Large Zero Autocorrelation Zone of Golay Sequences and 4^q-QAM Golay Complementary Sequences

Guang Gong[1] Fei Huo[1] and Yang Yang[2,3]

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

Waterloo, Ontario N2L 3G1, CANADA

[2]Institute of Mobile Communications, Southwest Jiaotong University

Chengdu, 610031, P.R. CHINA

Email: ggong@calliope.uwaterloo.ca, fhuo@engmail.uwaterloo.ca,

yang_data@yahoo.cn

Abstract

Sequences with good correlation properties have been widely adopted in modern communications, radar and sonar applications. In this paper, we present our new findings on some constructions of single H-ary Golay sequence and 4^q-QAM Golay complementary sequence with a large zero autocorrelation zone, where $H \geq 2$ is an arbitrary even integer and $q \geq 2$ is an arbitrary integer. Those new results on Golay sequences and QAM Golay complementary sequences can be explored during synchronization and detection at the receiver end and thus improve the performance of the communication system.

Index Terms. Golay sequence, zero autocorrelation zone (ZACZ), quadrature amplitude modulation (QAM), synchronization, channel estimation.

1 Introduction

In modern communications, sequences with good correlation properties are desired for receiver synchronization and detection purposes. In 1961, Golay proposed the idea of aperiodic complementary sequence pairs [6], of which the sum of out-of-phase aperiodic autocorrelation equals to zero. Later on, Davis and Jedwab formulated a method for constructing Golay complementary pairs by using quadratic generalized boolean functions [3]. Due to this correlation property, Golay sequences have been proposed to construct Hadamard matrix for direct sequence code division multiple access (DS-CDMA) system [21], and to control the peak envelope power (PEP) in orthogonal frequency-division multiplexing (OFDM) system [24, 25, 26, 27].

The utilization of Golay sequences in the two above scenarios are based on the property that the sum of out-of-phase autocorrelation of the pair equals to zero. However, synchronization and detection

[3]Yang Yang is current a visiting Ph. D student (Oct. 2010- Sep. 2012) in the ECE, University of Waterloo.

of the signal is equivalent to computing its own autocorrelation. In this case, investigation of the autocorrelation of single sequence is of our interest in this paper. This is also the case with conventional CDMA and quasi-synchronous code-division multiple-access (QS-CDMA) system.

QS-CDMA differs from conventional CDMA system [7] in that it allows a small time delay in the arrival signals of different users. In this case, sequences with low or zero correlations centered at the origin are desired to eliminate or reduce the multiple access and multipath interference at the receiver end during detection. Such sequences are called low correlation zone (LCZ) and zero correlation zone (ZCZ) sequences respectively [16]. As a result, the construction of new LCZ or ZCZ sequences for QS-CDMA system has received researchers's much attention [4, 5, 9, 10, 12, 17, 18, 22, 23, 28].

Our motivation is to examine the correlation properties of Golay sequences and quadrature amplitude modulation (QAM) Golay complementary sequences when it is being utilized for signal detection and synchronization purposes in applications such as CDMA and conventional linear time invariant (LTI) system. More specifically, if single Golay sequence or QAM Golay complementary sequence inherits some fixed or attractive autocorrelation property which can be exploited during detection and thus improves the performance of the system. Please refer to [2, 13, 14, 1, 15] more details on QAM Golay complementary sequences. In this paper, we will present our findings on several constructions of Golay sequences and QAM Golay complementary sequences with a zero autocorrelation zone (ZACZ) of length approximate an half, a quarter or one eighth of their periods.

This paper is organized as follows. In Section 2, we provide the necessary preliminary materials required in the later sections. In Sections 3 and 4, we show the large ZACZ of Golay sequences and QAM Golay complementary sequences. In Section 5, we demonstrate the ZACZ with concrete examples. Finally, we conclude our paper in Section 6.

2 Definitions and Preliminaries

Let $H \geq 2$ be an arbitrary integer and ξ be the primitive H-th root of unity, i.e., $\xi = \exp(2\pi\sqrt{-1}/H)$. For a sequence $a = (a_0, a_1, \cdots, a_{N-1})$ over Z_H with period N, its *aperiodic autocorrelation function* and *periodic autocorrelation function* are respectively defined by

$$C_a(\tau) = \sum_{i=0}^{N-1-\tau} \xi^{a_i - a_{i+\tau}}, \tau = 0, 1, \cdots,$$

and

$$R_a(\tau) = \sum_{i=0}^{N-1} \xi^{a_i - a_{i+\tau}}, \tau = 0, 1, \cdots.$$

Definition 1 *Let δ_1 and δ_2 be two integers with $0 < \delta_1 < \delta_2 < N$ and denote $L = \delta_2 - \delta_1 + 1$. If the periodic autocorrelation function of a is equal to zero with a range $\delta_1 \le \tau \le \delta_2$, then the sequence a has a zero autocorrelation zone (ZACZ) of length L.*

This definition is a variation of the definition given in [4].

Let a and b be two sequences over Z_H with period N. The 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. The *algebraic degree* is defined by the maximum value of the size of the set I with $a_I \neq 0$.

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.

Definition 2 *Define a sequence $a = \{a_i\}_{i=0}^{2^m-1}$ over $\mathbb{Z}_H$, whose elements are given by*

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

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 [3]. Later on, Paterson generalized this result by replacing $\mathbb{Z}_{2^h}$ with $\mathbb{Z}_H$ [19], where $H \ge 2$ is an arbitrary even integer.

Fact 1 (Corollary 11, [19]) *Let $a = \{a_i\}_{i=0}^{2^m-1}$ be the sequence given in Definition 2. 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 $c_k \in \mathbb{Z}_4$, $k = 0, 1, \cdots, m$, and $s_{i,e}$ 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:

$$
\begin{aligned}
A_i &= \gamma \sum_{e=0}^{q-1} r_j \xi^{a_{i,e}} \\
B_i &= \gamma \sum_{e=0}^{q-1} r_j \xi^{b_{i,e}},
\end{aligned}
\tag{2}
$$

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

Fact 2 (Theorem 2, [15]) *The two sequence A and B form a 4^q-QAM Golay complementary pair. Furthermore, for $q = 2$, A and B become 16-QAM Golay complementary pair which are constructed by Chong, Venkataramani and Tarokh in [2]; For $q = 3$, A and B become 64-QAM Golay complementary pair which are presented by Lee and Golomb in [13].*

Remark 1 *Note that there are some typos and missing cases in the original publication of [2] and [13]. However, those are corrected in [14]. Some additional cases about 64-QAM Golay complementary sequences, which are not of those forms above, are presented in [1].*

In the remaining of this paper, we adopt the following notations: For an integer τ, $1 \leq \tau \leq 2^m - 1$, two integers i and i', $0 \leq i, i', j, j' < 2^m$, we set $j = (i + \tau) \mod 2^m$ and $j' = (i' + \tau) \mod 2^m$, and let $(i_1, \cdots, i_m)$, $(i'_1, \cdots, i'_m)$, $(j_1, \cdots, j_m)$ and $(j'_1, \cdots, j'_m)$ be the binary representations of i, i', j, j', respectively.

3 Zero Autocorrelation Zone of Golay Sequences

In this section, we will study the ZACZ of Golay sequences.

3.1 Pre-described Conditions

In this subsection, we list 3 sets of conditions on permutations π and affine transformation $\sum_{k=1}^{m} c_k i_k + c_0$.

(A) (1) $\pi(1) = 1$, $\pi(2) = 2$ and $2c_1 = 0$.

(2) $\pi(2) = 2$, $\pi(3) = 1$, $\pi(4) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(3) $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$, $2c_1 = 0$ and $c_1 = 2c_2 + t$, where

$$t = \begin{cases} \frac{H}{2}, & \text{for Golay sequences defined by equality (1)} \\ 2, & \text{for QAM Golay complementary sequences defined by equality (2).} \end{cases}$$

(B) $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(C) (1) $\pi(1) = 1$, $\pi(2) = 3$, $\pi(3) = 2$ and $2c_1 = 0$.

(2) $\pi(1) = 1$, $\pi(2) = 3$, $\pi(m) = 2$ and $2c_1 = 0$.

(3) $\pi(1) = 2$, $\pi(2) = 4$, $\pi(3) = 1$, $\pi(4) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(4) $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$, $\pi(4) = 4$, $2c_1 = 0$ and $c_1 = 2c_2$.

Define a mapping $\pi'(k) = \pi(m + 1 - k)$, $k \in \{1, \cdots, m\}$. Replacing π by π', the above three sets of the conditions on permutations π and affine transformation $\sum_{k=1}^{m} c_k i_k + c_0$ above can be written as follows.

(A') (1) $\pi(m) = 1$, $\pi(m-1) = 2$ and $2c_1 = 0$.

(2) $\pi(m-1) = 2$, $\pi(m-2) = 1$, $\pi(m-3) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(3) $\pi(m) = 2$, $\pi(m-1) = 1$, $\pi(m-2) = 3$, $2c_1 = 0$ and $c_1 = 2c_2 + t$, where

$$t = \begin{cases} \frac{H}{2}, & \text{for Golay sequences defined by equality (1)} \\ 2, & \text{for QAM Golay complementary sequences defined by equality (2).} \end{cases}$$

(B') $\pi(m) = 2$, $\pi(m-1) = 1$, $\pi(m-2) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(C') (1) $\pi(m) = 1$, $\pi(m-1) = 3$, $\pi(m-1) = 2$ and $2c_1 = 0$.

(2) $\pi(m) = 1$, $\pi(m-1) = 3$, $\pi(1) = 2$ and $2c_1 = 0$.

(3) $\pi(m) = 2$, $\pi(m-1) = 4$, $\pi(m-2) = 1$, $\pi(m-3) = 3$, $2c_1 = 0$ and $c_1 = 2c_2$.

(4) $\pi(m) = 2$, $\pi(m-1) = 3$, $\pi(m-2) = 1$, $\pi(m-3) = 4$, $2c_1 = 0$ and $c_1 = 2c_2$.

3.2 Main Results

Theorem 1 *If the Golay sequence a, defined by Definition 2, satisfies one of the condition listed in (A) or (A'), then the sequence a has the following property:*

$$R_a(\tau) = 0, \quad \tau \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m).$$

In other words, in one period $[0, 2^m)$, it has two zero autocorrelation zones of length 2^{m-2}, given by $(0, 2^{m-2}]$ and $[3 \cdot 2^{m-2}, 2^m)$, shown in Figure 1.

Figure 1: The Zero Autocorrelation Zone of Golay Sequence a Defined by (1) and Condition (A)

Theorem 2 *If the Golay sequence a, defined by Definition 2, satisfies one of the condition listed in (B) or (B'), then the sequence a has the following property:*

$$R_a(\tau) = 0, \quad \tau \in [2^{m-2}, 3 \cdot 2^{m-2}].$$

In other words, in one period $[0, 2^m)$, it has a zero autocorrelation zone of length $2^{m-1} + 1$, given by $[2^{m-2}, 3 \cdot 2^{m-2}]$, shown in Figure 2.

Theorem 3 *If the Golay sequence a, defined by Definition 2, satisfies one of the condition listed in (C) or (C'), then the sequence a has the following property:*

$$R_a(\tau) = 0, \quad \tau \in (0, 2^{m-3}] \cup [3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}] \cup [7 \cdot 2^{m-3}, 2^m).$$

In other words, in one period $[0, 2^m)$, it has three zero autocorrelation zones of respective length 2^{m-3}, $2^{m-2} + 1$, 2^{m-3}, given by $(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$ and $[7 \cdot 2^{m-3}, 2^m)$, shown in Figure 3.

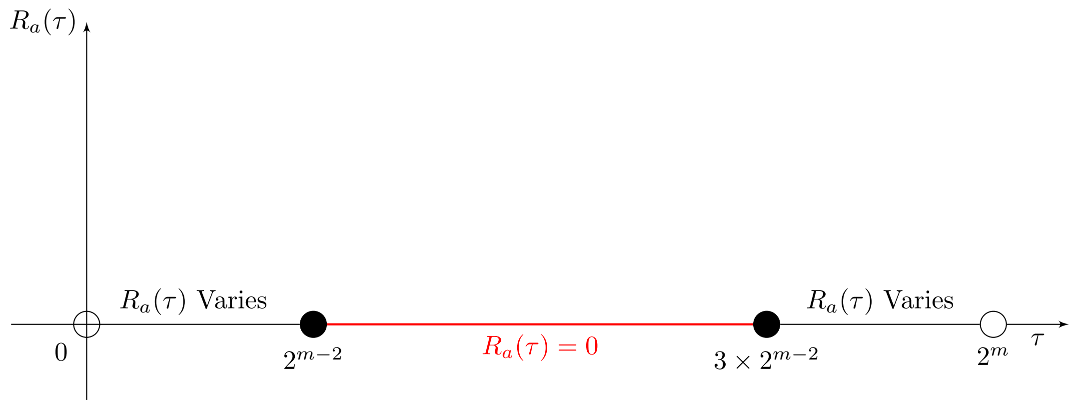

Figure 2: The Zero Autocorrelation Zone of Golay Sequence a Defined by (1) and Condition (B)

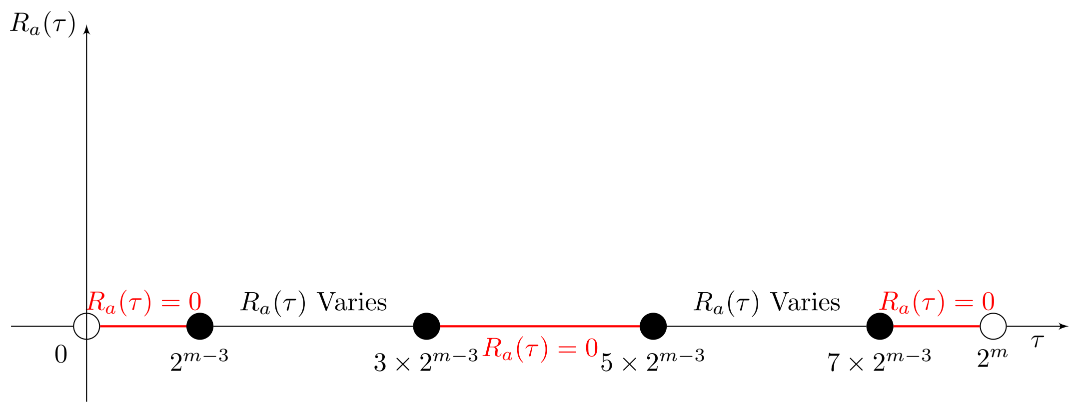

Figure 3: The Zero Autocorrelation Zone of Golay Sequence a Defined by (1) and Condition (C)

3.3 Proofs of the Main Results

The set $\{i : 0 \le i \le 2^m - 1\}$ can be divided into the following three disjoint subsets:

$$\begin{aligned} I_1(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} = j_{\pi(1)}\}; \\ I_2(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(m)} = j_{\pi(m)}\}; \\ I_3(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(m)} \ne j_{\pi(m)}\}. \end{aligned}$$

Then the periodic autocorrelation function $R_a(\tau)$ can be written as

$$R_a(\tau) = \sum_{i=0}^{2^m-1} \xi^{a_i - a_j} = \sum_{i \in I_1(\tau)} \xi^{a_i - a_j} + \sum_{i \in I_2(\tau)} \xi^{a_i - a_j} + \sum_{i \in I_3(\tau)} \xi^{a_i - a_j}. \quad (3)$$

Lemma 1 *For any Golay sequence a given by Definition 2, for an integer τ, $1 \leq \tau \leq 2^m - 1$, we have*

$$\sum_{i \in I_1(\tau)} \xi^{a_i - a_j} \quad = \quad 0.$$

Proof: Since $j = (i+\tau) \mod 2^m \neq i$, for each $i \in I_1(\tau)$, we can define v as follows:

$$v = \min\{1 \leq k \leq m : i_{\pi(k)} \neq j_{\pi(k)}\}.$$

From the definition of $I_1(\tau)$, it is immediately seen that $v \geq 2$. Let i' and j' be two integers with binary representations defined by

$$i'_{\pi(k)} = \begin{cases} i_{\pi(k)}, & k \neq v-1 \\ 1 - i_{\pi(k)}, & k = v-1 \end{cases}$$

and

$$j'_{\pi(k)} = \begin{cases} j_{\pi(k)}, & k \neq v-1 \\ 1 - j_{\pi(k)}, & k = v-1. \end{cases}$$

In other words, i' and j' are obtained from i and j by "flipping" the $(v-1)$-th bit in $(i_{\pi(1)}, \cdots, i_{\pi(m)})$ and $(j_{\pi(1)}, \cdots, j_{\pi(m)})$. We can derive the following results.

1) $j' - i' = j - i \equiv \tau \mod 2^m$ for any $i \in I_1(\tau)$.

2) $i'_{\pi(1)} = j'_{\pi(1)}$.

3) The mapping $i \to i'$ is a one-to-one mapping.

Hence i' enumerates $I_1(\tau)$ as i ranges over $I_1(\tau)$. For any given $i \in I_1(\tau)$, we have

$$a_i - a_j - a_{i'} + a_{j'} = \frac{H}{2}.$$

This equality implies $\xi^{a_i - a_j}/\xi^{a_{i'} - a_{j'}} = -1$, thus

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

Hence we have

$$2 \sum_{i \in I_1(\tau)} \xi^{a_i - a_j} = \sum_{i \in I_1(\tau)} \xi^{a_i - a_j} + \sum_{i' \in I_1(\tau)} \xi^{a_{i'} - a_{j'}} = \sum_{i \in I_1(\tau)} \left(\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}}\right) = 0.$$

Thus it follows that $\sum_{i \in I_1(\tau)} \xi^{a_i - a_j} = 0.$

$\square$

Lemma 2 *For any Golay sequence a given by Definition 2, for an integer τ, $1 \le \tau \le 2^m - 1$, we have*

$$\sum_{i \in I_2(\tau)} \xi^{a_i - a_j} \quad = \quad 0.$$

Proof: For any $i \in I_2(\tau)$, let i' and j' be the two integers with binary representations defined by

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

and

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

We have the following results:

1) $j' - i' = j - i \equiv \tau \mod 2^m$ for any $i \in I_2(\tau)$.

2) $i'_{\pi(1)} \ne j'_{\pi(1)}$ and $i'_{\pi(m)} = j'_{\pi(m)}$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above implies that i' enumerates $I_2(\tau)$ as i ranges over $I_2(\tau)$.

4) $a_i - a_j - a_{i'} + a_{j'} = \frac{H}{2}$. This implies $\xi^{a_i - a_j}/\xi^{a_{i'} - a_{j'}} = -1$, and then $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_2(\tau)$.

Hence the conclusion follows immediately.

□

By Lemmas 1 and 2, the periodic autocorrelation function $R_a(\tau)$ can be reduced as

$$R_a(\tau) = \sum_{i \in I_3(\tau)} \xi^{a_i - a_j}. \tag{4}$$

Now we will present the ZACZ findings of Golay sequences, i.e., equality in (4) is equal to zero.

Note that for the sets $I_1(\tau)$ and $I_2(\tau)$, their proofs are independent of the choice of permutations π and affine transformations $\sum_{i=1}^{m} c_i x_i + c_0$. However for the set $I_3(\tau)$, the proof for each case in Theorem 1 is different.

In order to prove Theorem 1, we need several lemmas on $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$ in the three cases.

Lemma 3 *Let a be the sequence given by Definition 2 and satisfy the condition (A)-(1). Then we have $i_{\pi(2)} \ne j_{\pi(2)}$ for any $i \in I_3(\tau)$, i.e.,*

$$I_3(\tau) \quad = \quad \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} \ne j_{\pi(2)}, i_{\pi(m)} \ne j_{\pi(m)}\}$$

and $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$ for any $\tau \in \{k : 1 \le k \le 2^{m-2}\}$.

Proof: We can partition $I_3(\tau)$ into the following two disjoint subsets:

$$\begin{aligned} I_4(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} = j_{\pi(2)}, i_{\pi(m)} \ne j_{\pi(m)}\}; \\ I_5(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} \ne j_{\pi(2)}, i_{\pi(m)} \ne j_{\pi(m)}\}. \end{aligned}$$

First we will show that $I_4(\tau)$ is an empty set. $i_{\pi(1)} \ne j_{\pi(1)}$ implies that: (i) $(i_{\pi(1)}, j_{\pi(1)}) = (0,1)$; or (ii) $(i_{\pi(1)}, j_{\pi(1)}) = (1,0)$.

(i) On one hand, note that $j \equiv (i+\tau) \bmod 2^m$ together with $i < 2^{m-1}$ and $\tau \le 2^{m-2}$, we have $j = i + \tau < 2^m$. On the other hand, we have

$$i + \tau < 2^{m-1} + 2^{m-2} = j_{\pi(1)} 2^{m-1} + j_{\pi(2)} 2^{m-2} \le j \quad \Rightarrow \quad i + \tau < j$$

which is a contradiction with $j = i + \tau$.

(ii) Note that $j \equiv (i+\tau) \bmod 2^m$ together with $j < 2^{m-1} < i < 2^m$ and $\tau \le 2^{m-2}$, we have $j = i + \tau - 2^m$. Similar as (i), we have

$$\begin{aligned} i + \tau &< (i_{\pi(1)} 2^{m-1} + i_{\pi(2)} 2^{m-2} + 2^{m-2}) + 2^{m-2} \\ &= i_{\pi(2)} 2^{m-2} + 2^m = j_{\pi(2)} 2^{m-2} + 2^m \le j + 2^m \\ &\Rightarrow i + \tau < j + 2^m \end{aligned}$$

which contradicts with that $j = i + \tau - 2^m$.

By the discussion above, we conclude that $I_4(\tau)$ is an empty set and $I_3(\tau) = I_5(\tau)$. Thus we have

$$\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = \sum_{i \in I_5(\tau)} \xi^{a_i - a_j}.$$

For the case $i \in I_5(\tau)$, let i' and j' be two integers with binary representations defined by

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

and

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

We have the following assertions:

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_5(\tau)$.

2) i' satisfies $i'_{\pi(1)} \ne j'_{\pi(1)}$, $i'_{\pi(2)} \ne j'_{\pi(2)}$, and $i'_{\pi(m)} \ne j'_{\pi(m)}$, i.e., $i' \in I_5(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_5(\tau)$ as i ranges over $I_5(\tau)$.

4) $a_i - a_j - (a_{i'} - a_{j'}) = \frac{H}{2}(i_{\pi(2)} + j_{\pi(2)}) + 2c_1(i_{\pi(1)} - j_{\pi(1)}) = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_5(\tau)$.

Hence we have $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = \sum_{i \in I_5(\tau)} \xi^{a_i - a_j} = 0$.

□

Lemma 4 *Let a be the sequence given by Definition 2 and satisfy the condition (A)-(2). Then we have* $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$ *for any* $\tau \in \{k : 1 \le k \le 2^{m-2}\}$.

Proof: We partition $I_3(\tau)$ into the following four disjoint subsets:

$$
\begin{aligned}
I_6(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} = j_{\pi(2)}, i_{\pi(3)} \ne j_{\pi(3)}, i_{\pi(4)} = j_{\pi(4)}, i_{\pi(m)} \ne j_{\pi(m)}\},\\
I_7(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} = j_{\pi(2)}, i_{\pi(3)} = j_{\pi(3)}, i_{\pi(4)} = j_{\pi(4)}, i_{\pi(m)} \ne j_{\pi(m)}\},\\
I_8(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} + j_{\pi(2)} + i_{\pi(4)} + j_{\pi(4)} = 1, i_{\pi(m)} \ne j_{\pi(m)}\}, \text{ and}\\
I_9(\tau) &= \{0 \le i \le 2^m - 1 : i_{\pi(1)} \ne j_{\pi(1)}, i_{\pi(2)} \ne j_{\pi(2)}, i_{\pi(4)} \ne j_{\pi(4)}, i_{\pi(m)} \ne j_{\pi(m)}\}.
\end{aligned}
$$

Similar to the analysis of $I_4(\tau)$, we have that $I_6(\tau)$ is an empty set. Thus

$$\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = \sum_{i \in I_7(\tau)} \xi^{a_i - a_j} + \sum_{i \in I_8(\tau)} \xi^{a_i - a_j} + \sum_{i \in I_9(\tau)} \xi^{a_i - a_j}. \tag{5}$$

Now we will show that

$$\sum_{i \in I_7(\tau)} \xi^{a_i - a_j} = 0 \tag{6}$$

$$\sum_{i \in I_8(\tau)} \xi^{a_i - a_j} = 0 \tag{7}$$

$$\sum_{i \in I_9(\tau)} \xi^{a_i - a_j} = 0. \tag{8}$$

For any given $i \in I_7(\tau)$, let i' and j' be two integers with binary representations defined by

$$i'_{\pi(k)} = \begin{cases} j_{\pi(k)}, & k = 2, 3 \\ 1 - j_{\pi(k)}, & \text{otherwise} \end{cases}$$

and

$$j'_{\pi(k)} = \begin{cases} i_{\pi(k)}, & k = 2, 3 \\ 1 - i_{\pi(k)}, & \text{otherwise.} \end{cases}$$

We have the following results.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_7(\tau)$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, $i'_{\pi(2)} = j'_{\pi(2)}$, $i'_{\pi(3)} = j'_{\pi(3)}$, $i'_{\pi(4)} = j'_{\pi(4)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_7(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_7(\tau)$ as i ranges over $I_7(\tau)$.

4) $a_i - a_j - (a_{i'} - a_{j'}) = \frac{H}{2}(i_{\pi(2)} + j_{\pi(2)} + i_{\pi(3)} + j_{\pi(3)} + i_{\pi(4)} + j_{\pi(4)} + i_{\pi(m)} + j_{\pi(m)}) = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_7(\tau)$.

Hence we have equality (6) holds.

For any given $i \in I_8(\tau)$, let i' and j' be two integers with binary representations defined by

$$i'_{\pi(k)} = \begin{cases} j_{\pi(k)}, & k = 3 \\ 1 - j_{\pi(k)}, & \text{otherwise} \end{cases}$$

and

$$j'_{\pi(k)} = \begin{cases} i_{\pi(k)}, & k = 3 \\ 1 - i_{\pi(k)}, & \text{otherwise.} \end{cases}$$

We have the following assertions.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_8(\tau)$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, $i'_{\pi(2)} + j'_{\pi(2)} + i'_{\pi(4)} + j'_{\pi(4)} = 1$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_8(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above shows that i' enumerates $I_8(\tau)$ as i ranges over $I_8(\tau)$.

4) $a_i - a_j - (a_{i'} - a_{j'}) = \frac{H}{2}(i_{\pi(1)} + j_{\pi(1)} + i_{\pi(2)} + j_{\pi(2)} + i_{\pi(4)} + j_{\pi(4)} + i_{\pi(m)} + j_{\pi(m)}) + 2c_1(i_{\pi(3)} - j_{\pi(3)}) = \frac{H}{2}$. This indicates that $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_8(\tau)$.

Hence equality (7) holds.

Assume $i \in I_9(\tau)$, for convenience, we denote the six-tuple $(i_{\pi(2)}, j_{\pi(2)}, i_{\pi(3)}, j_{\pi(3)}, i_{\pi(4)}, j_{\pi(4)}) \in Z_2^6$ by $\mathcal{A}_1$, and $(i'_{\pi(2)}, j'_{\pi(2)}, i'_{\pi(3)}, j'_{\pi(3)}, i'_{\pi(4)}, j'_{\pi(4)})$ by $\mathcal{B}_1$.

Since $i_{\pi(2)} \neq j_{\pi(2)}$ and $i_{\pi(4)} \neq j_{\pi(4)}$, the six-tuple $\mathcal{A}_1 \in \mathbb{Z}_2^6$ has 16 possibilities listed in Table 1. Note that $\pi(2) = 2$, $\pi(3) = 1$, $\pi(4) = 3$, the sign of $j - i$, will depend on the sign of value $\Delta := \sum_{k=2}^{4}(j_{\pi(k)} - i_{\pi(k)})2^{m-\pi(k)}$. If $\Delta > 0$, $\tau = j - i$; otherwise, $\tau = j + 2^m - i$. When $\tau \in \{k : 1 \leq k \leq 2^{m-2}\}$, we have shown that in the 12 cases, we have $j > i + 2^{m-2} \geq i + \tau$ or $j + 2^m > i + 2^{m-2} \geq i + \tau$. Hence, the six-tuple $\mathcal{A}_1$ must be one of the following four tuples: $(0,1,0,0,1,0)$, $(1,0,0,1,1,0)$, $(0,1,1,1,1,0)$, and $(1,0,1,0,1,0)$. When $k \neq 2,3,4$, let $i'_{\pi(k)} = i_{\pi(k)}$ and $j'_{\pi(k)} = j_{\pi(k)}$. When $k = 2,3,4$, $\mathcal{A}_1$ and $\mathcal{B}_1$ are given in the Table 1. We have the following assertions.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_9(\tau)$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, $i'_{\pi(2)} \neq j'_{\pi(2)}$, $i'_{\pi(4)} \neq j'_{\pi(4)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_9(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_9(\tau)$ as i ranges over $I_9(\tau)$.

4) $a_i - a_j - a_{i'} + a_{j'} = \frac{H}{2}\sum_{k=1}^{4}(i_{\pi(k)}i_{\pi(k+1)} - j_{\pi(k)}j_{\pi(k+1)} - i'_{\pi(k)}i'_{\pi(k+1)} + j'_{\pi(k)}j'_{\pi(k+1)}) + \sum_{k=2}^{4}(i_{\pi(k)} - j_{\pi(k)} - i'_{\pi(k)} + j'_{\pi(k)}) = c_1 - 2c_2 + \frac{H}{2} = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_9(\tau)$.

Hence equality (8) holds.

Table 1: Values of $\mathcal{A}_1$ and their corresponding $\mathcal{B}_1$

Item	$\mathcal{A}_1$	$j-i$	Remark	$\mathcal{B}_1$
1	$(0,1,0,0,0,1)$	>0	$i+2^{m-2} < 2^{m-3}+2^{m-2} \leq j$	
2	$(0,1,0,1,0,1)$	>0	$i+2^{m-2} < 2^{m-3}+2^{m-2} \leq j$	
3	$(0,1,1,0,0,1)$	<0	$i+2^{m-2} < (2^{m-1}+2^{m-3})+2^{m-2} < 2^m+j$	
4	$(0,1,1,1,0,1)$	>0	$i+2^{m-2} < 2^{m-1}+2^{m-3}+2^{m-2} \leq j$	
5	$(1,0,0,0,0,1)$	<0	$i+2^{m-2} < 2^{m-1}+2^{m-2} < 2^m+j$	
6	$(1,0,0,1,0,1)$	>0	$i+2^{m-2} < (2^{m-2}+2^{m-3})+2^{m-2} \leq j$	
7	$(1,0,1,0,0,1)$	<0	$i+2^{m-2} < (2^{m-2}+2^{m-1}+2^{m-3})+2^{m-2}$ $= 2^m+2^{m-3} \leq 2^m+j$	
8	$(1,0,1,1,0,1)$	<0	$i+2^{m-2} < (2^{m-2}+2^{m-1}+2^{m-3})+2^{m-2}$ $< 2^m+2^{m-1}+2^{m-3} \leq 2^m+j$	
9	$*(0,1,0,0,1,0)$	>0		$(1,0,0,1,1,0)$
10	$(0,1,0,1,1,0)$	>0	$i+2^{m-2} < 2^{m-2}+2^{m-2} < 2^{m-2}+2^{m-1} \leq j$	
11	$(0,1,1,0,1,0)$	<0	$i+2^{m-2} < (2^{m-1}+2^{m-2})+2^{m-2} \leq 2^m+j$	
12	$*(0,1,1,1,1,0)$	>0		$(1,0,1,0,1,0)$
13	$(1,0,0,0,1,0)$	<0	$i+2^{m-2} < 2^{m-2}+2^{m-2} \leq 2^m+j$	
14	$*(1,0,0,1,1,0)$	>0		$(0,1,0,0,1,0)$
15	$*(1,0,1,0,1,0)$	<0		$(0,1,1,1,1,0)$
16	$(1,0,1,1,1,0)$	<0	$i+2^{m-2} < 2^m+2^{m-1} \leq 2^m+j$	

By equalities (5)-(8), the conclusion follows immediately.

□

Lemma 5 *Let a be the sequence given by Definition 2 and satisfy the condition (A)-(3). Then we have* $\sum_{i\in I_3(\tau)}\xi^{a_i-a_j}=0$ *for any* $\tau\in\{k:1\le k\le 2^{m-2}\}$.

Proof: We can partition $I_3(\tau)$ into the following two disjoint subsets:

$$\begin{aligned} I_{10}(\tau) &= \{0\le i\le 2^m-1: i_{\pi(1)}\ne j_{\pi(1)}, i_{\pi(3)}=j_{\pi(3)}, i_{\pi(m)}\ne j_{\pi(m)}\};\\ I_{11}(\tau) &= \{0\le i\le 2^m-1: i_{\pi(1)}\ne j_{\pi(1)}, i_{\pi(3)}\ne j_{\pi(3)}, i_{\pi(m)}\ne j_{\pi(m)}\}.\end{aligned}$$

Then $\sum_{i\in I_3(\tau)}\xi^{a_i-a_j}$ can be written as

$$\sum_{i\in I_3(\tau)}\xi^{a_i-a_j}=\sum_{i\in I_{10}(\tau)}\xi^{a_i-a_j}+\sum_{i\in I_{11}(\tau)}\xi^{a_i-a_j}. \tag{9}$$

Now we will show that

$$\sum_{i\in I_{10}(\tau)}\xi^{a_i-a_j} = 0 \tag{10}$$

$$\sum_{i\in I_{11}(\tau)}\xi^{a_i-a_j} = 0 \tag{11}$$

then $\sum_{i\in I_3(\tau)}\xi^{a_i-a_j}=0$.

For any given $i\in I_{10}(\tau)$, let i' and j' be two integers with binary representations defined by

$$i'_{\pi(k)}=\begin{cases} j_{\pi(k)}, & k=2\\ 1-j_{\pi(k)}, & \text{otherwise}\end{cases}$$

and

$$j'_{\pi(k)}=\begin{cases} i_{\pi(k)}, & k=2\\ 1-i_{\pi(k)}, & \text{otherwise.}\end{cases}$$

We have the following results.

1) $j'-i'\equiv j-i\equiv\tau \mod 2^m$ for any $i\in I_{10}(\tau)$.

2) i' satisfies $i'_{\pi(1)}\ne j'_{\pi(1)}$, $i'_{\pi(3)}=j'_{\pi(3)}$, and $i'_{\pi(m)}\ne j'_{\pi(m)}$, i.e., $i'\in I_{10}(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_{10}(\tau)$ as i ranges over $I_{10}(\tau)$.

4) $a_i - a_j - (a_{i'} - a_{j'}) = \frac{H}{2}(i_{\pi(3)} + j_{\pi(3)} + i_{\pi(m)} + j_{\pi(m)}) = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_{10}(\tau)$.

Hence equality (10) holds.

Assume that $i \in I_{11}(\tau)$. For simplicity, we denote $(i_{\pi(1)}, j_{\pi(1)}, i_{\pi(2)}, j_{\pi(2)}, i_{\pi(3)}, j_{\pi(3)})$ by $\mathcal{A}_2$, and $(i'_{\pi(1)}, j'_{\pi(1)}, i'_{\pi(2)}, j'_{\pi(2)}, i'_{\pi(3)}, j'_{\pi(3)})$ by $\mathcal{B}_2$. Using the same argument as $i \in I_9(\tau)$, the six-tuple $\mathcal{A}_2 \in Z_2^6$ must be one of the four following tuples: $(0,1,0,0,1,0)$, $(1,0,0,1,1,0)$, $(0,1,1,1,1,0)$, and $(1,0,1,0,1,0)$.

When $k \neq 1,2,3$, let $i'_{\pi(k)} = i_{\pi(k)}$ and $j'_{\pi(k)} = j_{\pi(k)}$. When $k = 1,2,3$, $\mathcal{A}_2$ and $\mathcal{B}_2$ are given in the Table 2. We have the following results.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_{11}(\tau)$;

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, $i'_{\pi(3)} \neq j'_{\pi(3)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_{11}(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_{11}(\tau)$ as i ranges over $I_{11}(\tau)$.

4) $a_i - a_j - a_{i'} + a_{j'} = \frac{H}{2}\sum_{k=1}^{3}(i_{\pi(k)}i_{\pi(k+1)} - j_{\pi(k)}j_{\pi(k+1)} - i'_{\pi(k)}i'_{\pi(k+1)} + j'_{\pi(k)}j'_{\pi(k+1)}) + \sum_{k=1}^{3}(i_{\pi(k)} - j_{\pi(k)} - i'_{\pi(k)} + j'_{\pi(k)}) = c_1 - 2c_2 = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_{11}(\tau)$.

Hence equality (11) holds.

Table 2: Values of $\mathcal{A}_2$ and their corresponding tuples $\mathcal{B}_2$

Item	$\mathcal{A}_2$	$\mathcal{B}_2$
1	$(0,1,0,0,1,0)$	$(1,0,0,1,1,0)$
2	$(1,0,0,1,1,0)$	$(0,1,0,0,1,0)$
3	$(0,1,1,1,1,0)$	$(1,0,1,0,1,0)$
4	$(1,0,1,0,1,0)$	$(0,1,1,1,1,0)$

By (9), (10) and (11), we finish the proof.

□

Proof of Theorem 1. Note that $R_a(\tau) = R_a(2^m - \tau)$ for any integer τ. By equality (4), it is sufficient to prove that

$$\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0, \quad \tau \in \{k : 1 \leq k \leq 2^{m-2}\}$$

holds for the condition given by (A)-(1), (A)-(2) and (A)-(3). This has been given in Lemmas 3, 4 and 5. Hence, the conclusion holds under the condition (A).

Define a mapping $\pi'(k) = \pi(m+1-k)$, $k \in \{1, \cdots, m\}$. Replacing π by π', the conclusion under the condition (A') follows immediately from the conclusion under the condition (A).

$\square$

Remark 2 *The result in (A)-(1) of Theorem 1 in the case of $H = 2$ has been reported in [8].*

Proof of Theorem 2. Compared with the condition given by (A)-(3) in Theorem 1, the condition given by (B) are the same except for the value of $c_1 - 2c_2$. Because $c_1 - 2c_2$ is only present in $i \in I_{11}(\tau)$, it is sufficient to prove $\sum_{i\in I_{11}(\tau)} \xi^{a_i - a_j} = 0$ to complete the proof for this theorem.

Assume $i \in I_{11}(\tau)$. For simplicity to describe, we denote $(i_{\pi(1)}, j_{\pi(1)}, i_{\pi(2)}, j_{\pi(2)}, i_{\pi(3)}, j_{\pi(3)})$ by $\mathcal{A}_3$, and $(i'_{\pi(1)}, j'_{\pi(1)}, i'_{\pi(2)}, j'_{\pi(2)}, i'_{\pi(3)}, j'_{\pi(3)})$ by $\mathcal{B}_3$.

Since $i_{\pi(1)} \neq j_{\pi(1)}$, $i_{\pi(2)} \neq j_{\pi(2)}$, the six-tuple $\mathcal{A}_3 \in \mathbb{Z}_2^6$ has 16 possibilities listed in Table 3. Note that $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$, the sign of $j - i$, will depend on the sign of the value $\Delta := \sum_{k=1}^{3}(j_{\pi(k)} - i_{\pi(k)})2^{m-\pi(k)}$. If $\Delta > 0$, $\tau = j - i$; otherwise, $\tau = j + 2^m - i$. When $\tau \in \{k : 2^{m-2} \leq k \leq 2^{m-1}\}$, we have shown that in the 12 cases, we have $j > i + 2^{m-1} \geq i + \tau$, $j + 2^m > i + 2^{m-1} \geq i + \tau$, $i + \tau \geq i + 2^{m+2} > j$, or $i + \tau \geq i + 2^{m-2} > 2^m + j$. Hence, the six-tuple $\mathcal{A}_3$ must be one of the following four tuples: $(0,1,0,0,1,0)$, $(1,0,0,1,1,0)$, $(0,1,1,1,1,0)$, and $(1,0,1,0,1,0)$.

When $k \neq 1, 2, 3$, let $i'_{\pi(k)} = i_{\pi(k)}$ and $j'_{\pi(k)} = j_{\pi(k)}$. When $k = 1, 2, 3$, $\mathcal{A}_3$ and $\mathcal{B}_3$ are given in the Table 3. We have the following assertions.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_{11}(\tau)$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, $i'_{\pi(3)} \neq j'_{\pi(3)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_{11}(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above shows that i' enumerates $I_{11}(\tau)$ as i ranges over $I_{11}(\tau)$.

4) $a_i - a_j - a_{i'} + a_{j'} = \frac{H}{2}\sum_{k=1}^{3}(i_{\pi(k)}i_{\pi(k+1)} - j_{\pi(k)}j_{\pi(k+1)} - i'_{\pi(k)}i'_{\pi(k+1)} + j'_{\pi(k)}j'_{\pi(k+1)}) + \sum_{k=1}^{3}(i_{\pi(k)} - j_{\pi(k)} - i'_{\pi(k)} + j'_{\pi(k)}) = c_1 - 2c_2 + \frac{H}{2} = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_{11}(\tau)$.

Hence the equality (11) holds.

Summarizing all cases above, the conclusion holds under the condition (B).

Define a mapping $\pi'(k) = \pi(m+1-k)$, $k \in \{1, \cdots, m\}$. Replacing π by π', the conclusion under the condition (B') follows immediately from the conclusion under the condition (B).

$\square$

In order to prove Theorem 3, we need several lemmas.

Table 3: Possibilities of $\mathcal{A}_3$ and their corresponding tuples $\mathcal{B}_3$

Item	$\mathcal{A}_3$	$j-i$	Remark	$\mathcal{B}_3$
1	$*(0,1,0,0,0,1)$	>0		$(1,0,1,0,0,1)$
2	$(0,1,0,1,0,1)$	>0	$i+2^{m-1}<2^{m-3}+2^{m-1}<j$	
3	$(0,1,1,0,0,1)$	<0	$i+2^{m-1}<(2^{m-1}+2^{m-3})+2^{m-1}<2^m+j$	
4	$*(0,1,1,1,0,1)$	>0		$(1,0,0,1,0,1)$
5	$(1,0,0,0,0,1)$	<0	$i+2^{m-1}<(2^{m-2}+2^{m-3})+2^{m-1}<j+2^m$	
6	$*(1,0,0,1,0,1)$	>0		$(0,1,1,1,0,1)$
7	$*(1,0,1,0,0,1)$	<0		$(0,1,0,0,0,1)$
8	$(1,0,1,1,0,1)$	<0	$i+2^{m-1}<(2^{m-2}+2^{m-1}+2^{m-3})+2^{m-1}$ $=2^m+2^{m-2}+2^{m-3}<2^m+j$	
9	$(0,1,0,0,1,0)$	>0	$i+2^{m-2}\geq 2^{m-3}+2^{m-2}>j$	
10	$(0,1,0,1,1,0)$	>0	$i+2^{m-1}<2\cdot 2^{m-3}+2^{m-1}=2^{m-2}+2^{m-1}\leq j$	
11	$(0,1,1,0,1,0)$	<0	$i+2^{m-1}<(2^{m-1}+2\cdot 2^{m-3})+2^{m-1}\leq 2^m+j$	
12	$(0,1,1,1,1,0)$	>0	$i+2^{m-2}\geq(2^{m-1}+2^{m-3})+2^{m-2}>j$	
13	$(1,0,0,0,1,0)$	<0	$i+2^{m-1}<2^{m-1}+2^{m-1}\leq 2^m+j$	
14	$(1,0,0,1,1,0)$	>0	$i+2^{m-1}<2^{m-1}+2^{m-1}\leq 2^m+j$	
15	$(1,0,1,0,1,0)$	<0	$i+2^{m-2}\geq(2^{m-1}+2^{m-2}+2^{m-3})+2^{m-2}>2^m+j$	
16	$(1,0,1,1,1,0)$	<0	$i+2^{m-1}<2^m+2^{m-1}\leq 2^m+j$	

Lemma 6 *Let a be the sequence given by Definition 2 and satisfy the condition (C)-(1). Then one has* $\sum_{i\in I_3(\tau)}\xi^{a_i-a_j}=0$ *for any* $\tau\in\{k:1\leq k\leq 2^{m-3}\}\cup\{k:3\cdot 2^{m-3}\leq k\leq 2^{m-1}\}$.

Proof: We partition $I_3(\tau)$ into the following three disjoint subsets:

$$\begin{aligned}
I_{12}(\tau) &= \{0\leq i\leq 2^m-1: i_{\pi(1)}\neq j_{\pi(1)}, i_{\pi(2)}=j_{\pi(2)}, i_{\pi(3)}\neq j_{\pi(3)}, i_{\pi(m)}\neq j_{\pi(m)}\};\\
I_{13}(\tau) &= \{0\leq i\leq 2^m-1: i_{\pi(1)}\neq j_{\pi(1)}, i_{\pi(2)}=j_{\pi(2)}, i_{\pi(3)}=j_{\pi(3)}, i_{\pi(m)}\neq j_{\pi(m)}\};\\
I_{14}(\tau) &= \{0\leq i\leq 2^m-1: i_{\pi(1)}\neq j_{\pi(1)}, i_{\pi(2)}\neq j_{\pi(2)}, i_{\pi(m)}\neq j_{\pi(m)}\}.
\end{aligned}$$

First we will show that the subset $I_{12}(\tau)$ is an empty set. In this case, $i_{\pi(1)}\neq j_{\pi(1)}$ and $i_{\pi(3)}\neq j_{\pi(3)}$ implies $(i_{\pi(1)}, j_{\pi(1)}, i_{\pi(3)}, j_{\pi(3)})$ must be one of $(0,1,0,1)$, $(0,1,1,0)$, $(1,0,0,1)$, and $(1,0,1,0)$. When $\tau\in\{k:1\leq k\leq 2^{m-3}\}\cup\{k:3\cdot 2^{m-3}\leq k\leq 2^{m-1}\}$, we have shown that in Tables 4 and 5, we have $j>i+\tau$, $j+2^m>i+\tau$, $i+\tau>j$, or $i+\tau>2^m+j$. This contradicts with $j\equiv(i+\tau)\mod 2^m$.

By the discussion above, the set $I_{12}(\tau)$ is an empty set. Then $\sum_{i\in I_3(\tau)}\xi^{a_i-a_j}$ can be written as

$$\sum_{i\in I_3(\tau)}\xi^{a_i-a_j}=\sum_{i\in I_{13}(\tau)}\xi^{a_i-a_j}+\sum_{i\in I_{14}(\tau)}\xi^{a_i-a_j}. \tag{12}$$

Table 4: The case $\tau \in \{k : 1 \le k \le 2^{m-3}\}$

Item	$(i_{\pi(1)}, j_{\pi(1)}, i_{\pi(3)}, j_{\pi(3)})$	$j-i$	Remark
1	$(0,1,0,1)$	>0	$i+\tau < 2^{m-2}+2^{m-1} = j_{\pi(3)}2^{m-2} + j_{\pi(1)}2^{m-1} \le j$
2	$(0,1,1,0)$	>0	$i+\tau < (i_{\pi(2)}2^{m-3}+2^{m-2}+2^{m-3})+2^{m-3}$ $= i_{\pi(2)}2^{m-3}+2^{m-1} = j_{\pi(2)}2^{m-3}+2^{m-1} \le j$
3	$(1,0,0,1)$	<0	$i+\tau < (i_{\pi(1)}2^{m-1}+i_{\pi(2)}2^{m-3}+2^{m-3})+2^{m-1}$ $< j_{\pi(2)}2^{m-3}+j_{\pi(3)}2^{m-2}+2^m \le j+2^m$
4	$(1,0,1,0)$	>0	$i+\tau < (i_{\pi(1)}2^{m-1}+i_{\pi(2)}2^{m-3}+2^{m-2}+2^{m-3})$ $+2^{m-3} = j_{\pi(2)}2^{m-2}+2^m \le j+2^m$

Table 5: The case $\tau \in \{k : 3 \cdot 2^{m-3} \le k \le 2^{m-1}\}$

Item	$(i_{\pi(1)}, j_{\pi(1)}, i_{\pi(3)}, j_{\pi(3)})$	$j-i$	Remark
1	$(0,1,0,1)$	>0	$i+\tau < 2^{m-2}+2^{m-1} = j_{\pi(3)}2^{m-2} + j_{\pi(1)}2^{m-1} \le j$
2	$(0,1,1,0)$	>0	$i+\tau \ge (i_{\pi(2)}2^{m-3}+2^{m-2})+3\cdot 2^{m-3}$ $= j_{\pi(2)}2^{m-3}+2^{m-1}+2^{m-3} > j$
3	$(1,0,0,1)$	<0	$i+\tau < (i_{\pi(1)}2^{m-1}+i_{\pi(2)}2^{m-3}+2^{m-3})+2^{m-1}$ $< j_{\pi(2)}2^{m-3}+j_{\pi(3)}2^{m-2}+2^m \le j+2^m$
4	$(1,0,1,0)$	>0	$i+\tau \ge (i_{\pi(1)}2^{m-1}+i_{\pi(2)}2^{m-3}+2^{m-2})+3\cdot 2^{m-3}$ $= j_{\pi(2)}2^{m-2}+2^m+2^{m-3} > j+2^m$

Now we will show that

$$\sum_{i \in I_{13}(\tau)} \xi^{a_i - a_j} = 0 \tag{13}$$

$$\sum_{i \in I_{14}(\tau)} \xi^{a_i - a_j} = 0 \tag{14}$$

then $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$.

For the case $i \in I_{13}(\tau)$, let i' and j' be two integers with binary representations defined by

$$i'_{\pi(k)} = \begin{cases} 1 - i_{\pi(k)}, & k = 2 \\ i_{\pi(k)}, & k \ne 2 \end{cases}$$

and

$$j'_{\pi(k)} = \begin{cases} 1 - j_{\pi(k)}, & k = 2 \\ j_{\pi(k)}, & k \ne 2. \end{cases}$$

We can derive the following results.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_{13}(\tau)$ by using $i_{\pi(2)} = j_{\pi(2)}$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, $i'_{\pi(2)} = j'_{\pi(2)}$, $i'_{\pi(3)} = j'_{\pi(3)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_{13}(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above shows that i' enumerates $I_{13}(\tau)$ as i ranges over $I_{13}(\tau)$.

4) $a_i - a_j - (a_{i'} - a_{j'}) = \frac{H}{2}(i_{\pi(1)} + j_{\pi(1)} + i_{\pi(3)} + j_{\pi(3)}) = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_{13}(\tau)$.

Hence equality (13) holds.

For the case $i \in I_{14}(\tau)$, let i' and j' be two integers with binary representations defined by

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

and

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

We can derive the following assertions.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_{14}(\tau)$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, $i'_{\pi(2)} \neq j'_{\pi(2)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_{14}(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_{14}(\tau)$ as i ranges over $I_{14}(\tau)$.

4) $a_i - a_j - (a_{i'} - a_{j'}) = \frac{H}{2}(i_{\pi(2)} + j_{\pi(2)}) = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_{14}(\tau)$.

Hence equality (14) holds.

□

Lemma 7 *Let a be the sequence given by Definition 2 and satisfy the condition (C)-(2). Then one has* $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$ *for any* $\tau \in \{k : 1 \leq k \leq 2^{m-3}\} \cup \{k : 3 \cdot 2^{m-3} \leq k \leq 2^{m-1}\}$.

Proof: The set $I_3(\tau)$ is divided into two disjoint subsets $I_{14}(\tau)$ and $I_{15}(\tau)$, where

$$I_{15}(\tau) = \{0 \leq i \leq 2^m - 1 : i_{\pi(1)} \neq j_{\pi(1)}, i_{\pi(2)} = j_{\pi(2)}, i_{\pi(m)} \neq j_{\pi(m)}\}.$$

Using the same argument as $i \in I_{12}(\tau)$ and $i \in I_{14}(\tau)$, we have that the subset $I_{15}(\tau)$ is an empty set and $\sum_{i \in I_{14}(\tau)} \xi^{a_i - a_j} = 0$. We also have $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = \sum_{i \in I_{14}(\tau)} \xi^{a_i - a_j} = 0$.

□

Lemma 8 *Let a be the sequence given by Definition 2 and satisfy the condition (C)-(3). Then one has* $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$ *where*

$$\tau \in \{k : 1 \le k \le 2^{m-3}\} \cup \{k : 3 \cdot 2^{m-3} \le k \le 2^{m-1}\}.$$

Proof: For simplicity, we denote $(i_{\pi(1)}, j_{\pi(1)}, i_{\pi(2)}, j_{\pi(2)}, i_{\pi(3)}, j_{\pi(3)}, i_{\pi(4)}, j_{\pi(4)})$ by $\mathcal{A}_4$ and the corresponding eight-tuple $(i'_{\pi(1)}, j'_{\pi(1)}, i'_{\pi(2)}, j'_{\pi(2)}, i'_{\pi(3)}, j'_{\pi(3)}, i'_{\pi(4)}, j'_{\pi(4)})$ by $\mathcal{B}_4$.

Assume that $i \in I_3(\tau)$. The eight-tuple $\mathcal{A}_4 \in \mathbb{Z}_2^8$ has 128 possibilities since $i_{\pi(1)} \ne j_{\pi(1)}$. Note that $\pi(1) = 2$, $\pi(2) = 4$, $\pi(3) = 1$, $\pi(4) = 3$, the sign of $j - i$ will depend on the sign of the value $\Delta := \sum_{k=1}^{4} (j_{\pi(k)} - i_{\pi(k)}) 2^{m-\pi(k)}$. If $\Delta > 0$, $\tau = j - i$; otherwise, $\tau = j + 2^m - i$. When $\tau \in \{k : 1 \le k \le 2^{m-3}\} \cup \{k : 3 \cdot 2^{m-3} \le k \le 2^{m-1}\}$, there are 104 possible pairs (i, j) that satisfy $j > i + 2^{m-1} \ge i + \tau$, $j + 2^m > i + 2^{m-1} \ge i + \tau$, $i + \tau \ge i + 2^{m+2} > j$, or $i + \tau \ge i + 2^{m-2} > 2^m + j$. Hence, the eight-tuple $\mathcal{A}_4 \in Z_2^8$ must be one of the remaining 24 possibilities as shown in Table 6. When $k = 1, 2, 3, 4$, the corresponding tuples $\mathcal{B}_4$ are also given for any given $\mathcal{A}_4$. When $k > 4$, let $i'_{\pi(k)} = i_{\pi(k)}$ and $j'_{\pi(k)} = j_{\pi(k)}$.

Table 6: Possibilities of $\mathcal{A}_4$ and their corresponding tuples $\mathcal{B}_4$

Item	$\mathcal{A}_4$	$\mathcal{B}_4$	Item	$\mathcal{A}_4$	$\mathcal{B}_4$
1	(0, 1, 1, 0, 1, 1, 1, 0)	(1, 0, 1, 0, 1, 0, 1, 0)	13	(1, 0, 1, 0, 1, 0, 1, 0)	(0, 1, 1, 0, 1, 1, 1, 0)
2	(0, 1, 1, 0, 0, 0, 1, 0)	(1, 0, 1, 0, 0, 1, 1, 0)	14	(1, 0, 1, 0, 0, 1, 1, 0)	(0, 1, 1, 0, 0, 0, 1, 0)
3	(0, 1, 0, 0, 1, 1, 1, 0)	(1, 0, 0, 0, 0, 1, 1, 0)	15	(1, 0, 0, 0, 0, 1, 1, 0)	(0, 1, 0, 0, 1, 1, 1, 0)
4	(0, 1, 0, 0, 0, 0, 1, 0)	(1, 0, 0, 0, 1, 0, 1, 0)	16	(1, 0, 0, 0, 1, 0, 1, 0)	(0, 1, 0, 0, 0, 0, 1, 0)
5	(0, 1, 1, 1, 0, 0, 1, 0)	(1, 0, 1, 1, 0, 1, 1, 0)	17	(1, 0, 1, 1, 0, 1, 1, 0)	(0, 1, 1, 1, 0, 0, 1, 0)
6	(0, 1, 0, 0, 0, 0, 0, 1)	(1, 0, 0, 0, 0, 1, 0, 1)	18	(1, 0, 0, 0, 0, 1, 0, 1)	(0, 1, 0, 0, 0, 0, 0, 1)
7	(0, 1, 0, 0, 1, 1, 0, 1)	(1, 0, 0, 0, 1, 0, 0, 1)	19	(1, 0, 0, 0, 1, 0, 0, 1)	(0, 1, 0, 0, 1, 1, 0, 1)
8	(0, 1, 0, 1, 0, 0, 0, 1)	(1, 0, 0, 1, 1, 0, 0, 1)	20	(1, 0, 0, 1, 1, 0, 0, 1)	(0, 1, 0, 1, 0, 0, 0, 1)
9	(0, 1, 0, 1, 1, 1, 0, 1)	(1, 0, 0, 1, 0, 1, 0, 1)	21	(1, 0, 0, 1, 0, 1, 0, 1)	(0, 1, 0, 1, 1, 1, 0, 1)
10	(0, 1, 1, 1, 0, 0, 0, 1)	(1, 0, 1, 1, 1, 0, 0, 1)	22	(1, 0, 1, 1, 1, 0, 0, 1)	(0, 1, 1, 1, 0, 0, 0, 1)
11	(0, 1, 1, 1, 1, 1, 0, 1)	(1, 0, 1, 1, 0, 1, 0, 1)	23	(1, 0, 1, 1, 0, 1, 0, 1)	(0, 1, 1, 1, 1, 1, 0, 1)
12	(0, 1, 1, 1, 1, 1, 1, 0)	(1, 0, 1, 1, 1, 0, 1, 0)	24	(1, 0, 1, 1, 1, 0, 1, 0)	(0, 1, 1, 1, 1, 1, 1, 0)

We have the following assertions.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_3(\tau)$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_3(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_3(\tau)$ as i ranges over $I_3(\tau)$.

4) $a_i - a_j - a_{i'} + a_{j'} = \frac{H}{2}\sum_{k=1}^{3}(i_{\pi(k)}i_{\pi(k+1)} - j_{\pi(k)}j_{\pi(k+1)} - i'_{\pi(k)}i'_{\pi(k+1)} + j'_{\pi(k)}j'_{\pi(k+1)}) + \sum_{k=1}^{3}(i_{\pi(k)} - j_{\pi(k)} - i'_{\pi(k)} + j'_{\pi(k)}) = c_1 - 2c_2 + \frac{H}{2} = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_3(\tau)$.

Hence we have $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$.

□

Lemma 9 *Let a be the sequence given by Definition 2 and satisfy the condition (C)-(4). Then one has* $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$ *for any* $\tau \in \{k : 1 \leq k \leq 2^{m-3}\} \cup \{k : 3 \cdot 2^{m-3} \leq k \leq 2^{m-1}\}$.

Proof: For simplicity, we denote $(i_{\pi(1)}, j_{\pi(1)}, i_{\pi(2)}, j_{\pi(2)}, i_{\pi(3)}, j_{\pi(3)}, i_{\pi(4)}, j_{\pi(4)})$ by $\mathcal{A}_5$ and the corresponding eight-tuple $(i'_{\pi(1)}, j'_{\pi(1)}, i'_{\pi(2)}, j'_{\pi(2)}, i'_{\pi(3)}, j'_{\pi(3)}, i'_{\pi(4)}, j'_{\pi(4)})$ by $\mathcal{B}_5$.

Assume $i \in I_3(\tau)$, the eight-tuple $\mathcal{A}_5 \in \mathbb{Z}_2^8$ has 128 possibilities since $i_{\pi(1)} \neq j_{\pi(1)}$. Note that $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$, $\pi(4) = 4$, the sign of $j - i$ will depend on the sign of the value $\Delta := \sum_{k=1}^{4}(j_{\pi(k)} - i_{\pi(k)})2^{m-\pi(k)}$. If $\Delta > 0$, $\tau = j - i$; otherwise, $\tau = j + 2^m - i$. When $\tau \in \{k : 1 \leq k \leq 2^{m-3}\} \cup \{k : 3 \cdot 2^{m-3} \leq k \leq 2^{m-1}\}$, there are 104 pairs (i, j) that satisfy $j > i + 2^{m-1} \geq i + \tau$, $j + 2^m > i + 2^{m-1} \geq i + \tau$, $i + \tau \geq i + 2^{m+2} > j$, or $i + \tau \geq i + 2^{m-2} > 2^m + j$. Hence, the eight-tuple $\mathcal{A}_5 \in Z_2^8$ must be one of the left 24 pairs in Table 7. When $k = 1, 2, 3, 4$, the corresponding tuples $\mathcal{B}_5$ are also given for any given $\mathcal{A}_5$. When $k > 4$, let $i'_{\pi(k)} = i_{\pi(k)}$ and $j'_{\pi(k)} = j_{\pi(k)}$.

We have the following assertions.

1) $j' - i' \equiv j - i \equiv \tau \mod 2^m$ for any $i \in I_3(\tau)$.

2) i' satisfies $i'_{\pi(1)} \neq j'_{\pi(1)}$, and $i'_{\pi(m)} \neq j'_{\pi(m)}$, i.e., $i' \in I_3(\tau)$.

3) The mapping $i \to i'$ is a one-to-one mapping. This together with the two facts above indicates that i' enumerates $I_3(\tau)$ as i ranges over $I_3(\tau)$.

4) $a_i - a_j - a_{i'} + a_{j'} = \frac{H}{2}\sum_{k=1}^{3}(i_{\pi(k)}i_{\pi(k+1)} - j_{\pi(k)}j_{\pi(k+1)} - i'_{\pi(k)}i'_{\pi(k+1)} + j'_{\pi(k)}j'_{\pi(k+1)}) + \sum_{k=1}^{3}(i_{\pi(k)} - j_{\pi(k)} - i'_{\pi(k)} + j'_{\pi(k)}) = c_1 - 2c_2 + \frac{H}{2} = \frac{H}{2}$. This implies $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$ for any $i \in I_3(\tau)$.

Hence we have $\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$.

□

Table 7: Possibilities of $\mathcal{A}_5$ and their corresponding tuples $\mathcal{B}_5$

Item	$\mathcal{A}_5$	$\mathcal{B}_5$	Item	$\mathcal{A}_5$	$\mathcal{B}_5$
1	$(0,1,1,0,1,1,1,0)$	$(1,0,1,0,1,0,1,0)$	13	$(1,0,1,0,1,0,1,0)$	$(0,1,1,0,1,1,1,0)$
2	$(0,1,1,0,0,0,1,0)$	$(1,0,1,0,0,1,1,0)$	14	$(1,0,1,0,0,1,1,0)$	$(0,1,1,0,0,0,1,0)$
3	$(0,1,0,1,0,0,0,0)$	$(1,0,0,1,1,0,0,0)$	15	$(1,0,0,1,1,0,0,0)$	$(0,1,0,1,0,0,0,0)$
4	$(0,1,0,1,0,0,1,1)$	$(1,0,0,1,0,1,1,1)$	16	$(1,0,0,1,0,1,1,1)$	$(0,1,0,1,0,0,1,1)$
5	$(0,1,0,1,1,1,0,0)$	$(1,0,0,1,0,1,0,0)$	17	$(1,0,0,1,0,1,0,0)$	$(0,1,0,1,1,1,0,0)$
6	$(0,1,0,1,1,1,1,1)$	$(1,0,0,1,1,0,1,1)$	18	$(1,0,0,1,1,0,1,1)$	$(0,1,0,1,1,1,1,1)$
7	$(0,1,1,0,0,0,0,0)$	$(1,0,1,0,0,1,0,0)$	19	$(1,0,1,0,0,1,0,0)$	$(0,1,1,0,0,0,0,0)$
8	$(0,1,0,1,0,0,0,1)$	$(1,0,0,1,1,0,0,1)$	20	$(1,0,0,1,1,0,0,1)$	$(0,1,0,1,0,0,0,1)$
9	$(0,1,0,1,1,1,0,1)$	$(1,0,0,1,0,1,0,1)$	21	$(1,0,0,1,0,1,0,1)$	$(0,1,0,1,1,1,0,1)$
10	$(0,1,1,0,0,0,1,1)$	$(0,1,1,0,1,1,1,1)$	22	$(0,1,1,0,1,1,1,1)$	$(0,1,1,0,0,0,1,1)$
11	$(0,1,1,0,1,1,0,0)$	$(1,0,1,0,1,0,0,0)$	23	$(1,0,1,0,1,0,0,0)$	$(0,1,1,0,1,1,0,0)$
12	$(1,0,1,0,1,0,1,1)$	$(1,0,1,0,0,1,1,1)$	24	$(1,0,1,0,0,1,1,1)$	$(1,0,1,0,1,0,1,1)$

Proof of Theorem 3. Since $R_a(\tau) = R_a(2^m - \tau)$ for any τ, then by (4), it is sufficient to prove

$$\sum_{i \in I_3(\tau)} \xi^{a_i - a_j} = 0$$

is equal to zero for any $\tau \in \{k : 1 \le k \le 2^{m-3}\} \cup \{k : 3 \cdot 2^{m-3} \le k \le 2^{m-1}\}$, which have been given in Lemmas 6-9 for the condition (C)-(1), (C)-(2), (C)-(3) and (C)-(4). Hence, the conclusion holds under the condition (C).

Define a mapping $\pi'(k) = \pi(m + 1 - k)$, $k \in \{1, \cdots, m\}$. Replacing π by π', the conclusion under the condition (C') follows immediately from the conclusion under the condition (C).

□

4 Zero Autocorrelation Zone of 4^q-QAM Golay Complementary Sequences

In this section, we will consider the ZACZ of 4^q-QAM Golay complementary sequences defined by (2), which are based on the quaternary Golay sequences. So throughout this section, we always assume that $H = 4$ and ξ is the primitive 4-th root of unity. For convenience to describe, denote $s_{i,0} := 0$ for $0 \le i < 2^m$.

4.1 Results

Theorem 4 *If the 4^q-QAM Golay complementary sequence A, defined by (2) with ($s_{i,e} = d_{e,0} + d_{e,1}i_{\pi(m)}$ or $s_{i,e} = d_{e,0} + d_{e,1}i_{\pi(1)}$) for any $d_{e,0}, d_{e,1} \in \mathbb{Z}_4$, satisfies one of the condition listed in (A) or (A'), then the sequence A has the following property:*

$$R_A(\tau) = 0, \quad \tau \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m).$$

In other words, in one period $[0, 2^m)$, it has two zero autocorrelation zones of length 2^{m-2}, given by $(0, 2^{m-2}]$ and $[3 \cdot 2^{m-2}, 2^m)$.

Theorem 5 *If the 4^q-QAM Golay complementary sequence A, defined by (2) with ($s_{i,e} = d_{e,0} + d_{e,1}i_{\pi(m)}$ or $s_{i,e} = d_{e,0} + d_{e,1}i_{\pi(1)}$) for any $d_{e,0}, d_{e,1} \in \mathbb{Z}_4$, satisfies one of the condition listed in (B) or (B'), then the sequence A has the following property:*

$$R_A(\tau) = 0, \quad \tau \in [2^{m-2}, 3 \cdot 2^{m-2}].$$

In other words, in one period $[0, 2^m)$, it has a zero autocorrelation zone of length $2^{m-1} + 1$, given by $[2^{m-2}, 3 \cdot 2^{m-2}]$.

Theorem 6 *If the 4^q-QAM Golay complementary sequence A, defined by (2) with ($s_{i,e} = d_{e,0} + d_{e,1}i_{\pi(m)}$ or $s_{i,e} = d_{e,0} + d_{e,1}i_{\pi(1)}$) for any $d_{e,0}, d_{e,1} \in \mathbb{Z}_4$, satisfies one of the condition listed in (C) or (C'), then the sequence A has the following property:*

$$R_A(\tau) = 0, \quad \tau \in (0, 2^{m-3}] \cup [3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}] \cup [7 \cdot 2^{m-3}, 2^m).$$

In other words, in one period $[0, 2^m)$, it has three zero autocorrelation zones of respective length 2^{m-3}, $2^{m-2} + 1$, 2^{m-3}, given by $(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$ and $[7 \cdot 2^{m-3}, 2^m)$.

4.2 Proofs of the Results

In Section 3, the idea of the proof on the ZACZ of Golay sequence a is to define one-to-one mappings $i \to i'$ and $j \to j'$, $0 \le i \le 2^m - 1$ such that $\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}} = 0$. Hence we have

$$2 \sum_{i=0}^{2^m-1} \xi^{a_i - a_j} = \sum_{i=0}^{2^m-1} \xi^{a_i - a_j} + \sum_{i'=0}^{2^m-1} \xi^{a_{i'} - a_{j'}} = \sum_{i=0}^{2^m-1} \left(\xi^{a_i - a_j} + \xi^{a_{i'} - a_{j'}}\right) = 0.$$

That is $\sum_{i=0}^{2^m-1} \xi^{a_i - a_j} = 0$.

Note that $a_{i,0}$ is a quaternary Golay sequence. Under those definitions of (i', j') and conditions of π and (c_1, c_2) in Section 3, we have

$$a_{i,0} - a_{j,0} - (a_{i',0} - a_{j',0}) = 2 \tag{15}$$

and

$$i_{\pi(m)} = i'_{\pi(m)}, j_{\pi(m)} = j'_{\pi(m)}.$$

Let $s_{i,k} = d_{0,k} + d_{1,k} i_{\pi(m)}$, $1 \le k \le q-1$, then the latter equality indicates that

$$s_{i,e} - s_{j,f} = s_{i',e} - s_{j',f} \tag{16}$$

for any $0 \le e, f \le q-1$. Equalities (15) and (16) implies that

$$a_{i,e} - a_{j,f} - (a_{i',e} - a_{j',f}) = a_{i,0} - a_{j,0} - (a_{i',0} - a_{j',0}) + s_{i,e} - s_{j,f} - (s_{i',e} - s_{j',f}) = 2$$

or

$$\xi^{a_{i,e}-a_{j,f}} = \xi^{a_{i',e}-a_{j',f}}.$$

Similar to the discussion to the Golay sequence in Section 3, we have

$$2\sum_{i=0}^{2^m-1} \xi^{a_{i,e}-a_{j,f}} = \sum_{i=0}^{2^m-1} \xi^{a_{i,e}-a_{j,f}} + \sum_{i'=0}^{2^m-1} \xi^{a_{i',e}-a_{j',f}} = \sum_{i=0}^{2^m-1} \left(\xi^{a_{i,e}-a_{j,f}} + \xi^{a_{i',e}-a_{j',f}}\right) = 0$$

for any $0 \le e, f \le q-1$, i.e., $\sum_{i=0}^{2^m-1} \xi^{a_{i,e}-a_{j,f}} = 0$. Hence, for any given τ, $1 \le \tau \le 2^m - 1$,

$$\begin{aligned} R_A(\tau) &= \sum_{i=0}^{2^m-1} \left(\gamma \sum_{e=0}^{q-1} r_e \xi^{a_{i,e}}\right) \left(\gamma \sum_{f=0}^{q-1} r_f \xi^{a_{j,f}}\right)^* \\ &= \sum_{i=0}^{2^m-1} \sum_{e,f=0}^{q-1} r_e r_f \xi^{a_{i,e}-a_{j,f}} \\ &= \sum_{e,f=0}^{q-1} r_e r_f \sum_{i=0}^{2^m-1} \xi^{a_{i,e}-a_{j,f}} \\ &= 0. \end{aligned}$$

Naturally, the proofs of Theorems 4, 5 and 6 are similar to the proofs of Theorems 1, 2 and 3, respectively. So we omit them here.

We have presented the ZACZ for certain QAM Golay complementary sequences in Cases 1 and 2 in Fact 2. For the QAM Golay sequences in Case 3 under the conditions in Theorems 4 - 6 as above, some have a large ZACZ, while others do not. The following three examples under the condition in (A)-(1), (A)-(2) and (A)-(3) of Theorem 4 illustrate this fact. The first sequence has a ZACZ of length 8, while the other two do not have.

Example 1 *Let $q = 2$ and $m = 5$. Let $\pi = (1)$, $c_1 = 0$ and $s_i^{(1)} = 1 + i_{\pi(2)} + i_{\pi(3)}$. Then such 16-QAM Golay sequence A defined in Theorem 2 has $R_A(\tau) = 0$ for $\tau \in (0, 8] \cup [24, 32)$, or has two zero autocorrelation zones of length 8.*

Example 2 *Let $q = 2$ and $m = 5$. Let $\pi = (143)$, $c_1 = 0$, $c_2 = 0$ and $s_i^{(1)} = 1 + i_{\pi(2)} + i_{\pi(3)}$. Then such 16-QAM Golay sequence A defined in Theorem 2 has no a ZACZ of length 8.*

Example 3 *Let $q = 2$ and $m = 5$. Let $\pi = (12)$, $c_1 = 2$, $c_2 = 0$ and $s_i^{(1)} = 1 + i_{\pi(2)} + i_{\pi(3)}$. Then such 16-QAM Golay sequence A defined in Theorem 2 has no a ZACZ of length 8.*

Remark 3 *The sequences constructed in Theorems 4 - 6 belong to the first two constructions in (2). For the third construction, the above three examples show that it may have some classes of 4^q-QAM Golay complementary sequence with a large ZACZ. By computer search, we found that, if $q = 2$, $m = \{4, 5\}$, $\pi(1) = 1$, $\pi(2) = 2$ and $2c_1 = 0$, and $2d_0^{(1)} + d_1^{(1)} + d_2^{(1)} = 0$, then the 16-QAM Golay complementary sequence A defined by (2) has $R_A(\tau) = 0$ for $\tau \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m)$, two zero autocorrelation zones of length 2^{m-2}. However, the techniques that we used in Section 3 and in this section cannot apply to this case.*

We summarized all the results obtained in Sections 3 and 4 in Table 8.

Table 8: Parameters of Golay or QAM Golay complementary sequences with zero autocorrelation zone property

Permutation π	$(c_1, c_2) \in \mathbb{Z}_H \times \mathbb{Z}_H$	Zero Autocorrelation Zone
$\pi(1) = 1, \pi(2) = 2$	$2c_1 = 0$	$(0, 2^{m-2}]$, $[3 \cdot 2^{m-2}, 2^m)$
$\pi(m) = 1, \pi(m-1) = 2$	$2c_1 = 0$	$(0, 2^{m-2}]$, $[3 \cdot 2^{m-2}, 2^m)$
$\pi(2) = 2$, $\pi(3) = 1$, $\pi(4) = 3$	$2c_1 = 0, c_1 = 2c_2$	$(0, 2^{m-2}]$, $[3 \cdot 2^{m-2}, 2^m)$
$\pi(m-1) = 2$, $\pi(m-2) = 1$, $\pi(m-3) = 3$	$2c_1 = 0, c_1 = 2c_2$	$(0, 2^{m-2}]$, $[3 \cdot 2^{m-2}, 2^m)$
$\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$	$2c_1 = 0, c_1 = 2c_2 + t$	$(0, 2^{m-2}]$, $[3 \cdot 2^{m-2}, 2^m)$
$\pi(m) = 2$, $\pi(m-1) = 1$, $\pi(m-2) = 3$	$2c_1 = 0, c_1 = 2c_2 + t$	$(0, 2^{m-2}]$, $[3 \cdot 2^{m-2}, 2^m)$
$\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$	$2c_1 = 0, c_1 = 2c_2$	$[2^{m-2}, 3 \cdot 2^{m-2}]$
$\pi(m) = 2$, $\pi(m-1) = 1$, $\pi(m-2) = 3$	$2c_1 = 0, c_1 = 2c_2$	$[2^{m-2}, 3 \cdot 2^{m-2}]$
$\pi(1) = 1$, $\pi(2) = 3$, $\pi(3) = 2$	$2c_1 = 0$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$
$\pi(m) = 1$, $\pi(m-1) = 3$, $\pi(m-2) = 2$	$2c_1 = 0$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$
$\pi(1) = 1$, $\pi(2) = 3$, $\pi(m) = 2$	$2c_1 = 0$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$
$\pi(m) = 1$, $\pi(m-1) = 3$, $\pi(1) = 2$	$2c_1 = 0$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$
$\pi(1) = 2$, $\pi(2) = 4$, $\pi(3) = 1$, $\pi(4) = 3$	$2c_1 = 0, c_1 = 2c_2$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$
$\pi(m) = 2$, $\pi(m-1) = 4$, $\pi(m-2) = 1$, $\pi(m-3) = 3$	$2c_1 = 0, c_1 = 2c_2$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$
$\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$, $\pi(4) = 4$	$2c_1 = 0, c_1 = 2c_2$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$
$\pi(m) = 2$, $\pi(m-1) = 3$, $\pi(m-2) = 1$, $\pi(m-3) = 4$	$2c_1 = 0, c_1 = 2c_2$	$(0, 2^{m-3}]$, $[3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}]$, $[7 \cdot 2^{m-3}, 2^m)$

5 Examples

In the previous two sections, we have showed there exists a large ZACZ for certain Golay sequences and QAM Golay complementary sequences. With selected permutations π and affine transformations

$\sum_{k=1}^{m} c_{\pi(k)} + c_0$, these sequences have a large ZACZ, which can be divided into the following three cases.

(i) $R_a(\tau) = 0$ and $R_A(\tau) = 0$ for $\tau \in (0, 2^{m-2}] \cup [3 \cdot 2^{m-2}, 2^m)$.

(ii) $R_a(\tau) = 0$ and $R_A(\tau) = 0$ for $\tau \in [2^{m-2}, 3 \cdot 2^{m-2}]$.

(iii) $R_a(\tau) = 0$ and $R_A(\tau) = 0$ for $\tau \in (0, 2^{m-3}] \cup [3 \cdot 2^{m-3}, 5 \cdot 3^{m-3}] \cup [7 \cdot 2^{m-3}, 2^m)$.

In this section, we'll use empirical results to demonstrate these three categories of ZACZ. A total of 6 Golay sequences of length 32 labeled by $A_1, \cdots, A_6$ are given in Table 9.

Table 9: Examples of binary or quaternary Golay sequences of length 32 with their Autocorrelation

Condition	$\pi = (1)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 1, 1, 0, 0)$, $H = 2$
Sequence	$A_1 = (0,0,0,1,1,1,0,1,1,1,1,0,1,1,0,1,0,0,0,1,1,1,0,1,0,0,0,1,0,0,1,0)$
$\{R_{A_1}(\tau)\}_1^{31}$	$(0,0,0,0,0,0,0,-4,0,-4,0,-12,0,4,0,4,0,-12,0,-4,0,-4,0,0,0,0,0,0,0,0,0)$
Condition	$\pi = (1)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 1, 1, 0, 0)$, $H = 4$
Sequence	$A_2 = (0,0,0,2,1,1,3,1,1,1,1,3,0,0,2,0,0,0,0,2,1,1,3,1,3,3,3,1,2,2,0,2)$
$\{R_{A_2}(\tau)\}_1^{31}$	$(0,0,0,0,0,0,0,4j,0,4j,0,12j,0,-4j,0,4j,0,-12j,0,-4j,0,-4j,0,0,0,0,0,0,0,0,0)$
Condition	$\pi = (12)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 2$
Sequence	$A_3 = (0,1,0,0,0,1,1,1,0,1,0,0,0,1,1,1,0,1,0,0,1,0,0,0,1,0,1,1,0,1,1,1)$
$\{R_{A_3}(\tau)\}_1^{31}$	$(-4,0,-4,0,-12,0,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,4,0,-12,0,-4,0,-4)$
Condition	$\pi = (12)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 4$
Sequence	$A_4 = (0,1,0,3,0,1,2,1,0,1,0,3,0,1,2,1,0,1,0,3,2,3,0,3,2,3,2,1,0,1,2,1)$
$\{R_{A_4}(\tau)\}_1^{31}$	$(4j,0,12j,0,-4j,0,4j,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,-4j,0,4j,0,-12j,0,-4j)$
Condition	$\pi = (23)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 2$
Sequence	$A_5 = (0,1,0,0,0,1,0,0,0,1,1,1,1,0,0,0,0,1,0,0,1,0,1,1,0,1,1,1,0,1,1,1)$
$\{R_{A_5}(\tau)\}_1^{31}$	$(0,0,0,0,-4,0,-4,0,-12,0,4,0,0,0,0,0,0,0,0,0,0,4,0,-12,0,-4,0,-4,0,0,0,0)$
Condition	$\pi = (23)$, $(c_0, c_1, c_2, c_3, c_4, c_5) = (0, 0, 0, 0, 0, 1)$, $H = 4$
Sequence	$A_6 = (0,1,0,3,0,1,0,3,0,1,2,1,2,3,0,3,0,1,0,3,2,3,2,1,0,1,2,1,0,1,2,1)$
$\{R_{A_6}(\tau)\}_1^{31}$	$(0,0,0,0,4j,0,12j,0,-4j,0,4j,0,0,0,0,0,0,0,0,0,0,-4j,0,4j,0,-12j,0,-4j,0,0,0,0)$

The sequences A_1, A_3 and A_5 are binary Golay sequences. With the same permutation and coefficients of linear terms in (1), by only changing H from 2 to 4, we obtain three quaternary Golay sequences in A_2, A_4 and A_6. Note that for the figures of quaternary Golay sequences, autocorrelation is graphed in the form of magnitude, because they contain both real and imaginary parts. We can observe that all 6 sequences contain a large ZACZ. Moreover, each quaternary Golay sequence has exactly the same ZACZ trend as its corresponding binary case. Both A_1 and A_2 have two ZACZs of length 8 around

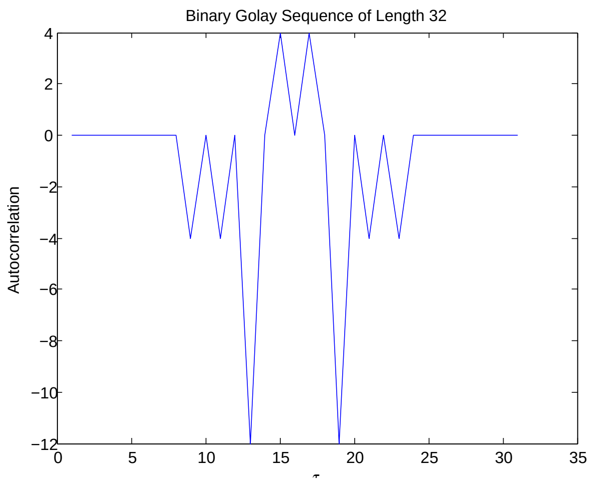

Figure 4: The Autocorrelation of A_1

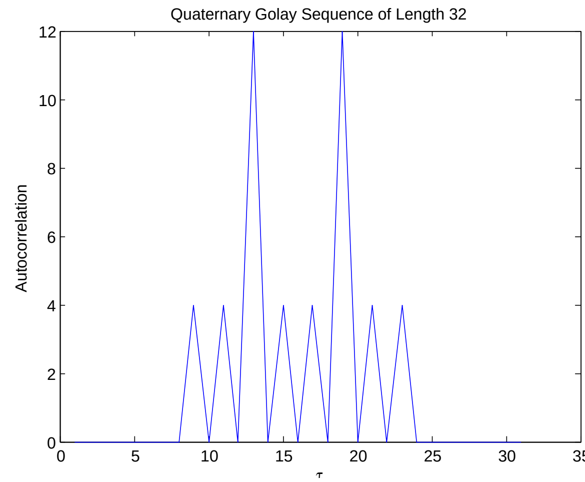

Figure 5: The Autocorrelation of A_2

the two sides of the origin. Both A_3 and A_4 have a ZACZ of length 17 in the middle, while A_5 and A_6 have three ZACZs: two ZACZs of length 4 on both around the two sides of origin and one ZACZ of length 9 in the middle.

6 Conclusions and Discussions

In this paper, we have shown several constructions of GDJ Golay sequences over $\mathbb{Z}_H$ and 4^q-QAM Golay complementary sequences which contain a large zero autocorrelation zone, where $H \geq 2$ is an arbitrary even integer and $q \geq 2$ is an arbitrary integer. Sequences with large ZACZ property can have wide implications in many areas. Potential applications include system synchronization, channel estimation and construction of signal set. This can be briefly illustrated as follows.

Synchronization: The synchronization of the signal is equivalent to computing its own autocorrelations [11, 20]. If the signal delay does not exceed of the ZACZ, then early synchronization or late synchronization will introduce no interference to the system. There will only be a peak value at the origin (i.e., correct synchronization). Thus the synchronization of system can be achieved.

Channel Estimation : Golay sequences with large ZACZ property can be used as pilot signals for channel estimation purposes in an LTI system. The relationship between input $x(t)$, channel impulse repones $h(t)$ and received signal $y(t)$ and white Gaussian noise $n(t)$ is given by [11]

$$y(t) = x(t) \otimes h(t) + n(t) \tag{17}$$

where $\otimes$ is the convolution operator. Once synchronization of signal is achieved as explained above using its large ZACZ property, then the received signal $y(t)$ can be accurately recovered. Note from

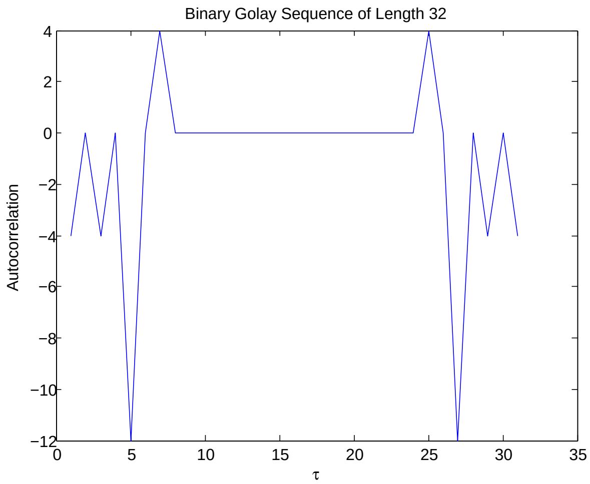

Figure 6: The Autocorrelation of A_3

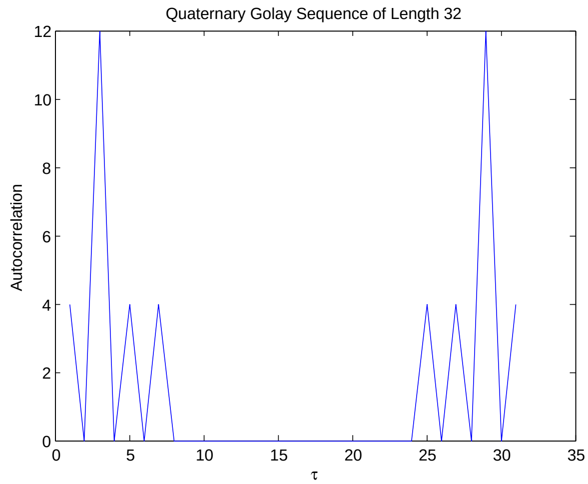

Figure 7: The Autocorrelation of A_4

(17), we have the approximated channel impulse response is:

$$Y(f) = X(f)H(f) + N(f) \implies \frac{Y(f)}{X(f)} = H(f) + \frac{N(f)}{X(f)}$$

where $X(f)$, $Y(f)$ and $N(f)$ are the Fourier transforms of $x(t)$, $y(t)$ and $n(t)$ respectively. Therefore, the approximated channel response $\hat{h}(t)$ is:

$$\hat{h}(t) \approx \mathcal{F}^{-1}\frac{Y(f)}{X(f)}$$

where $\mathcal{F}^{-1}$ is the inverse Fourier transform operator.

Another possible application of Golay sequences with large ZACZ is that it can be used to construct spreading sequence sets for CDMA systems. This will be a future research work.

Acknowledgment

The work is supported by NSERC Discovery Grant.

References

[1] 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.

[2] 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.

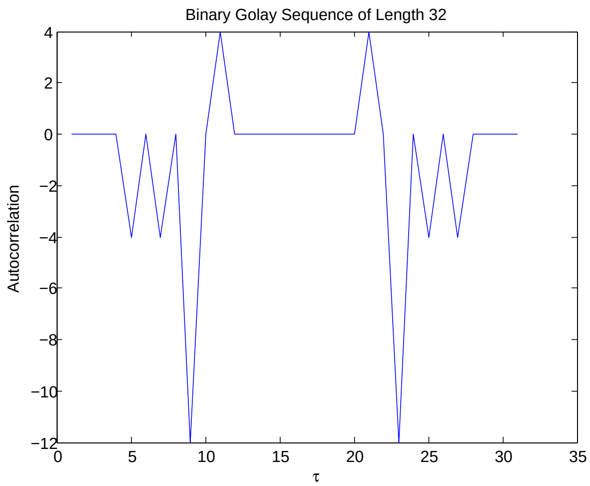

Figure 8: The Autocorrelation of A_5

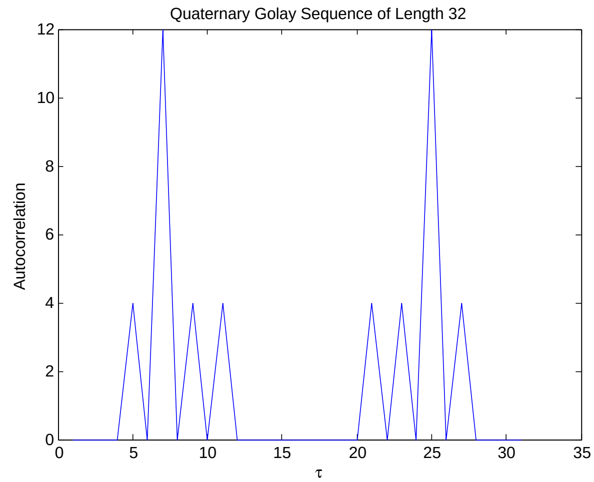

Figure 9: The Autocorrelation of A_6

[3] 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.

[4] X. M. Deng and P. Z. Fan, "Spreading sequence sets with zero correlation zone," *Electron. Lett.*, vol. 36, no. 11 pp. 993-994, May 2000.

[5] P. Z. Fan and L. Hao, "Generalized orthogonal sequences and their applications in synchronous CDMA system," *IEICE Trans. Fundam.*, vol. E83-A, no. 11, pp. 1-16, Nov. 2000.

[6] M. J. E. Golay, "Complementary series," *IRE Trans. Inform. Theory, vol. IT-7*, no. 2, pp. 82-87, Apr. 1961.

[7] 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.

[8] G. Gong, F. Huo, and Y. Yang, "Large zero autocorrelation zone of Golay sequences," *IEEE Globe Communications Conference 2011*, Houston, Texas, USA, Dec. 5-9th, 2011, submitted.

[9] T. Hayashi, "Binay sequences with orthogonal subsequences and a zero-correlation zone: Pair-preserving shuffled sequences," *IEICE Trans. Fundam.*, vol. E85-A, no. 6, pp. 1420-1425, 2002.

[10] T. Hayashi, "A generalization of binary zero-correlation zone sequence sets constructed from Hadamard matrices," *IEICE Trans. Fundam.*, vol. E87-A, no. 1, pp. 559-565, 2004.

[11] S. Haykin and M. Moher. *Communication Systems.* John Wiley & Sons, U.S, 2009.

[12] H.G. Hu and G. Gong, "New sets of zero or low correlation zone sequences via interleaving techniques," *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1702-1713, April 2010.

[13] 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.

[14] 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.

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

[16] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Tech.*, vol. 47, pp. 1268-1275, 1998.

[17] A. Rathinakumar and A. K. Chaturvedi, "A new framework for constructing mutually orthogonal complementary sets and ZCZ sequences," *IEEE. Trans. Inform. Theory*, vol. 52, no. 8, pp. 3817-3826, Aug. 2006.

[18] A. Rathinakumar and A. K. Chaturvedi, "Complete mutually orthogonal Golay complementary sets from Reed-Muller codes," *IEEE. Trans. Inform. Theory*, vol. 54, no. 3, pp. 1339-1346, Mar. 2008.

[19] 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.

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

[21] J. R. Seberry, B. J. Wysocki, and T. A. Wysocki, "On a use of Golay sequences for asynchronous DS CDMA applications," *Advanced Signal Processing for Communication Systems The International Series in Engineering and Computer Science*, Vol. 703, pp. 183-196, 2002.

[22] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on the maximum correlation of sequence set with low or zero correlation zone," *Electron. Lett.*, vol. 36, pp. 551-552, Mar. 2000.

[23] X. H. Tang and W. H. Mow, "Design of spreading codes for quasisynchronous CDMA with intercell interference," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 1, pp. 84-93, Jan. 2006.

[24] R. D. J. van Nee, "OFDM codes for peak-to-average power reduction anderror correction," *in Proc. IEEE GLOBECOM*, London, U.K, pp. 740-744, Nov. 1996.

[25] T. A. Wilkinson and A. E. Jones, "Minimization of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding," *in Proc. IEEE 45th Vehicular Technology Conf.*, Chicago, IL, pp. 825-829, Jul. 1995.

[26] T. A. Wilkinson and A. E. Jones, "Combined coding for error control and increasedrob ustness to system nonlinearities in OFDM," *in Proc. IEEE 46th Vehicular Technology Conf.*, Atlanta, GA, pp. 904-908, 1996.

[27] D.Wulich, "Reduction of peak to mean ratio of multicarrier modulation using cyclic coding," *Electron. Lett.*, vol. 32, pp. 432-433, 1996.

[28] Z.C. Zhou, X.H. Tang, and G. Gong, "A new class of sequences with zero or low correlation zone based on interleaving technique," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4267-4273, April 2008.