On the Perfect Cyclically Conjugated Even and Odd Periodic Autocorrelation Properties of Quaternary Golay Sequences

Yang Yang[1,2,3] Guang Gong[2] and Xiaohu Tang[1]

[1]Institute of Mobile Communications, Southwest Jiaotong University

Chengdu, 610031, P.R. CHINA

[2]Department of Electrical and Computer Engineering University of Waterloo

Waterloo, Ontario N2L 3G1, CANADA

Email: yang_data@yahoo.cn, xhutang@ieee.org,

ggong@calliope.uwaterloo.ca

Abstract

A sequence is called perfect if its autocorrelation function is a delta function. In this paper, we give a new definition of autocorrelation function: generalized even and odd periodic autocorrelation, and generalized even and odd periodic cyclically conjugated autocorrelation. In particular, we study a special case of autocorrelation function called cyclically conjugated autocorrelation function. As a result, we present several classes of perfect cyclically conjugated even periodic and odd periodic autocorrelation of quaternary Golay sequences. We also considered such perfect property for 4^q-QAM Golay sequences, $q \geq 2$ being an integer. Those proposed sequences could be used for synchronization and detection if the time delay is known.

Index Terms. Golay sequence, quadrature amplitude modulation (QAM), cyclically conjugated even periodic autocorrelation, cyclically conjugated odd periodic autocorrelation.

1 Introduction

Sequences have been widely used in modern communications, radar, sonar, and in the field of measuring techniques [6, 20, 33]. Correlation is a measure of the similarity or relatedness between two sequences. Generally speaking, in practical systems sequences with perfect even periodic or odd periodic autocorrelation property are very favorable [11], [21], [28]-[33]. Unfortunately, their design seems extremely hard. So far, only little results are known and in

[3]Yang Yang is a visiting Ph. D. student (Oct. 2010- Sep. 2012) in the Department of Electrical and Computer Engineering, University of Waterloo.

most cases such sequences are widely believed to be not existent. Thus, people have to look for other solutions. One alternative way is to construct a pair or a set of sequences such that the sum of their autocorrelation functions is a delta function.

In [8, 9, 10], a pair of binary sequences was first introduced by Golay in connection with infrared multislit spectrometry. Such sequences pairs have a property that the sum of their respective aperiodic autocorrelation function is a delta function. For short, in the literature the pair is called Golay pair and each sequence is called a Golay sequence. Golay sequences are used in fields such as in multislit spectrometry, ultrasound measurements, acoustic measurements, radar pulse compression, Wi-Fi networks, 3G CDMA wireless networks, and OFDM communication systems.

In this paper, we will propose a new definition of autocorrelation function: generalized even and odd periodic autocorrelation, and generalized even and odd periodic cyclically conjugated autocorrelation. In particular, we consider a new autocorrelation, called cyclically conjugated autocorrelation. By using the technique of the generalized Boolean function technique developed by Davis and Jedwab [5], we investigate the cyclically conjugated even periodic autocorrelation and odd periodic autocorrelation properties of Golay sequence. Most notably, we find several classes of quaternary Golay sequences with perfect cyclically conjugated even periodic or odd periodic autocorrelation. Due to the close relationship between Golay sequences and quadrature amplitude modulation (QAM) Golay sequences, we next extend our analysis to QAM Golay sequences. Those proposed sequences could be used in synchronization and detection if the time delay is known.

This paper is organized as follows. In Section 2, we provide the necessary background information and notions used throughout the paper. In Section 3, we review some known perfect and odd perfect sequences, and give an necessary condition of even and odd perfect cyclically conjugated sequences. In Section 4, we present the perfect cyclically conjugated even periodic or odd periodic autocorrelation property of some Golay sequences. In Section 5, we construct perfect cyclically conjugated even periodic or periodic autocorrelation of QAM Golay sequences. Finally, some concluding remarks are given in Section 6.

2 Definitions and Preliminaries

For a complex-valued sequence $a = (a_0, a_1, \cdots, a_{N-1})$ with period N and a complex number δ, its *aperiodic autocorrelation function*, *generalized even periodic autocorrelation function* and *generalized odd periodic autocorrelation* at shift τ are respectively defined by

$$C_a(\tau) = \sum_{i=0}^{N-1-\tau} a_i (a_{i+\tau})^*, \quad 0 \leq \tau \leq N-1 \tag{1}$$

$$R_{a,\delta}(\tau) = C_a(\tau) + \delta (C_a(N-\tau))^* \tag{2}$$

$$\hat{R}_{a,\delta}(\tau) = C_a(\tau) + \delta C_a(N-\tau) \tag{3}$$

where x^* denotes the complex conjugate of the complex number x. The sequence a is called generalized perfect even periodic sequence with respect to δ if $R_{a,\delta}(\tau) = 0$ for $1 \leq \tau \leq N-1$, and it is called generalized perfect odd periodic sequence with respect to δ if $\hat{R}_{a,\delta}(\tau) = 0$ for $1 \leq \tau \leq N-1$.

In particular, $R_{a,1}(\tau)$ is the even periodic autocorrelation function of the sequence a, and $R_{a,-1}(\tau)$ is the odd periodic autocorrelation function of the sequence a [28, 29, 30]. In this paper, we discuss another two types of periodic autocorrelations $\hat{R}_{a,1}(\tau)$ and $\hat{R}_{a,-1}(\tau)$.

Definition 1 *The cyclically conjugated even periodic autocorrelation F_a and cyclically conjugated odd periodic autocorrelation $\hat{F}_a$ are respectively defined as*

$$F_a(\tau) = \hat{R}_{a,1}(\tau) = C_a(\tau) + C_a(N-\tau) \tag{4}$$

$$\hat{F}_a(\tau) = \hat{R}_{a,-1}(\tau) = C_a(\tau) - C_a(N-\tau). \tag{5}$$

A sequence a of length N is said to have perfect cyclically conjugated even (resp. odd) periodic autocorrelation if $F_a(\tau) = 0$ (resp. $\hat{F}_a(\tau) = 0$) for $1 \leq \tau \leq N-1$.

Note that if $a_i \in \{-1, 1\}$, then $R_{a,1}(\tau) = \hat{R}_{a,-1}(\tau) = F_a(\tau)$ and $R_{a,-1}(\tau) = \hat{R}_{a,1}(\tau) = \hat{F}_a(\tau)$. However, they are different for the rest of the cases of the values of a_i. In the remainder of this paper, we will propose several classes of perfect conjugated cyclically even (resp. odd) periodic sequences.

Let $H \geq 2$ be an integer, $\mathbb{Z}_H$ be the integer residue ring modulo H, and ξ be the primitive H-th root of unity, i.e., $\xi = \exp(2\pi\sqrt{-1}/H)$. A modulated sequence of sequence $(a_0, a_1, \cdots, a_{N-1})$

over Z_H is written as the complex sequence $(\xi^{a_0}, \xi^{a_1}, \cdots, \xi^{a_{N-1}})$. In the following, we will use those two expressions of sequences interchangeably for convenience.

Let a and b be two sequences with period N. The pair of sequences a and b are called a *Golay complementary pair* if $C_a(\tau) + C_b(\tau) = 0$ for any $1 \le \tau \le N-1$. Any one of them is called a *Golay sequence*.

A *generalized Boolean function* $f(x_1, \cdots, x_m)$ with m variables is a mapping from $\{0,1\}^m$ to $\mathbb{Z}_H$, which has a unique representation as a multiple polynomial over $\mathbb{Z}_H$ of the special form:

$$f(x_1, \cdots, x_m) = \sum_{I \in \{1, \cdots, m\}} a_I \prod_{i \in I} x_i, \ a_I \in \mathbb{Z}_H, x_i \in \{0,1\}.$$

This is called the *algebraic normal form* of f.

Let $(i_1, \cdots, i_m)$ be the binary representation of the integer $i = \sum_{k=1}^{m} i_k 2^{m-k}$. The *truth table* of a Boolean function $f(x_1, \cdots, x_m)$ is a binary string of length 2^m, where the i-th element of the string is equal to $f(i_1, \cdots, i_m)$. For example, $m = 3$, we have

$$f = (f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1)).$$

In the following, we introduce some notations. We always assume that $m \ge 4$ is an integer and π is a permutation from $\{1, \cdots, m\}$ to itself. Define a sequence $a = \{a_i\}_{i=0}^{2^m-1}$ over $\mathbb{Z}_H$, whose elements are given by

$$a_i = \frac{H}{2} \sum_{k=1}^{m-1} i_{\pi(k)} i_{\pi(k+1)} + \sum_{k=1}^{m} c_k i_k + c_0 \tag{6}$$

where $c_i \in \mathbb{Z}_H$, $i = 0, 1, \cdots, m$.

When $H = 2^h$, $h \ge 1$ an integer, Davis and Jedwab proved that $\{a_i\}$ and $\{a_i + 2^{h-1} i_{\pi(1)} + c'\}$ form a Golay complementary pair for any $c' \in \mathbb{Z}_{2^h}$ in the Theorem 3 of [5]. Later on, Paterson generalized this result by replacing $\mathbb{Z}_{2^h}$ with $\mathbb{Z}_H$ [26], where $H \ge 2$ is an even integer.

Fact 1 *Let $a = \{a_i\}_{i=0}^{2^m-1}$ be the sequence given in* (6)*. Then the pair of the sequences a_i and $a_i + \frac{H}{2} i_{\pi(1)} + c'$ form a Golay complementary pair for any $c' \in \mathbb{Z}_H$.*

We define

$$\begin{aligned}
a_{i,0} &= 2\sum_{k=1}^{m-1} i_{\pi(k)} i_{\pi(k+1)} + \sum_{k=1}^{m} c_k i_k + c_0 \\
b_{i,0} &= a_{i,0} + \mu_i \\
a_{i,e} &= a_{i,0} + s_{i,e} \\
b_{i,e} &= b_{i,0} + s_{i,e} = a_{i,e} + \mu_i, 1 \leq e \leq q-1,
\end{aligned}$$

where $c_k \in \mathbb{Z}_4$, $k = 0, 1, \cdots, m$, $s_{i,e}$ and μ_i are defined as one of the following cases:

1. $s_{i,e} = d_{e,0} + d_{e,1} i_{\pi(m)}$, $\mu_i = 2i_{\pi(1)}$ for any $d_{e,0}, d_{e,1} \in \mathbb{Z}_4$.
2. $s_{i,e} = d_{e,0} + d_{e,1} i_{\pi(1)}$, $\mu_i = 2i_{\pi(m)}$ for any $d_{e,0}, d_{e,1} \in \mathbb{Z}_4$.
3. $s_{i,e} = d_{e,0} + d_{e,1} i_{\pi(w)} + d_{e,2} i_{\pi(w+1)}$, $2d_{e,0} + d_{e,1} + d_{e,2} = 0$, $\mu_i = 2i_{\pi(1)}$, or $\mu_i = 2i_{\pi(m)}$ for any $d_{e,0}, d_{e,1}, d_{e,2} \in \mathbb{Z}_4$ and $1 \leq w \leq m-1$.

We construct a pair of 4^q-QAM sequences $A = \{A_i\}_{i=0}^{2^m-1}$ and $B = \{B_i\}_{i=0}^{2^m-1}$ as follows:

$$\begin{aligned}
A_i &= \gamma \sum_{e=0}^{q-1} r_e \omega^{a_{i,e}} \\
B_i &= \gamma \sum_{e=0}^{q-1} r_e \omega^{b_{i,e}},
\end{aligned} \tag{7}$$

where $\gamma = e^{j\pi/4}$, $\omega = \sqrt{-1}$, and $r_e = \frac{2^{q-1-e}}{\sqrt{(4^q-1)/3}}$, $a_{i,e}, b_{i,e} \in \mathbb{Z}_4$, $0 \leq e \leq q-1$.

Fact 2 *The two sequences A and B form a 4^q-QAM Golay complementary pair [19]. Furthermore, for $q = 2$, A and B become 16-QAM Golay complementary pair which were constructed by Chong, Venkataramani and Tarokh in [3]. For $q = 3$, A and B become 64-QAM Golay complementary pair which were presented by Lee and Golomb in [17].*

Remark 1 *Note that there are some typos and missing cases in [3] and [17], which were corrected in [18]. Some additional cases about 64-QAM Golay complementary sequences, which are not of those forms above, were presented in [2].*

3 Perfect Polyphase Sequences

In this section, we summarized the known results of polyphase sequences with perfect even or odd periodic autocorrelation property. Known results on perfect sequences are as follows. Here perfect sequences is the sequence s of length N such that $R_{s,1}(\tau) = 0$ for $1 \leq \tau \leq N-1$.

- Binary sequences: The only known perfect sequence is of length $N = 4$: $(1, 1, 1, -1)$. Jungnickel and Pott [14] conjectured that except for $N = 4$ no other perfect binary sequences exist (circulant Hadamard matrix conjecture). Mossinghoff [23] showed that the conjecture holds for $N < 548964900$.

- Ternary sequences: In [22], Luke and Schotten proved that there does not exist any almost binary sequence s of length $N > 2$. There are ternary sequences given by Ipatov [13] and Hoholdt-Justesen sequences [12].

- Quaternary sequences: Perfect quaternary sequences exist for $N = 2, 4, 8, 16$ (Milewski and Frank-sequences) [6]. Mow [24] that no other perfect quaternary sequences exist.

- Polyphase sequences: Perfect polyphase sequences include Frank-Zadoff-Chu sequences [7, 4], Milewski sequences [25] and their various modifications and combinations [6]. Using those known polyphase sequences, Krengel [16] constructed new perfect polyphase sequences.

Known results on odd perfect sequences are as follows. Here odd perfect sequences is the sequence s of length N such that $R_{s,-1}(\tau) = 0$ for $1 \leq \tau \leq N-1$.

- Binary sequences: The only known perfect sequence is of length $N = 2$: $(1, 1)$ and no other odd perfect sequence exist for $N > 2$ [27, 22].

- Ternary sequences: There exists almost binary sequence s of length $N = q + 1$ (q an odd prime power) with odd perfect property. In [15], Krengel constructed odd perfect ternary sequences by using the shift sequences of m-sequences.

- Quaternary sequences: odd perfect quaternary sequences are known for length $N = 2$ and 4. In [22], the authors conjectured that no other odd-perfect quaternary sequences exist.

- Polyphase sequences: Krengel [16] constructed odd perfect polyphase sequences derived from Frank-Zadoff-Chu sequences and Milewski sequences, and shift sequences of m-sequences.

Using Magma, we exhaustive searched quaternary sequence of length N, $2 \leq N \leq 16$, and there does not exist any sequence s with property $R_{s,\delta}(\tau) = 0$, $1 \leq \tau \leq N-1$, where $\delta = \xi$ or ξ^3, and $\xi = \sqrt{-1}$. We think that there does not exist such kind of perfect quaternary sequence of length N. The following lemma gives the necessary condition to the perfect conjugated cyclically even or odd periodic autocorrelation property.

Lemma 1 *Let s be a sequence over Z_H with $\hat{R}_{s,\delta}(\tau) = 0$ for $1 \leq \tau < N$. Then $\delta \in \{\pm 1\}$, i.e., s has perfect conjugated cyclically even or odd periodic autocorrelation property.*

Proof. The two equalities

$$\begin{aligned} C_s(1) + \delta C_s(N-1) &= 0 \\ C_s(N-1) + \delta C_s(1) &= 0 \end{aligned}$$

indicate that $C_s(1) - \delta^2 C_s(1) = (1-\delta^2)C_s(1) = 0$. Since $|C_s(1)| = 1 \neq 0$, then $1 - \delta^2 = 0$ or $\delta = \pm 1$.

□

In the next section, we will show that some quaternary Golay sequences have perfect conjugated cyclically even or odd periodic autocorrelation property.

4 Perfect Cyclically Conjugated Golay Sequences

In this section, we study the cyclically conjugated even periodic and odd periodic autocorrelation property of quaternary Golay sequences defined by (6).

4.1 Main results

Theorem 1 *For the quaternary Golay sequence defined by* (6)*, the sequence is a perfect cyclically conjugated even-periodic sequence if*

(A) $\pi(1) = 1$, $c_{\pi(1)} \in \mathbb{Z}_4$, $c_{\pi(2)}, c_{\pi(m)} \in \{1,3\}$, *and* $c_{\pi(k)} \in \{0,2\}$, $3 \leq k \leq m-1$.

(B) $\pi(m) = 1$, $c_{\pi(m)} \in \mathbb{Z}_H$, $c_{\pi(m-1)}, c_{\pi(1)} \in \{1,3\}$, *and* $c_{\pi(k)} \in \{0,2\}$, $2 \leq k \leq m-2$.

Theorem 2 *For the quaternary Golay sequence defined by* (6)*, the sequence is a perfect cyclically conjugated odd periodic sequence if*

(A) $\pi(1)=1$, $c_{\pi(1)}\in\mathbb{Z}_4$, $c_{\pi(2)}\in\{1,3\}$, *and* $c_{\pi(k)}\in\{0,2\}$, $k\geq 3$.

(B) $\pi(m)=1$, $c_{\pi(m)}\in\mathbb{Z}_4$, $c_{\pi(m-1)}\in\{1,3\}$, *and* $c_{\pi(k)}\in\{0,2\}$, $k\leq m-2$.

As a illustration, we give four quaternary sequences in the following examples, where we always assume that $m=4$ and π is a permutation of $\{1,2,3,4\}$.

Example 1 *Let* π *be the identity permutation of* $\{1,2,3,4\}$ *and* $(c_0,c_1,c_2,c_3,c_4)=(0,0,1,0,1)$. *Then such Golay sequence* $a=(0,1,0,3,1,2,3,2,0,1,0,3,3,0,1,0)$ *is a quaternary sequence with perfect cyclically conjugated even periodic autocorrelation.*

Example 2 *Le* π *be the identity permutation of* $\{1,2,3,4\}$ *and* $(c_0,c_1,c_2,c_3,c_4)=(0,0,1,0,0)$. *Then such Golay sequence* $a=(0,0,0,2,1,1,3,1,0,0,0,2,3,3,1,3)$ *is a quaternary sequence with perfect cyclically conjugated odd periodic autocorrelation.*

Example 3 *Le* $\pi=(4,3,2,1)$ *and* $(c_0,c_{\pi(1)},c_{\pi(2)},c_{\pi(3)},c_{\pi(4)})=(0,1,0,1,0)$. *Then such Golay sequence* $a=(0,1,0,3,1,2,3,2,0,1,0,3,3,0,1,0)$ *is a quaternary sequence with perfect cyclically conjugated even periodic autocorrelation.*

Example 4 *Let* $\pi=(4,3,2,1)$ *and* $(c_0,c_{\pi(1)},c_{\pi(2)},c_{\pi(3)},c_{\pi(4)})=(0,0,0,1,0)$. *Then such Golay sequence* $a=(0,0,0,2,1,1,3,1,0,0,0,2,3,3,1,3)$ *is a quaternary sequence with perfect cyclically conjugated odd periodic autocorrelation.*

4.2 Proofs of the main results

In the remainder of this paper, for an integer τ, $1\leq\tau\leq 2^m-1$, $0\leq i,i'\leq 2^m-1-\tau$ and $0\leq u\leq\tau-1$, we set $j=i+\tau$, $j'=i'+\tau$, $v=u+2^m-\tau$, and let $(i_1,\cdots,i_m)$, $(i'_1,\cdots,i'_m)$, $(j_1,\cdots,j_m)$, $(j'_1,\cdots,j'_m)$, $(u_1,u_2,\cdots,u_m)$ and $(v_1,v_2,\cdots,v_m)$ be the binary representations of i, i', j, j', u and v, respectively. By the definition of the aperiodic autocorrelation, we have

$$\mathrm{C}_a(\tau) \;=\; \sum_{i=0}^{2^m-1-\tau}\xi^{a_i-a_j}$$

Now we partition $\{i : 0 \le i \le 2^m - 1 - \tau\}$ into the following three disjoint subsets:

$$\begin{aligned} J_1(\tau) &= \{0 \le i < 2^m - \tau : i_{\pi(1)} = j_{\pi(1)}\} \\ J_2(\tau) &= \{0 \le i < 2^m - \tau : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(m)} = j_{\pi(m)}\} \\ J_3(\tau) &= \{0 \le i < 2^m - \tau : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(m)} \ne j_{\pi(m)}\}. \end{aligned}$$

Hence, we have

$$\sum_{i=0}^{2^m-1-\tau} \xi^{a_i - a_j} = \sum_{i \in J_1(\tau)} \xi^{a_i - a_j} + \sum_{i \in J_2(\tau)} \xi^{a_i - a_j} + \sum_{i \in J_3(\tau)} \xi^{a_i - a_j}. \tag{8}$$

Lemma 2 $\sum_{i \in J_1(\tau)} \xi^{a_i - a_j} = 0$.

Proof. Since $j \ne i$, we can define z as follows:

$$z = \min\{1 \le k \le m : i_{\pi(k)} \ne j_{\pi(k)}\}. \tag{9}$$

Obviously, $z \ge 2$.

For any $i \in J_1(\tau)$, let i' and j' be the two integers whose bits in the binary representation are defined by

$$i'_{\pi(k)} = \begin{cases} i_{\pi(k)}, & k \ne z-1 \\ 1 - i_{\pi(k)}, & k = z-1 \end{cases} \tag{10}$$

and

$$j'_{\pi(k)} = \begin{cases} j_{\pi(k)}, & k \ne z-1 \\ 1 - j_{\pi(k)}, & k = z-1. \end{cases} \tag{11}$$

In other words, i' and j' are obtained from i and j by “flipping” the $(z-1)$-th bit in $(i_{\pi(1)}, \cdots, i_{\pi(m)})$ and $(j_{\pi(1)}, \cdots, j_{\pi(m)})$. Note that the following facts hold.

- $i \to i'$ is a one-to-one mapping.
- $j' - i' = j - i = \tau$.
- $i'_{\pi(1)} = j'_{\pi(1)}$.

Therefore, i' enumerates all the elements in $J_1(\tau)$ as i ranges over $J_1(\tau)$.

Given $i \in J_1(\tau)$, by the definition of z in (9) we then have

$$\begin{aligned} a_i - a_j - a_{i'} + a_{j'} &= \begin{cases} 2(i_{\pi(2)} + j_{\pi(2)}), & z = 2 \\ 2(i_{\pi(z-2)} + j_{\pi(z-2)} + i_{\pi(z)} + j_{\pi(z)}), & z > 2 \end{cases} \\ &= 2, \end{aligned}$$

which indicates that $\xi^{a_i - a_j}/\xi^{a_{i'} - a_{j'}} = -1$, i.e.,

$$\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0.$$

Hence, we have

$$\begin{aligned} 2 \sum_{i \in J_1(\tau)} \xi^{a_i - a_j} &= \sum_{i \in J_1(\tau)} \xi^{a_i - a_j} + \sum_{i' \in J_1(\tau)} \xi^{a_{i'} - a_{j'}} \\ &= \sum_{i \in J_1(\tau)} \left(\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} \right) = 0. \end{aligned}$$

□

Lemma 3 $\sum_{i \in J_2(\tau)} \xi^{a_i - a_j} = 0.$

Proof. For the case $i \in J_2(\tau)$, setting i' and j' to be the two integers defined by

$$i'_{\pi(k)} = 1 - j_{\pi(k)}, \quad k = 1, \cdots, m \tag{12}$$

and

$$j'_{\pi(k)} = 1 - i_{\pi(k)}, \quad k = 1, \cdots, m. \tag{13}$$

Similar to the discussion of $i \in J_1(\tau)$, we can prove that

$$a_i - a_j - a_{i'} + a_{j'} = i_{\pi(1)} + j_{\pi(1)} + i_{\pi(m)} + j_{\pi(m)} = 2$$

for $i \in J_2(\tau)$, which results in $\sum_{i \in J_2(\tau)} \xi^{a_i - a_j} = 0$.

□

Note that for the cases $J_1(\tau)$ and $J_2(\tau)$, their proofs are independent of the choice of permutation π and the linear part $\sum_{i=1}^{m} c_i x_i + c_0$. Therefore, by Lemmas 2 and 3, (8) can be reduced as

$$\mathrm{C}_a(\tau) = \sum_{i \in J_3(\tau)} \xi^{a_i - a_j}.$$

Replacing τ by $2^m - \tau$, similarly we have

$$\mathrm{C}_a(2^m - \tau) = \sum_{i \in J_3(2^m-\tau)} \xi^{a_i - a_j}.$$

Note that

$$\begin{aligned} F_a(\tau) &= \mathrm{C}_a(\tau) + \mathrm{C}_a(2^m - \tau) \\ \hat{F}_a(\tau) &= \mathrm{C}_a(\tau) - \mathrm{C}_a(2^m - \tau). \end{aligned}$$

We have

$$F_a(\tau) = \sum_{i \in J_3(\tau)} \xi^{a_i - a_j} + \sum_{i \in J_3(2^m-\tau)} \xi^{a_i - a_j} \tag{14}$$

and

$$\hat{F}_a(\tau) = \sum_{i \in J_3(\tau)} \xi^{a_i - a_j} - \sum_{i \in J_3(2^m-\tau)} \xi^{a_i - a_j}. \tag{15}$$

Proof of Theorem 1: First we prove the case (A). To prove that a is a sequence with perfect conjugated cyclically even periodic sequence is equivalent to show that the left side of (14) is equal to zero.

For any given $i \in J_3(\tau)$, since $j > i$, $\pi(1) = 1$ and $i_{\pi(1)} \neq j_{\pi(1)}$, we have $i_{\pi(1)} = 0$ and $j_{\pi(1)} = 1$. In this case, let u and v be the two integers whose bits in the binary representation are defined by

$$u_{\pi(k)} = \begin{cases} i_{\pi(k)}, & k = 1 \\ j_{\pi(k)}, & k \neq 1 \end{cases} \tag{16}$$

and

$$v_{\pi(k)} = \begin{cases} j_{\pi(k)}, & k = 1 \\ i_{\pi(k)}, & k \neq 1. \end{cases} \tag{17}$$

It is obvious to see that $0 \leq u, v \leq 2^n - 1$. Note that the following facts hold.

- $i \to v$ is a one-to-one mapping.
- $v - u = 2^{m-1}(j_{\pi(1)} - i_{\pi(1)}) + \sum_{k=2}^{m} 2^{m-\pi(k)}(i_{\pi(k)} - j_{\pi(k)}) = 2^m - (j - i) = 2^m - \tau$.

Therefore, u enumerates all the elements in $J_3(2^m - \tau)$ as i ranges over $J_3(\tau)$. We also have

$$\begin{aligned}
& (a_i - a_j) - (a_u - a_v) \\
= \quad & 2(i_{\pi(1)} - j_{\pi(1)})(i_{\pi(2)} - j_{\pi(2)}) + \sum_{k=2}^{m} 2c_{\pi(k)}(i_{\pi(k)} - j_{\pi(k)}) \\
= \quad & 2(i_{\pi(1)} - j_{\pi(1)} + 1)(i_{\pi(2)} - j_{\pi(2)}) + \sum_{k=3}^{m} 2c_{\pi(k)}(i_{\pi(k)} - j_{\pi(k)}) = 2,
\end{aligned}$$

where the second identity comes from $c_{\pi(2)} \in \{1, 3\}$, and the last identity follows from to $c_{\pi(m)} \in \{1, 3\}$, $c_{\pi(k)} \in \{0, 2\}$, $3 \leq k \leq m - 1$, $i_{\pi(1)} \neq j_{\pi(1)}$ and $i_{\pi(m)} \neq j_{\pi(m)}$. The equality above indicates $\xi^{a_i - a_j}/\xi^{a_u - a_v} = -1$, or

$$\xi^{a_i - a_j} + \xi^{a_u - a_v} = 0.$$

In this way, the two terms will cancel each other. Compute

$$\sum_{i \in J_3(\tau)} \xi^{a_i - a_j} + \sum_{u \in J_3(2^m - \tau)} \xi^{a_u - a_v} = \sum_{i \in J_3(\tau)} (\xi^{a_i - a_j} + \xi^{a_u - a_v}) = 0.$$

Hence, the equality (14) is equal to zero. Then we finish the proof for the case (i).

For the case (B), by defining a mapping $\pi'(k) = \pi(m+1-k)$, $k \in \{1, \cdots, m\}$, and replacing π by π', the conclusion follows from that in case (A).

$\square$

Proof of Theorem 2: To prove that a is a sequence with perfect conjugated cyclically odd periodic autocorrelation is equivalent to show that the left side of (15) is equal to zero. By similar discussion to that in Theorem 1, it is easily checked that for $i \in J_3(\tau)$

$$(a_i - a_j) - (a_u - a_v) = 2(i_{\pi(1)} - j_{\pi(1)})(i_{\pi(2)} - j_{\pi(2)}) + \sum_{i=2}^{m} 2c_{\pi(i)}(i_{\pi(i)} - j_{\pi(i)}) = 0.$$

which indicates $\xi^{a_i-a_j}/\xi^{a_u-a_v}=1$, or

$$\xi^{a_i-a_j}-\xi^{a_u-a_v}=0.$$

The conclusions then follow.

$\square$

5 Perfect Cyclically Conjugated 4^q-QAM Golay Sequences

In this section, using the perfect quaternary sequences derived in the Section, we will show that 4^q-QAM Golay sequences also have the perfect cyclically conjugated even periodic and odd periodic autocorrelation property.

5.1 Main results

Theorem 3 *Let A be the 4^q-QAM Golay sequence defined by Definition 7. Then the sequence A has perfect cyclically conjugated even periodic autocorrelation property if*

(A) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{0,1,2,3\}\times\{1,3\}\times\{0,2\}^{m-3}\times\{1,3\}$, $\pi(1)=1$ *and* $s_{i,e}=d_{e,0}+2i_{\pi(k)}+2i_{\pi(k+1)}$, $e=1,2,\cdots,q-1$, $d_{e,0}=0,2$, $2\leq k\leq m-1$.

(B) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{1,3\}\times\{0,2\}^{m-3}\times\{1,3\}\times\{0,1,2,3\}$, $\pi(m)=1$ *and* $s_{i,e}=d_{e,0}+2i_{\pi(k)}+2i_{\pi(k+1)}$, $d_{e,0}=0,2$, $e=1,2,\cdots,q-1$, $1\leq k\leq m-2$.

(C) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{0,1,2,3\}\times\{1,3\}\times\{0,2\}^{m-3}\times\{1,3\}$, $\pi(1)=1$ *and* $s_{i,1}=d_{1,0}+d_{1,1}i_{\pi(1)}$, $(d_{1,0},d_{1,1})\in\{(1,2),(3,2)\}$.

(D) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{1,3\}\times\{0,2\}^{m-3}\times\{1,3\}\times\{0,1,2,3\}$, $\pi(m)=1$ *and* $s_{i,1}=d_{1,0}+d_{1,1}i_{\pi(m)}$, $(d_{1,0},d_{1,1})\in\{(1,2),(3,2)\}$.

Theorem 4 *Let A be the 4^q-QAM Golay sequence defined by Definition 7 with $s_{i,e}=d_{e,0}+2i_{\pi(k)}+2i_{\pi(k+1)}$, $e=1,2\cdots,q-1$, $2\leq k\leq m-1$. Then the sequence A has perfect cyclically conjugated odd periodic autocorrelation property if*

(A) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{0,1,2,3\}\times\{1,3\}\times\{0,2\}^{m-2}$, $\pi(1)=1$ *and* $s_{i,e}=d_{e,0}+2i_{\pi(k)}+2i_{\pi(k+1)}$, $d_{e,0}=0,2$, $e=1,2,\cdots,q-1$, $2\leq k\leq m-1$.

(B) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{0,2\}^{m-2}\times\{1,3\}\times\{0,1,2,3\}$, $\pi(m)=1$ *and* $s_{i,e}=d_{e,0}+2i_{\pi(k)}+2i_{\pi(k+1)}$, $d_{e,0}=0,2$, $e=1,2,\cdots,q-1$, $1\le k\le m-2$.

(C) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{0,1,2,3\}\times\{1,3\}\times\{0,2\}^{m-2}$, $\pi(1)=1$ *and* $s_{i,1}=d_{1,0}+d_{1,1}i_{\pi(1)}$, $(d_{1,0},d_{1,1})\in\{(1,2),(3,2)\}$.

(D) $(c_{\pi(1)},\cdots,c_{\pi(m)})\in\{0,2\}^{m-2}\times\{1,3\}\times\{0,1,2,3\}$, $\pi(m)=1$ *and* $s_{i,1}=d_{1,0}+d_{1,1}i_{\pi(m)}$, $(d_{1,0},d_{1,1})\in\{(1,2),(3,2)\}$.

5.2 Proofs of main results

Proof of Theorem 3: For convenience of description, denote $s_{i,0}=0$, $0\le i\le 2^m-1$. Consider the aperiodic autocorrelation of 4^q-QAM Golay complementary sequence A:

$$\begin{aligned}C_A(\tau) &= \sum_{i=0}^{2^m-1-\tau}(\sum_{e=0}^{q-1}r_e\xi^{a_i+s_{i,e}})(\sum_{f=0}^{q-1}r_f\xi^{a_i+s_{i,f}})^*\\ &= \sum_{i=0}^{2^m-1-\tau}(\sum_{e,f=0}^{q-1}r_er_f\xi^{s_{i,e}-s_{j,f}})\xi^{a_i-a_j}.\end{aligned}$$

Hence the cyclically conjugated even periodic autocorrelation of 4^q-QAM Golay complementary sequence A is equal to

$$\begin{aligned}F_A(\tau) &= \sum_{i=0}^{2^m-1-\tau}(\sum_{e,f=0}^{q-1}r_er_f\xi^{s_{i,e}-s_{j,f}})\xi^{a_i-a_j}+\sum_{u=0}^{\tau-1}(\sum_{e,f=0}^{q-1}r_er_f\xi^{s_{u,e}-s_{v,f}})\xi^{a_u-a_v}\\ &= \sum_{e,f=1}^{q-1}r_er_f\left(\sum_{i=0}^{2^m-\tau-1}\xi^{a_i-a_j+s_{i,e}-s_{j,f}}+\sum_{u=0}^{\tau-1}\xi^{a_u-a_v+s_{u,e}-s_{v,f}}\right)\\ &\quad+\sum_{e=1}^{q-1}r_0r_e\left(\sum_{i=0}^{2^m-\tau-1}\xi^{a_i-a_j}(\xi^{s_{i,e}}+\xi^{-s_{j,e}})+\sum_{u=0}^{\tau-1}\xi^{a_u-a_v}(\xi^{s_{u,e}}+\xi^{-s_{v,e}})\right)\\ &\quad+r_0^2\left(\sum_{i=0}^{2^m-\tau-1}\xi^{a_i-a_j}+\sum_{u=0}^{\tau-1}\xi^{a_u-a_v}\right).\end{aligned}$$

Note that $s_{i,e}-s_{j,f}=d_{e,0}-d_{f,0}+2(i_{\pi(k)}+i_{\pi(k+1)}-j_{\pi(k)}-j_{\pi(k+1)})$ for any $1\le e,f\le q-1$. Note that both $\{a_i\}$ and $\{a_i+2(i_{\pi(k)}+i_{\pi(k+1)})\}$ are two perfect cyclically conjugated even periodic autocorrelation sequences over $\mathbb{Z}_4$, i.e.,

$$\sum_{u=0}^{2^m-\tau-1} \xi^{a_i-a_j+s_{i,e}-s_{j,f}} + \sum_{u=0}^{\tau-1} \xi^{a_u-a_v+s_{u,e}-s_{v,f}} = 0$$

and

$$\sum_{i=0}^{2^m-\tau-1} \xi^{a_i-a_j} + \sum_{u=0}^{\tau-1} \xi^{a_u-a_v} = 0.$$

Thus, $F_A(\tau)$ can be reduced as

$$F_A(\tau) \quad = \quad \sum_{e=1}^{q-1} r_0 r_e \left(\sum_{i=0}^{2^m-\tau-1} \xi^{a_i-a_j}(\xi^{s_{i,e}} + \xi^{-s_{j,e}}) + \sum_{u=0}^{\tau-1} \xi^{a_u-a_v}(\xi^{s_{u,e}} + \xi^{-s_{v,e}}) \right).$$

Similar to Section 4, the set $\{i : 0 \leq i \leq 2^m - 1 - \tau\}$ can be divided into three disjoint subsets $J_1(\tau)$, $J_2(\tau)$ and $J_3(\tau)$. By the similar argument, we can check that the following equalities hold

$$\begin{aligned}
\xi^{s_{i,e}} + \xi^{-s_{j,e}} &= \xi^{s_{i',e}} + \xi^{-s_{j',e}}, \ i \in J_1(\tau) \\
\xi^{s_{i,e}} + \xi^{-s_{j,e}} &= \xi^{s_{i',e}} + \xi^{-s_{j',e}}, \ i \in J_2(\tau) \\
\xi^{s_{i,e}} + \xi^{-s_{j,e}} &= \xi^{s_{u,e}} + \xi^{-s_{v,e}}, \ i \in J_3(\tau)
\end{aligned}$$

where i' and j' for $i \in J_1(\tau)$ are given by (10) and (11); i' and j' for $i \in J_2(\tau)$ are given by (12) and (13); and u and v for $i \in J_3(\tau)$ are given by (16) and (17). Then we have

$$\begin{aligned}
\xi^{a_i-a_j}(\xi^{s_{i,e}} + \xi^{-s_{j,e}}) + \xi^{a_{i'}-a_{j'}}(\xi^{s_{i',e}} + \xi^{-s_{j',e}}) &= 0, \ i \in J_1(\tau) \\
\xi^{a_i-a_j}(\xi^{s_{i,e}} + \xi^{-s_{j,e}}) + \xi^{a_{i'}-a_{j'}}(\xi^{s_{i',e}} + \xi^{-s_{j',e}}) &= 0, \ i \in J_2(\tau) \\
\xi^{a_i-a_j}(\xi^{s_{i,e}} + \xi^{-s_{j,e}}) + \xi^{a_u-a_v}(\xi^{s_{u,e}} + \xi^{-s_{v,e}}) &= 0, \ i \in J_3(\tau)
\end{aligned}$$

which indicates that

$$\sum_{i=0}^{2^m-\tau-1} \xi^{a_i-a_j}(\xi^{s_{i,e}} + \xi^{-s_{j,e}}) + \sum_{u=0}^{\tau-1} \xi^{a_u-a_v}(\xi^{s_{u,e}} + \xi^{-s_{v,e}}) = 0$$

or $F_A(\tau) = 0$.

$\square$

Proof of Theorem 4: The proof is quite similar to that of Theorem 3. For simplicity, we omit it.

□

6 Conclusion

In this paper, we introduced two new kinds of autocorrelation of a sequence: cyclically conjugated even periodic autocorrelation and cyclically conjugated odd periodic autocorrelation. In particular, we proposed several classes of quaternary Golay sequences and 4^q-QAM Golay sequences with such perfect autocorrelation property, where q is a positive integer with $q \geq 2$. An interesting problem is to search new sequences with perfect cyclically conjugated even periodic autocorrelation and cyclically conjugated odd periodic autocorrelation.

Acknowledgement

The authors wish to thank Professor Matthew G. Parker for valuable comments and suggestions on the terminology of cyclically conjugated autocorrelation.

References

[1] K.T. Arasu, W. Launey, and S.L. Ma, "On circulant complex Hadamard matrices," *Designs, Codes and Cryptography*, vol. 25, pp. 123-142, 2005.

[2] C. Y. Chang, Y. Li, and J. Hirata, "New 64-QAM Golay complementary sequences," *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2479-2485, May. 2010.

[3] C. V. Chong, R. Venkataramani, and V. Tarokh, "A new construction of 16-QAM Golay complementary sequences," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 2953-2959, Nov. 2003.

[4] D.C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inf. Theory*, vol. 18, no. 4, pp. 531-532, 1972.

[5] J.A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2397–2417, Nov. 1999.

[6] P.Z. Fan and M. Darnell, *Sequence design for communications applications*, Research Studies Press, John Wiley & Sons Ltd, London, 1996.

[7] R. Frank, S. Zadoff, and R. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory*, vol. 8, no. 6, pp. 381-382, 1962.

[8] M.J.E. Golay, "Multislit spectroscopy," *J. Opt. Soc. Amer.*, vol. 39, pp. 437–444, 1949.

[9] M.J.E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. 7, pp. 82–87, 1961.

[10] M.J.E. Golay, "Note on "Complementary series"," *Proc. IRE*, vol. 50, pp. 84, 1962.

[11] S. W. Golomb and G. Gong, *Signal Designs With Good Correlation: For Wireless Communication, Cryptography and Radar Applications.* Cambridge, U.K: Cambridge Univeristy Press, 2005.

[12] T. Hoholdt, and J. Justesen, "Ternary sequences with perfect periodic auto-correlation," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 4, pp. 597-600, 1983.

[13] V.P. Ipatov, "Periodic discrete signals with optimal correlation properties," Moscow, "Radio i svyaz", ISBN-5-256-00986-9, 1992.

[14] D. Jungnickel and A. Pott, "Difference sets: An introduction," *in Difference Sets, Sequences and their Correlation Properties*, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds., 1999, vol. 542, NATO Science Series C, pp. 259-296, 1999.

[15] E.I. Krengel. Almost-perfect and odd-perfect ternary sequences. In T. Helleseth, D. Sarwate, H.-Y., Song, and K. Yang, editors, *Sequences and Their Applications– SETA 2004, Seoul, Korea, October 24-28, 2004, volume 3486 of Lecture Notes in Computer Science*, pages 197-207. Springer, 2005.

[16] E.I. Krengel. Some constructions of almost-perfect, odd-perfect and perfect polyphase and almost-polyphse sequences. In C. Carlet and A. Pott, editors, *Sequences and Their Applications–2010, Paris, France, September 13-17, 2010, volume 6338 of Lecture Notes in Computer Science*, pages 387-398. Springer, 2010.

[17] H. Lee and S.W. Golomb, "A new construction of 64-QAM Golay complementary sequences," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1663-1670, April 2006.

[18] Y. Li, "Commnents on "A new construction of 16-QAM Golay complementary sequences" and extension for 64-QAM Golay sequences," *IEEE Trans. Inform. Theory*, vol. 54, no. 7, pp. 3246-3251, July 2008.

[19] Y. Li, "A construction of general QAM Golay complementary sequences," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5765-5771, May 2010.

[20] N. Levanon, Radar Principles. New York: wiley, 1988.

[21] H.D. Lüke and H.D. Schotten, "Odd-perfect almost binary correlation sequences," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, pp. 495–498, Jan. 1995.

[22] H.D. Lüke and H.D. Schotten. Binary and quadriphase sequence with optimal autocorrelation: A survey. *IEEE Trans. Inform. Theory*, 49(12): 3271-3282, 2003.

[23] M. J. Mossinghoff, "Wieferich pairs and Barker sequences," *Des. Codes Cryptogr.*, vol. 53, no. 3, pp. 1-15, 2009.

[24] W. H. Mow, "A unified construction of perfect polyphase sequences," *in Proc. IEEE Int. Symp. Information Theory (ISIT'95)*, p. 459, 1995.

[25] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," *IBM Journal of Research and Development*, vol. 27, no. 5, pp. 425-431, 1983.

[26] K.G. Paterson, "Generalized Reed-Muller codes and power control for OFDM modulation," *IEEE. Trans. Inform. Theory*, vol. 46, no. 1, pp. 104–120, Feb. 2000.

[27] A. Pott. "Difference triangles and negaperiodic autocorrelation functions," *Discrete Mathematics*, 308(13): 2854-2861, 2008.

[28] M.B. Pursley, *A Introduction to Digital Communications.* Pearson Prentice Hall, U.S, 2005.

[29] M.B. Pursley, "Performance evaluation for phase-coded spread-spectrum multiple-access communication—Part I: System analysis," *IEEE Trans. Inform. Theory*, vol. com-25, no. 8, pp. 795-799, Aug. 1977.

[30] M.B. Pursley, "Performance evaluation for phase-coded spread-spectrum multiple-access communication—Part II: Code sequence analysis," *IEEE Trans. Inform. Theory*, vol. com-25, no. 8, pp. 800-803, Aug. 1977.

[31] D.V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–619, May 1980.

[32] H.D. Schotten, "New optimum ternary complementary sets and almost quadriphase, perfect sequences," *in Int. Conference on Neural Networks and Signal Processing (ICNNSP'95)*, Nanjing, China, Dec. 10-13, 1995, pp. 1106–1109, 1995.

[33] R. Sivaswamy, "Self-clutter cancellation and ambiguity properties of subcomplementary sequences," *IEEE Trans, Aerosp. Electron. Sysr.*, vol. AES-18, pp. 163–180, Mar. 1982.