Kuwait J. Sci. **43 (1)** pp. 1-14, 2016

A class of almost *r*-phase sequences with ideal autocorrelation

Shenghua Li[1*], Lianfei Luo[1], Hannuo Zhao[1,2]

[1]*Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, Hubei, China*

[2]*School of Business, Shaanxi Institute of International Trade and Commerce, Xianyang 712046, shaanxi, China*

[*]*Corresponding Author: E-mail: lishmag2014@163.com, lsh@hubu.edu.cn*

Abstract

For an odd prime $N \equiv 1 \pmod{r}$, $\phi(r)$ almost r-phase sequences of period N are constructed based on cyclotomy, where r is a positive integer and ϕ is Euler's function. The new sequences have ideal autocorrelation property. Moreover, these almost r-phase sequences are modified to obtain $r\phi(r)$ r-phase sequences with good autocorrelation, which include known polyphase power-residue sequences, Legendre sequences ($r = 2$) and quadriphase sequences ($r = 4$). The autocorrelation distribution of these r-phase sequences are determined completely.

Keywords: Almost r-phase sequence; correlation distribution; cyclotomic class; cyclotomic number; ideal autocorrelation.

AMS Subject Classification: 11T22, 94A60, 94A55.

1. Introduction

Sequences with good correlation have been widely used in communication system and cryptography (Ciftlikli & Develi, 2004; Golomb & Gong, 2005; Huang & Tu, 2015; Rushanan, 2006). The sequences with good correlation applied in code division multiple access (CDMA) can successfully acquire the correct timing information and distinguish multiple users. On the other hand, the sequences with good correlation employed as key stream generators in stream cipher cryptography and digital signature algorithms can resist crosscorrelation attacks. With the growing need of high-speed data communications, the polyphase modulation scheme has been adopted as a transmission standard. Thus, constructing for polyphase sequences and sequence families with good correlation have been paid more attention to by many researchers nowadays (Chung *et al.*, 2011; Kim *et al.*, 2005; Tang & Lindner, 2009; Yu & Gong, 2010; Wang *et al.*, 2013; Zeng *et al.*, 2006; Zhou & Tang, 2011).

Since for an odd prime $N = rf + 1$, the cyclotomic classes of order r give a partition

of $\{1,2,\cdots,N-1\}$, they are often used to define cyclotomic sequences with period N (Ding & Helleseth, 1998; Lüke *et al.*, 2000; Green & Green, 2003; Meidl, 2009). The autocorrelation of cyclotomic sequences is associated with the cyclotomic number introduced by Gauss (Storer, 1967). In this paper, we focus on the construction for almost r-phase cyclotomic sequences with ideal autocorrelation (IA). An almost r-phase sequence means that in one period of the sequence, the element "zero" occurs exactly once and all the other elements are taken from the set of complex rth roots of unity. Tang & Lindner (2009) have constructed two almost quadriphase sequences with IA by listing two defining set for the sequences. We will give defining sets for almost r-phase sequences, and present a criterion for them, such that the corresponding sequences have IA property. Each defining set is a permutation of $\{0,1,\cdots,r-1\}$, which is required to be an arithmetic progression, and the common difference is relatively prime to r. The permutations ensure that the new almost r-phase sequences are optimal balanced among the complex rth roots of unity. All the autocorrelation computations are based on the results of cyclotomy (Dickson, 1935). By replacing the "zero" with any complex rth root of unity, we can transform the almost r-phase sequences obtained into r-phase sequences, which include some known cyclotomic sequences (Green & Green, 2003; Tang & Lindner, 2009). The autocorrelation of new r-phase sequences are considered from the IA of the corresponding almost r-phase sequences, and the autocorrelation distribution can be determined completely. It is shown that all new r-phase sequences have good autocorrelation and can be efficiently implemented.

This paper is organized as follows. In Section 2, we give some basic concepts and definitions on sequences, and properties of cyclotomic classes and cyclotomic numbers. In Section 3, we first define a class of almost r-phase sequences, then give the conditions such that the sequences have IA property. Moreover, we give a classification of all these sequences with IA. In Section 4, we construct a class of new r-phase sequences associated with the almost r-phase sequences in the previous section, and their autocorrelation distributions are determined completely. Concluding remarks are given in the last section.

2. Preliminaries

In this section, we introduce some notations and preliminaries, which will be used in this paper. For more details, the reader is referred to Cusick *et al.* (1998) and Golomb & Gong (2005).

Following notations will be used throughout this paper.

- $\mathbb{Z}$, the ring of integers, and $\mathbb{Z}^+$ denotes the set of all positive integers;
- $\mathbb{Z}_t$, an integer residue ring of modulo t, and $\mathbb{Z}_t^* = \mathbb{Z}_t \setminus \{0\}$;
- $N = rf + 1$, an odd prime, where r, f are two positive integers;

- θ, a fixed primitive element of $\mathbb{Z}_N$;
- D_j, $j \in \mathbb{Z}_r$, the cyclotomic classes of order r, where $D_0 = \{\theta^{rk} \mid 0 \le k \le f-1, k \in \mathbf{Z}\}$ is the multiplicative subgroup generated by θ^r, and $D_j = \theta^j D_0$ for $j \in \mathbb{Z}_r^*$, so $\mathbb{Z}_N^* = \cup_{j \in \mathbb{Z}_r} D_j$;
- (i, j), $i, j \in \mathbb{Z}_r$, the cyclotomic numbers of order r, defined by $|(D_i + 1) \cap D_j|$;
- $\omega = e^{2\pi\sqrt{-1}/r}$, a primitive rth root of unity, and $\mathfrak{A} = \{\omega^i \mid i \in \mathbb{Z}_r\}$, the set of all powers of ω;
- $\phi(n)$, $n \in \mathbb{Z}^+$, Euler phi function, the number of integers between 1 and n relatively prime to n.

First, we state some important definitions on sequences. Let $\mathbb{S}$ be a complex-valued set and $\mathrm{s} = \{s_i\}$, $s_i \in \mathbb{S}$, $i \ge 0$ be a sequence of period N. We denote s by $\{s_0, s_2, \cdots, s_{N-1}\}$ for simplicity. For $\lambda \in \mathbb{S}$, the λ-multiplier of s is defined by $\lambda \bullet \mathrm{s} = \{\lambda \cdot s_i\}$. For $k \in \mathbb{Z}^+$, the k-decimation of s is defined by $D^k(\mathrm{s}) = \{s_{ki}\}$, and it is known that $D^k(\mathrm{s})$ also has period N if and only if $\gcd(k, N) = 1$. L^τ, $0 \le \tau < N$, is a left τ-shift operator on a sequence, *i.e.*, $L^\tau(\mathrm{s}) = \{s_{i+\tau}\}$. The autocorrelation of s at τ $(0 \le \tau < N)$ is defined as

$$C_{\mathrm{s}}(\tau) = \sum_{i=0}^{N-1} s_i (s_{i+\tau})^*, \tag{2.1}$$

where the * denotes the complex conjugation. The sequence s is said to have ideal autocorrelation (IA) property if $C_{\mathrm{s}}(\tau) = -1$ for $\tau \ne 0$. Let $\delta_{\mathrm{s}} = \max |C_{\mathrm{s}}(\tau)|$ for $\tau \ne 0$. If δ_{s} is very small, we say s has good autocorrelation.

Definition 2.1. The sequence s of period N is said to be an almost r-phase sequence if $s_0 = 0$ and $s_i \in \mathfrak{A}$ for $1 \le i \le N-1$.

Definition 2.2. Two almost r-phase sequences s and t of period N are called equivalent if

$$\mathrm{t} = \lambda \bullet L^\tau(D^k(\mathrm{s})),$$

where $\lambda \in \mathfrak{A}$, $0 \le \tau \le N-1$, and k is a positive integer with $\gcd(k, N) = 1$.

Remark 2.3. By (2.1), one may check that the left shift, multiplier, and decimation operators on sequences do not change their autocorrelations.

To determine the autocorrelation of polyphase sequences, we need the following lemma on cyclotomy.

Lemma 2.4. The cyclotomic classes and cyclotomic numbers of order r have the following properties:

1) $|D_j| = f$ for $0 \le j \le r-1$.

2) If $a \in D_j$, then $aD_i = D_{i+j}$, where the subscript $i+j$ is performed modulo r.

3) -1 belongs to D_0 if f is even, and belongs to $D_{r/2}$ otherwise. Note that r must be even for odd f.

4) Diagonal Sums (Sze *et al.*, 2003)

$$\sum_{m=0}^{r-1}(m,m+n)=\begin{cases} f-1, & \text{if } n=0, \\ f, & \text{otherwise.} \end{cases} \tag{2.2}$$

In next section, we will define sequences associated with cyclotomic classes, and discuss the autocorrelation by Lemma 2.4.

3. Almost r-phase sequences with ideal autocorrelation

Definition 3.1. Let $\mathrm{P}=(p_0, p_1, \cdots, p_{r-1})$ be a permutation of $\mathbb{Z}_r$. Corresponding to P, an almost r-phase sequence s of period N is defined as

$$s_i=\begin{cases} 0, & i=0, \\ \omega^j, & i \in D_{p_j}, \quad 1 \le i \le N-1, \end{cases} \tag{3.1}$$

and P is called the defining set for s.

By 1) of Lemma 2.4, s has optimal balance among ω^j's, $j \in \mathbb{Z}_r$. Next, we consider the autocorrelation of s.

Theorem 3.2. Let $(p_0, p_1, \cdots, p_{r-1})$ be the defining set for an almost r-phase sequence s. Then the sequence s has IA property if the following two conditions are satisfied:

1) $p_l - p_{l-1} \equiv d \pmod r$, $0 \le l \le r-1$, where d is a fixed integer and the subscript $l-1$ is performed modulo r;

2) $\gcd(d, r)=1$.

Proof. Since $C_{\mathrm{s}}(\tau)=N-1$ is the trivial value for $\tau=0$, we only need to consider the case that $\tau \neq 0$.

Note that $(\omega^j)^*=\omega^{r-j}$ for each $j \in \mathbb{Z}_r$. Then, for a fixed k, $k \in \mathbb{Z}_r$, $s_i(s_{i+\tau})^*$ is equal to ω^k if and only if $i \in D_{p_j}$ and $i+\tau \in D_{p_{j+(r-k)}}$ for some j, $0 \le j \le r-1$. Thus by (2.1), the autocorrelation of s can be computed as

$$C_{\mathrm{s}}(\tau)=\sum_{k=0}^{r-1}\omega^k\left(\sum_{j=0}^{r-1}\left|\left\{i : i \in D_{p_j}, i+\tau \in D_{p_{j+(r-k)}}\right\}\right|\right).$$

By the condition 1), we have

$$\begin{aligned} C_s(\tau) &= \sum_{k=0}^{r-1} \omega^k \left(\sum_{j=0}^{r-1} \left| \left\{ i : i \in D_{p_j}, i+\tau \in D_{p_j+(r-k)d} \right\} \right| \right) \\ &= \sum_{k=0}^{r-1} \omega^k \left(\sum_{m=0}^{r-1} \left| \left\{ i : i \in D_m, i+\tau \in D_{m-kd} \right\} \right| \right) \\ &= \sum_{k=0}^{r-1} \omega^k \left(\sum_{m=0}^{r-1} \left| \left(D_{m-kd} - \tau \right) \cap D_m \right| \right), \end{aligned}$$

where the second identity follows from that P is a permutation.

For $\tau \neq 0$, there must exist an integer b such that $-\tau = \theta^b$. Now we first consider the inner summation

$$\Gamma_k = \sum_{m=0}^{r-1} \left| \left(D_{m-kd} + \theta^b \right) \cap D_m \right|, \quad 0 \le k < r.$$

Simplify Γ_k as follows

$$\begin{aligned} \Gamma_k &= \sum_{m=0}^{r-1} \left| \left(\theta^{-b} D_{m-kd} + 1 \right) \cap \theta^{-b} D_m \right| \\ &= \sum_{m=0}^{r-1} \left| \left(D_{m-kd-b} + 1 \right) \cap D_{m-b} \right| \\ &= \sum_{m=0}^{r-1} \left(m - kd - b, m - b \right) \\ &= \sum_{m=0}^{r-1} \left(m - kd, m \right). \end{aligned}$$

Since $\gcd(d,r) = 1$, we have $\left\{ (-kd) \pmod r \mid k \in \mathbb{Z}_r \right\} = \mathbb{Z}_r$. Then, by (2.2), Γ_k is equal to $f-1$ if $k = 0$, and f otherwise. Therefore, we get

$$C_s(\tau) = \sum_{k=0}^{r-1} \omega^k \Gamma_k = f - 1 + f \sum_{k=1}^{r-1} \omega^k.$$

Since ω is a primitive rth root of unity, we get $\sum_{k=1}^{r-1} \omega^k = -1$. Thus, $C_s(\tau) = -1$ for $\tau \neq 0$, and so s has IA property.

Example 3.3. Let $N = 19 = 9 \times 2 + 1$, $r = 9$, $\omega^9 = 1$, and $\theta = 2$, a primitive element of $\mathbb{Z}_{19}$. Then the cyclotomic classes of order 9 are

$$D_0 = \{1,18\},\ D_1 = \{2,17\},\ D_2 = \{4,15\},$$

$$D_3 = \{8,11\},\ D_4 = \{3,16\},\ D_5 = \{6,13\},$$

$$D_6 = \{7,12\},\ D_7 = \{5,14\},\ D_8 = \{9,10\}.$$

Let $\mathrm{P}=(0,4,8,3,7,2,6,1,5)$, then the almost 9-phase sequence of period 19 defined by (3.1) is given as follows

$$\mathrm{s}=\{01\omega^7\omega\ \omega^5\omega^4\omega^8\omega^6\omega^3\omega^2\omega^2\omega^3\omega^6\omega^8\omega^4\omega^5\omega\ \omega^7 1\}.$$

Since P satisfies the conditions in Theorem 3.2, s has IA property, which has been confirmed by a computer program.

Next, we consider the number of the almost r-phase sequences with IA satisfying the conditions in Theorem 3.2. Note that two almost r-phase sequences are shift nonequivalent since only their first elements are equal to 0. Thus, we only need to investigate the decimation and multiplier of the almost r-phase sequence defined by (3.1).

Lemma 3.4. Let $(p_0, p_1, \cdots, p_{r-1})$ be the defining set for the almost r-phase sequence s, and $a \in D_h$ for some $h \in \mathbb{Z}_r$. Then the defining set for $D^a(\mathrm{s})$ is

$$(p_0-h, p_1-h, \cdots, p_{r-1}-h).$$

Proof. Let $\mathrm{t}=D^a(\mathrm{s})$. Then $t_0=s_0=0$, and $t_i=s_{ai}=\omega^j$ for $1\le i\le N-1$, where j satisfies $ai\in D_{p_j}$. Since $ai\in D_{p_j}$ if and only if $i\in a^{-1}D_{p_j}=D_{p_j-h}$, the result follows.

Lemma 3.5. Let $(p_0, p_1, \cdots, p_{r-1})$ be the defining set for the almost r-phase sequence s, and $\lambda=\omega^k$ for some $k\in\mathbb{Z}_r$. Then the defining set for $\lambda\bullet$s is $(p_{0-k}, p_{1-k}, \cdots, p_{r-1-k})$, where the subscript $j-k\in\mathbb{Z}_r$, $0\le j\le r-1$.

Proof. Let $\mathrm{t}=\lambda\bullet\mathrm{s}$. Then $t_0=\lambda s_0=0$, and $t_i=\lambda s_i=\omega^{k+j}$ for $1\le i\le N-1$, where j satisfies $i\in D_{p_j}$. Thus, $t_i=\omega^j$ for $i\in D_{p_{j-k}}$, which completes the proof.

From the two lemmas above, both the decimation and multiplier operators on the sequence defined by (3.1) do not change the difference of two neighbouring elements of the defining set. Thus, two almost r-phase sequences corresponding to two distinct differences d_1 and d_2 respectively in Theorem 3.2 are nonequivalent. Therefore, we have the following theorem

Theorem 3.6. There are $\phi(r)$ nonequivalent almost r-phase sequences with IA, whose defining sets satisfy the conditions in Theorem 3.2.

Remark 3.7. Tang & Lindner (2009) constructed two nonequivalent almost quadriphase sequences with IA by giving the defining sets $(0,1,2,3)$ and $(0,3,2,1)$ respectively, and proved that there were only these two nonequivalent almost quadriphase sequences. It is easily checked that the two defining sets satisfy the conditions in Theorem 3.2 and $\phi(4)=2$.

By Lemma 3.5, two sequences in Definition 3.1 corresponding to a permutation and its cyclic shift respectively are equivalent. Thus, we can assume that the first

element of a defining set satisfying the conditions in Theorem 3.2 is always 0 for each *d*. From Theorem 3.6, we have six almost 9-phase sequences of period 19 with IA, which are listed in Table 1.

Table 1. The almost 9-phase sequences of period 19 with IA

d	s
1	$01\omega\ \omega^4\omega^2\omega^7\omega^5\omega^6\omega^3\omega^8\omega^8\omega^3\omega^6\omega^5\omega^7\omega^2\omega^4\omega\ 1$
2	$01\omega^5\omega^2\omega\ \omega^8\omega^7\omega^3\omega^6\omega^4\omega^4\omega^6\omega^3\omega^7\omega^8\omega\ \omega^2\omega^5 1$
4	$01\omega^7\omega\ \omega^5\omega^4\omega^8\omega^6\omega^3\omega^2\omega^2\omega^3\omega^6\omega^8\omega^4\omega^5\omega\ \omega^7 1$
5	$01\omega^2\omega^8\omega^4\omega^5\omega\ \omega^3\omega^6\omega^7\omega^7\omega^6\omega^3\omega\ \omega^5\omega^4\omega^8\omega^2 1$
7	$01\omega^4\omega^7\omega^8\omega\ \omega^2\omega^6\omega^3\omega^5\omega^5\omega^3\omega^6\omega^2\omega\ \omega^8\omega^7\omega^4 1$
8	$01\omega^8\omega^5\omega^7\omega^2\omega^4\omega^3\omega^6\omega\ \omega\ \omega^6\omega^3\omega^4\omega^2\omega^7\omega^5\omega^8 1$

4. R-phase sequences with good autocorrelation

In this section, we will construct *r*-phase sequences associated with the almost *r*-phase sequences in the previous section.

Definition 4.1. Let s be the sequence in Definition 3.1, the corresponding *r*-phase sequence s' is defined by

$$s'_i = \begin{cases} \omega^c, & i = 0, \\ s_i, & 1 \le i \le N-1, \end{cases} \tag{4.1}$$

where $c \in \mathbb{Z}_r$, is a constant.

Note that $C_{s'}(0) = N$, is the trivial value. Next, we will determine the autocorrelation of s' for $\tau \neq 0$.

Lemma 4.2. Let s' be defined by (4.1). Then, the autocorrelation of the sequence s' is given by

$$C_{s'}(\tau) = \omega^c (s_\tau)^* + (-1)^f \cdot \omega^{r-c} \cdot s_\tau - 1, \quad 0 < \tau \le N-1. \tag{4.2}$$

Proof. By (2.1), the autocorrelation becomes

$$C_{s'}(\tau) = s'_0 \cdot (s'_\tau)^* + s'_{-\tau} \cdot (s'_0)^* + \sum_{i \neq 0, -\tau}^{N-1} s_i (s_{i+\tau})^*$$

$$= s'_0 \cdot (s'_\tau)^* + s'_{-\tau} \cdot (s'_0)^* + \sum_{i=0}^{N-1} s_i (s_{i+\tau})^* - s_0 \cdot (s_\tau)^* - s_{-\tau} \cdot (s_0)^*.$$

Now, we assume that $\tau \neq 0$. From the definitions of s and s', and IA property of s, we have

$$C_{s'}(\tau) = \omega^c \cdot (s_\tau)^* + s_{-\tau} \cdot \omega^{r-c} - 1$$

$$= \omega^c \cdot (s_\tau)^* + \omega^{r-c} \cdot s_{-1} \cdot s_\tau - 1,$$

where the last identity follows from that $s_{-\tau} = s_{-1} \cdot s_\tau$ by 2) of Lemma 2.4.

Next, we consider s_{-1}. Let $(p_0, p_1, \cdots, p_{r-1})$ be the defining set for s. Note that $p_0 = 0$, $p_{r/2} = r/2$ for even r, and r must be even for odd f. Then from 3) of Lemma 2.4 and the definition of s, we have $s_{-1} = \omega^0 = 1$ for even f, and $s_{-1} = \omega^{r/2} = -1$ otherwise, *i.e.*, $s_{-1} = (-1)^f$. Thus, (4.2) follows.

Theorem 4.3. Let s' be defined by (4.1). Then the autocorrelation of the sequence s' satisfies the following distribution:

1) When r is even, there are two subcases:

i) If f is even, then

$$C_{s'}(\tau) = \begin{cases} N, & 1 \text{ time}, \\ 1, & f \text{ times}, \\ -3, & f \text{ times}, \\ \omega^j + \omega^{r-j} - 1, & 2f \text{ times}, \quad 1 \le j \le \frac{r}{2} - 1. \end{cases} \tag{4.3}$$

ii) If f is odd, then

$$C_{s'}(\tau) = \begin{cases} N, & 1 \text{ time}, \\ -1, & 2f \text{ times}, \\ \omega^j - \omega^{r-j} - 1, & 2f \text{ times}, \quad j = 1, \cdots, \frac{r-2}{4}, \frac{r}{2} + 1, \cdots, \frac{3r-2}{4}, \end{cases} \tag{4.4}$$

for $r \equiv 2 \pmod 4$, and

$$C_{s'}(\tau) = \begin{cases} N, & 1 \text{ time}, \\ -1, & 2f \text{ times}, \\ 2i - 1, & f \text{ times}, \\ -2i - 1, & f \text{ times}, \\ \omega^j - \omega^{r-j} - 1, & 2f \text{ times}, \quad j = 1, \cdots, \frac{r}{4} - 1, \frac{r}{2} + 1, \cdots, \frac{3r}{4} - 1, \end{cases} \tag{4.5}$$

for $r \equiv 0 \pmod 4$, where $i = \sqrt{-1}$.

2) When r is odd,

$$C_{s'}(\tau)=\begin{cases} N, & 1 \text{ time}, \\ 1, & f \text{ times}, \\ \omega^{j}+\omega^{r-j}-1, & 2f \text{ times}, \quad 1\le j\le \frac{r-1}{2}. \end{cases} \tag{4.6}$$

Proof. For the case $\tau=0$, the autocorrelation is trivial.

For $\tau\neq 0$, we have (4.2). Let $s_\tau=\omega^k$ for some $k\in\mathbb{Z}_r$, then

$$\begin{aligned} C_{s'}(\tau) &= \omega^{c}(\omega^{k})^{*}+(-1)^{f}\cdot\omega^{r-c}\cdot\omega^{k}-1 \\ &= \omega^{c+r-k}+(-1)^{f}\cdot\omega^{k+r-c}-1. \end{aligned}$$

Since $\omega^{k+r-c}=(\omega^{c+r-k})^{*}$, we get

$$C_{s'}(\tau)=\omega^{j}+(-1)^{f}\cdot\omega^{r-j}-1,$$

where $j\equiv(c+r-k) \pmod r$. Note that j runs through $\mathbb{Z}_r$ f times as τ runs through $\mathbb{Z}_N^{*}$. Next, we continue the computation for two subcases in view of the parity of r.

1) When r is even, f may be even or odd.

If f is even, then $C_{s'}(\tau)=\omega^{j}+\omega^{r-j}-1$. Note that $\omega^{j}+\omega^{r-j}=2\cos(\frac{2\pi j}{r})$. Then, when $j_1, j_2\in\mathbb{Z}_r$, $\omega^{j_1}+\omega^{r-j_1}=\omega^{j_2}+\omega^{r-j_2}$ if and only if $j_1=r-j_2$. Thus, we have (4.3).

If f is odd, then $C_{s'}(\tau)=\omega^{j}-\omega^{r-j}-1$. Note that $\omega^{j}-\omega^{r-j}=2i\sin(\frac{2\pi j}{r})$, where $i=\sqrt{-1}$. From the property of sine function, we have the following:

a) When $0\le j_1\le r/2$ and $r/2+1\le j_2\le r-1$, $\omega^{j_1}-\omega^{r-j_1}\neq\omega^{j_2}-\omega^{r-j_2}$.

b) When $0\le j_1, j_2\le r/2$, $\omega^{j_1}-\omega^{r-j_1}=\omega^{j_2}-\omega^{r-j_2}$ if and only if $j_1=r/2-j_2$.

c) When $r/2+1\le j_1, j_2\le r-1$, $\omega^{j_1}-\omega^{r-j_1}=\omega^{j_2}-\omega^{r-j_2}$ if and only if $j_1=3r/2-j_2$.

Thus we have (4.4) and (4.5).

2) When r is odd, f must be even for odd N. Thus, $C_{s'}(\tau)=\omega^{j}+\omega^{r-j}-1$, and (4.6) is obtained in a similar way.

Combining with all above, we complete the proof.

Note that $\omega^{j}+\omega^{r-j}$ must be real number for $j\in\mathbb{Z}_r$, and $\omega^{j}-\omega^{r-j}$ must be pure imaginary for $j\in\mathbb{Z}_r^{*}$. Then, we can determine the maximum autocorrelation of s' from Theorem 4.3 as follows.

Corollary 4.4. Let s' be defined in Definition 4.1. Then

1) For even r and even f, the autocorrelation is $(\frac{r}{2}+2)$-valued and $\delta_{s'}=3$.

2) For $r \equiv 2 \pmod 4$ and odd f, the autocorrelation is $(\frac{r}{2}+1)$-valued and $\delta_{s'} < \sqrt{5}$.

3) For $r \equiv 0 \pmod 4$ and odd f, the autocorrelation is $(\frac{r}{2}+2)$-valued and $\delta_{s'} = \sqrt{5}$.

4) For odd r, the autocorrelation is $(\frac{r-1}{2}+2)$-valued and $\delta_{s'} < 3$.

Remark 4.5. The upper bound of out-of-phase autocorrelation values of the new r-phase sequences is independent of the period N, and is the same as that of the polyphase power-residue sequences introduced by Green & Green (2003) and Sidel'nikov (1969). Note that the polyphase power-residue sequence is the special case of s' with $d = 1$ in Theorem 3.2. For the case $r = 2$, s' is the known Legendre sequence (Golomb & Gong, 2005), and here the last cases in (4.3) and (4.4) do not exist. For the case $r = 3$, $C_{s'}(\tau)$ is 3-valued, and $C_{s'}(\tau) = -2$ for the last case in (4.6). And the results in Tang & Lindner (2009) is included in Theorem 4.3 for the case $r = 4$.

Now, we give some examples of r-phase sequences. All the results have been confirmed by computer programmes.

Example 4.6. Let s be the almost 9-phase sequence in Example 3.3 and the constant c in (4.1) be equal to 0, then the corresponding 9-phase sequence s' of period 19 is obtained

$$\{1\,1\omega^7\omega\ \omega^5\omega^4\omega^8\omega^6\omega^3\omega^2\omega^2\omega^3\omega^6\omega^8\omega^4\omega^5\omega\ \omega^7 1\}.$$

We list the autocorrelation distribution in Table 2, which shows that the autocorrelation is 6-valued and $\delta_{s'} < 3$.

Table 2. The autocorrelation distribution of a 9-phase sequence with period 19

τ	$C_{s'}(\tau)$
0	19
1, 18	1
2, 9, 10, 17	$\omega^2+\omega^7-1$
3, 6, 13, 16	$\omega\ +\omega^8-1$
4, 5, 14, 15	$\omega^4+\omega^5-1$
7, 8, 11, 12	$\omega^3+\omega^6-1$

Example 4.7. Let $N = 41 = 8\times5+1$, $r = 8$, and $\theta = 7$, a primitive element of $\mathbb{Z}_{41}$. Then the cyclotomic classes of order 8 are

$$D_0 = \{1,10,16,18,37\},\ D_1 = \{3,7,13,29,30\},\ D_2 = \{5,8,9,21,39\},$$

$$D_3 = \{15,22,24,27,35\},\ D_4 = \{4,23,25,31,40\},\ D_5 = \{11,12,28,34,38\},$$

$$D_6 = \{2,20,32,33,36\},\ D_7 = \{6,14,17,19,26\}.$$

Let $(p_0, p_1, \cdots, p_7) = (0,3,6,1,4,7,2,5)$, $c = 0$. By Definition 4.1, we get an 8-phase sequence s' of period 41 as follows (only list the exponents)

$$\{00234653660773510505261414517334227120764\}.$$

We list the autocorrelation distribution in Table 3, which shows that the autocorrelation is 6-valued and $\delta_{s'} = \sqrt{5}$.

Table 3. The autocorrelation distribution of an 8-phase sequence with period 41

τ	$C_{s'}(\tau)$
0	41
1, 4, 10, 16, 18, 23, 25, 31, 37, 40	-1
5, 8, 9, 21, 39	$2i-1$
2, 20, 32, 33, 36	$-2i-1$
6, 11, 12, 14, 17, 19, 26, 28, 34, 38	$\omega\ -\omega^7-1$
3, 7, 13, 15, 22, 24, 27, 29, 30, 35	$\omega^5-\omega^3-1$

Example 4.8. Let $N = 31 = 6\times 5+1$, $r = 6$, and $\theta = 3$, a primitive element of $\mathbb{Z}_{31}$. Then the cyclotomic classes of order 6 are

$$D_0 = \{1,2,4,8,16\},\ D_1 = \{3,6,12,17,24\},\ D_2 = \{5,9,10,18,20\},$$
$$D_3 = \{15,23,27,29,30\},\ D_4 = \{7,14,19,25,28\},\ D_5 = \{11,13,21,22,26\}.$$

Let $(p_0, p_1, \cdots, p_5) = (0,5,4,3,2,1)$, $c = 2$. By Definition 4.1, we get a 6-phase sequence s' of period 31 as follows (only list the exponents)

$$\{20050452044151230542411352132 33\}$$

We list the autocorrelation distribution in Table 4, which shows that the autocorrelation is 4-valued and $\delta_{s'} < \sqrt{5}$.

Table 4. The autocorrelation distribution of a 6-phase sequence with period 31

τ	$C_{s'}(\tau)$
0	31
3, 6, 7, 12, 14, 17, 19, 24, 25, 28	-1
1, 2, 4, 8, 11, 13, 16, 21, 22, 26	$\omega\ -\omega^5-1$
5, 9, 10, 15, 18, 20, 23, 27, 29, 30	$\omega^4-\omega^2-1$

Next, we consider the number of r-phase sequences with good correlation we obtained. From the definition of s' and Theorem 3.6, we have

Corollary 4.9. There are $r\phi(r)$ nonequivalent r-phase sequences defined in (4.2), which satisfy Theorem 4.3 and Corollary 4.4.

5. Conclusions

In this paper, we construct a class of almost r-phase sequences with IA based on cyclotomy and give a classification of the new sequences. In addition, we study the r-phase sequences corresponding to the almost r-phase sequences with IA. The r-phase sequences have good autocorrelation and the autocorrelation distribution is determined completely. All the sequences we constructed have optimal balance and can be efficiently implemented in software. With good randomness properties, they can be used as spread spectrum sequences in communication system, and as the key streams or secret keys in cryptography. For example, as a practical application in stream ciphers, our construction can generate more pseudo-random sequences to meet the requirements that a lot of key streams are needed.

Acknowledgements

This work was supported in part by Project of Hubei Provincial Department of Education (Q20101004), and in part by the Project of Graduate School of Hubei University (070-150031).

References

Chung, J.S., No, J.S. & Chung, H. (2011) A construction of a new family of M-ary sequences with low correlation from Sidel'nikov sequences. IEEE Transactions on Information Theory, **57**(4):2301-2305.

Ciftlikli, C. & Develi, I. (2004) A plausible approach to determine most suitable spreading codes for a direct-sequence CDMA system. Kuwait Journal of Science & Engineering, **31**(2):235-259.

Cusick, T.W., Ding, C. & Renvall, A. (1998) Stream Ciphers and Number Theory. Elsevier, Amsterdam.

Dickson, L.E. (1935) Cyclotomy, higher congruences, and Waring's problem. American Journal of Mathematics, **57**:391-424.

Ding, C. & Helleseth, T. (1998) On cyclotomic generator of order r. Information Processing Letters, **66**(1):21-25.

Golomb, S.W. & Gong, G. (2005) Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar. Cambridge University Press, Cambridge.

Green, D.H. & Green, P.R. (2003) Polyphase power-residue sequences. Royal Society of London Proceedings Series, A **459**(2032):817-827.

Huang, B. & Tu, H. (2015) Strongly secure certificateless one-pass authenticated key agreement scheme. Kuwait Journal of Science, **42**(1):91-108.

Kim, Y.S., Chung, J.S., No, J.S. & Chung, H. (2005) On the autocorrelation distributions of Sidel'nikov sequences. IEEE Transactions on Information Theory, **51**(9):3303-3307.

Lüke, H.D., Schotten, H.D. & Hadinejad-Mahram, H. (2000) Generalised Sidelnikov sequences with optimal autocorrelation properties. Electronics Letters, **36**(6):525-527.

Meidl, W. (2009) Remarks on a cyclotomic sequence. Designs, Codes and Cryptography, **51**(1):33-43.

Rushanan, J.J. (2006) Weil sequences: A family of binary sequences with good correlation properties. Proceeding of IEEE International Symposium on Information Theory 2006, Seattle, USA, 1648-1652.

Sidel'nikov, V.M. (1969) Some *k*-valued pseudo-random sequences and nearly equidistant codes. Problems of Information Transmission, **5**(1):12-16.

Storer, T. (1967) Cyclotomy and Difference Sets. Markham Publishing Co., Chicago.

Sze, T.W., Chanson, S., Ding, C., Helleseth, T. & Parker, M. (2003) Logarithm cartesian authentication codes. Information and Computation, **184**(1):93-108.

Tang, X. & Lindner, J. (2009) Almost quadriphase sequence with ideal autocorrelation property. IEEE Signal Processing Letters, **16**(1):38-40.

Wang, Z., Gong, G. & Yu, N.Y. (2013) New polyphase sequence families with low correlation derived from the Weil bound of exponential sums. IEEE Transactions on Information Theory, **59**(6):3990-3998.

Yu, N.Y. & Gong, G. (2010) Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation. IEEE Transactions on Information Theory, **56**(12):6376-6387.

Zeng, X., Hu, L. & Liu, Q. (2006) A novel method for constructing almost perfect polyphase sequences. Lecture Notes in Computer Science, **3969**:346-353.

Zhou, Z. & Tang, X. (2011) New nonbinary sequence families with low correlation, large size, and large linear span. Applied Mathematics Letters, **24**(7):1105-1110.

Submitted **:** 30/06/2014
Revised **:** 17/05/2015
Accepted **:** 31/05/2015

صنف من المتتاليات طورها r تقريباً و لها ارتباط ذاتي مثالي

[1،*]شنغهوا لي، [1]ليانفاي لوه، [1،2]هاننوه تشاو

[1]مختبر مفتاح هوبى الرياضيات التطبيقية - كلية الرياضيات والإحصاء - جامعة هوبى- ووهان 430062 - وهوبى- والصين

[2]كلية إدارة الأعمال- معهد شنشى التجارة الدولية والتجارة- شيانيانغ 712046- وشنشى- والصين

المقابلة المؤلف البريد الإلكتروني: lishmag2014@163.com ، lsh@hubu.edu.cn

خلاصة

نقوم في هذا البحث بإنشاء متتاليات Q(r) طورها r تقريباً ودورها N حيث r عدد صحيح موجب ، Q هي دالة على أويلر، و N عدد أولي فردي $N=1(\mathrm{mod}\ r)$. ويعتمد هذا الإنشاء على أولية العدد. و تمتاز هذه المتتاليات الجديدة بخاصية الارتباط الذاتي المثالي. إضافة إلى ذلك يمكن تعديل هذه المتتاليات للحصول على متتاليات Q(r) طورها r ولها ترابط ذاتي جيد، و تشمل هذه المتتاليات متتاليات معروفة مثل المتتاليات متعددة الأطوار راسبة الأس، متتاليات لوجندر (r=2) و المتتاليات رباعية الطور (r=4). و نقوم بالحصول و بشكل كامل على توزيع الارتباط لهذه المتتاليات.