end{aligned}$$

$$\begin{aligned}\mathrm{Im}R_{\beta_1^0}(\tau)=&d_\tau(A_0,A_1)+d_\tau(A_1,A_2)+d_\tau(A_2,A_3)+d_\tau(A_3,A_0)-d_\tau(A_1,A_0)-d_\tau(A_2,A_1)-d_\tau(A_3,A_2)-d_\tau(A_0,A_3)+\\&|\{0\}\cap(A_1+\tau)|+|A_3\cap\tau|-|A_1\cap\tau|-|\{0\}\cap(A_3+\tau)|=0.\end{aligned}$$

Therefore, $R_{\beta_1^0}(\tau)=\mathrm{Re}R_{\beta_1^0}(\tau)$ if $\tau\in D_0$. Similarly, we obtain the values $R_{\beta_1^0}(\tau)$ for $\tau\in D_l, 0\leqslant l<8$ as follows: when 2 is a quartic residue,

$$R_{\beta_1^0}(\tau)=\begin{cases}1, & \tau\in D_0\cup D_4,\\-1-y+\frac{1}{2}(x-a)=-1,3, & \tau\in D_1\cup D_5,\\-3-x+a=-7, & \tau\in D_2\cup D_6,\\-1+y+\frac{1}{2}(x-a)=-1,3, & \tau\in D_3\cup D_7;\end{cases}$$

and when 2 is not a quartic residue,

$$R_{\beta_1^0}(\tau)=\begin{cases}1-x+a=-3, & \tau\in D_0\cup D_4,\\-1+y+\frac{1}{2}(x-a)=-1,3, & \tau\in D_1\cup D_5,\\-3, & \tau\in D_2\cup D_6,\\-1-y+\frac{1}{2}(x-a)=-1,3, & \tau\in D_3\cup D_7.\end{cases}$$

Example 4.2. For $p=97=3^4+16$, let $\mathbb{F}_{97}^{\times}=\langle 5\rangle$; then, the cyclotomic classes of order 8 in $\mathbb{Z}_{97}$ are

DOI: 10.52396/JUSTC-2021-0234
JUSTC, **2022**, 52(3): 4

$$
\begin{aligned}
D_0 &= \{1, 6, 16, 22, 35, 36, 61, 62, 75, 81, 91, 96\},\\
D_1 &= \{5, 13, 14, 17, 19, 30, 67, 78, 80, 83, 84, 92\},\\
D_2 &= \{2, 12, 25, 27, 32, 44, 53, 65, 70, 72, 85, 95\},\\
D_3 &= \{10, 26, 28, 34, 37, 38, 59, 60, 63, 69, 71, 87\},\\
D_4 &= \{4, 9, 24, 33, 43, 47, 50, 54, 64, 73, 88, 93\},\\
D_5 &= \{20, 21, 23, 29, 41, 45, 52, 56, 68, 74, 76, 77\},\\
D_6 &= \{3, 8, 11, 18, 31, 48, 49, 66, 79, 86, 89, 94\},\\
D_7 &= \{7, 15, 39, 40, 42, 46, 51, 55, 57, 58, 82, 90\}.
\end{aligned}
$$

Let $i = 1$, $j = 3$ and $s = 0$, then,

$$
\begin{aligned}
\beta_1^0 &= 0022010120322111012133030232331220300331131023102201320131133003022133232030331210111223021010220,\\
\beta_3^0 &= 1133101031233000103022121323220331211220020132013310231020022111213302232312122030100033213010 1331,\\
\beta_7^0 &= 3311323213011222321200303101002113033002202310231132013202200330311200101303002123222110312323113.
\end{aligned}
$$

The quaternary sequence pair (u, v) of length 194 is

$$
\begin{aligned}
u = {}&02002123021001132101332320101310021221133332033200233023333112212\\
&00131010232331012311001203212002020021230210011321013323201013100\\
&2122113333203320023302333311221200131010232331012311001203212002,\\
v = {}&11133230110312003212203033030003110132002021102113302330202201323\\
&31222121121200301220312332101133333110123321302210300212112122213\\
&3231022020332033112011202002310113000303330302212300213011032 3311.
\end{aligned}
$$

Subsequently, $R_{u,v}(\tau) = 0$, $R_u(\tau)$ and $R_v(\tau)$ are as follows:

$$
\begin{aligned}
R_u(\tau)_{\tau=0}^{193} = \{&194, -6, -6, -6, -6, 6, -6, -2, -6, -6, -2, -6, -6, 6, 6, -2, -6, 6, -6,\\
&6, 6, 6, -6, 6, -6, -6, -2, -6, -2, 6, 6, -6, -6, -6, -2, -6, -6, -2, -2,\\
&-2, -2, 6, -2, -6, -6, 6, -2, -6, -6, -6, -6, -2, 6, -6, -6, -2, 6, -2,\\
&-2, -2, -2, -6, -6, -2, -6, -6, -6, 6, 6, -2, -6, -2, -6, -6, 6, -6, 6,\\
&6, 6, -6, 6, -6, -2, 6, 6, -6, -6, -2, -6, -6, -2, -6, 6, -6, -6, -6, -6,\\
&194, -6, -6, -6, -6, 6, -6, -2, -6, -6, -2, -6, -6, 6, 6, -2, -6, 6, -6,\\
&6, 6, 6, -6, 6, -6, -6, -2, -6, -2, 6, 6, -6, -6, -6, -2, -6, -6, -2, -2,\\
&-2, -2, 6, -2, -6, -6, 6, -2, -6, -6, -6, -6, -2, 6, -6, -6, -2, 6, -2,\\
&-2, -2, -2, -6, -6, -2, -6, -6, -6, 6, 6, -2, -6, -2, -6, -6, 6, -6, 6,\\
&6, 6, -6, 6, -6, -2, 6, 6, -6, -6, -2, -6, -6, -2, -6, 6, -6, -6, -6, -6\},
\end{aligned}
$$

$$
\begin{aligned}
R_v(\tau)_{\tau=0}^{193} = \{&194, 6, -6, 6, -6, -6, -6, 2, -6, 6, -2, 6, -6, -6, 6, 2, -6, -6, -6, -6,\\
&6, -6, -6, -6, -6, 6, -2, 6, -2, -6, 6, 6, -6, 6, -2, 6, -6, 2, -2, 2, -2, -6,\\
&-2, 6, -6, -6, -2, 6, -6, 6, -6, 2, 6, 6, -6, 2, 6, 2, -2, 2, -2, 6, -6, 2, -6,\\
&6, -6, -6, 6, -2, -6, 2, -6, 6, 6, 6, 6, -6, 6, 6, 6, 6, -2, -6, 6, 6, -6, 2, -6,\\
&6, -2, 6, 6, 6, -6, 6, -6, -194, -6, 6, -6, 6, 6, 6, -2, 6, -6, 2, -6, 6, 6, -6,\\
&-2, 6, 6, 6, 6, -6, 6, 6, 6, 6, -6, 2, -6, 2, 6, -6, -6, 6, -6, 2, -6, 6, -2, 2,\\
&-2, 2, 6, 2, -6, 6, 6, 2, -6, 6, -6, 6, -2, -6, -6, 6, -2, -6, -2, 2, -2, 2,\\
&-6, 6, -2, 6, -6, 6, 6, -6, 2, 6, -2, 6, -6, -6, -6, -6, 6, -6, -6, -6, -6,\\
&2, 6, -6, -6, 6, -2, 6, -6, 2, -6, -6, -6, 6, -6, 6\}.
\end{aligned}
$$

Remark 4.1. Note that the numbers of primes of the form x^2+4, x^2+9, x^4+16, etc., are all assumed to be infinite by the Bouniakowsky conjecture[14].

5 Conclusions

In this study, we constructed uncorrelated quaternary sequence pairs of length $2N$ by using the cyclotomic classes. The result shows that the sequence pairs are almost balanced and have low autocorrelation, except at a few positions. In the future work, studying other partitions of $\mathbb{Z}_N^*$ would be interesting. For example, if $N = pq$, the partitions of $\mathbb{Z}_{pq}^*$ may be choose as combinations of the generalized cyclotomic classes[15] introduced by Shen et al..

Acknowledgements

The work was supported by Anhui Initiative in Quantum Information Technologies (AHY150200), USTC Research Funds of the Double First-Class Initiative (YD0010002004), and the Fundamental Research Funds for the Central Universities (WK0010000068).

Conflict of interest

The authors declare that they have no conflict of interest.

Biographies

Yi Ouyang is a professor at the University of Science and Technology of China (USTC). He received the PhD degree in Mathematics from the University of Minnesota in 2000. His research interests include Fontaine theory of p-adic representations and (φ, Γ)-modules and its connection to Iwasawa theory, theory of elliptic curves and its application in cryptography, class groups and class numbers of number fields and function fields.

Sen Wang is working toward the PhD degree at the School of Mathematical Sciences, University of Science and Technology of China. His area of interests include sequence design and its applications.

References

[1] Fan P, Darnell M. Sequence Design for Communications Applications. London: Research Studies Press, 1996.
[2] Golomb S, Gong G. Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar. Cambridge, UK: Cambridge University Press, 2005.
[3] Cusick T, Ding C, Renvall A. Stream Ciphers and Number Theory. Amsterdam: North-Holland Publishing, 1998.
[4] Luo G, Cao X, Shi M, et al. Three new constructions of asymptotically optimal periodic quasi-complementary sequence sets with small alphabet sizes. *IEEE Trans. Inf. Theory,* **2021**, *67* (8): 5168–5177.
[5] Shi M, Qian L, Helleseth T, et al. Five-weight codes from three-valued correlation of M-sequences. *Adv. Math. Commun.,* **2021**: doi 10.3934/amc.2021022.
[6] Luo L, Ma W, Zhao F. Binary sequence pairs of period p^m-1 with optimal three-level correlation. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,* **2018**, *E101-A* (8): 1263–1266.
[7] Shen X, Jia Y, Song X. Constructions of binary sequence pairs of period $3p$ with optimal three-level correlation. *IEEE Commun. Lett.,* **2017**, *21* (10): 2150–2153.
[8] Peng X, Ren J, Xu C, et al. New families of binary sequence pairs with three-level correlation and odd composite length. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,* **2016**, *E99-A* (4): 874–879.
[9] Yang Y, Tang X, Zhou Z. The autocorrelation magnitude of balanced binary sequence pairs of prime period $N\equiv 1$ (mod 4) with optimal cross-correlation. *IEEE Commun. Lett.,* **2015**, *19* (4): 585–588.
[10] Li M, Peng W, Bai P, et al. Construction of several classes of binary and quaternary complete sequences and sequence pairs. *Wirel. Pers. Commun.,* **2015**, *82* (1): 113–122.
[11] Peng X, Xu C. New construction of quaternary sequence pairs with even period and three-level correlation. In: Proceedings of the Fifth International Workshop on Signal Design and Its Applications in Communications. IEEE, 2011: 72–75.
[12] Yang Y, Tang X. Balanced quaternary sequences pairs of odd period with (almost) optimal autocorrelation and cross-correlation. *IEEE Commun. Lett.,* **2014**, *18* (8): 1327–1330.
[13] Zhou Z, Li J, Yang Y, et al. Two constructions of quaternary periodic complementary pairs. *IEEE Commun. Lett.,* **2018**, *22* (12): 2507–2510.
[14] Bouniakowsky V. Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la de composition des entiers en facteurs. *Sc. Math. Phys.,* **1857**, *6*: 305–329.
[15] Shen X, Jia Y, Song X, et al. New construction methods for binary sequence pairs of period pq with ideal two-level correlation. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,* **2018**, *E101-A* (4): 704–712.

DOI: 10.52396/JUSTC-2021-0234
JUSTC, **2022**, 52(3): 4