A Construction of 4^q-QAM Golay Complementary Pairs Based on Non-standard Golay Complementary Sequences

Erzhong Xue Zilong Wang

State Key Laboratory of Integrated Service Networks,
School of Cyber Engineering, Xidian University
Xi'an, China

2524384374@qq.com, zlwang@xidian.edu.cn

Abstract

Golay complementary sequence pairs (GCPs) over QAM based on weighted-sum of standard Golay complementary sequences (GCSs) over QPSK and first order offsets and pairing difference were well studied. We proposed a construction of non-standard 4^q-QAM GCPs, which are based on weighted-sum of q non-standard QPSK GCSs, in the form of first order offset vectorial generalized Boolean function (V-GBF) and pairing different set V-GBFs.

Keywords: Golay complementary sequence, QPSK, QAM, generalized Boolean function.

1 Introduction

A pair of sequences is called a Golay complementary pair (GCP) if their aperiodic autocorrelation sums for any nonzero shifts are all equal to zero [8]. Each sequence in the GCP is called a Golay complementary sequence (GCS). GCSs have found numerous applications, especially in peak-to-mean envelope power ratio (PMEPR) control in orthogonal frequency-division multiplexing (OFDM) systems. An important study on the GCPs was made by Davis and Jedwab in [4] by a direct construction of polyphase GCSs based on generalized Boolean functions (GBFs), which have been referred to as the standard GCSs since then. The non-standard GCSs were found by computer search [13], and were explained by shared autocorrelation function [5] of quaternary GCPs of length 8 later on. A significant result was given by Fiedler, Jedwab and Parker [7] taking on a multi-dimensional (or array) construction approach.

Since quadrature amplitude modulation (QAM) are widely employed in high rate OFDM transmissions, 4^q-QAM GCSs of length 2^m were studied [9, 3, 10, 11, 2]. Those sequences are represented as the weighted-sum of q standard QPSK GCSs and compatible first order offsets in five cases by Li (the generalized cases I-III for $q \geq 2$) in 2010 [12] and Liu (the generalized cases IV-V for $q \geq 3$) in 2013 [14] respectively. In 2018, Budišin *et al.* [1] introduced a new algorithm to generate QAM GCPs by para-unitary matrices. However, for given q and sequences length 2^m, the acceptable unitary matrices over QAM can be obtained only by exhaustive search, and the lack of explicit algebraic expression of GCSs leads to unexpected duplication. Inspired by [1], Wang *et al.* [16] gave a generalized construction of 4^q-QAM GCPs derived from Golay complementary array pairs, in compatible with the generalized cases I-V, and also generating more GCPs for composite q.

The aforementioned QAM GCSs with explicit algebraic expression are all generated from standard QPSK GCSs. In 2008, Li [11] found out that non-standard QPSK GCSs with third-order algebraic normal form can be combined to generate QAM Golay sequences and also gave an example of 64-QAM Golay complementary pair. It was pointed out that " new QPSK Golay sequences lead to new QAM Golay sequences ". However, our research suggested that the offset and pairing difference set can not be adopted straightforwardly from the known QAM GCPs based on standard QPSK GCSs.

In this paper, we proposed a construction of 4^q-QAM GCPs, which are based on weighted-sum of q non-standard QPSK GCSs, in the form of first order offset V-GBFs and pairing different set V-GBFs. We found that the offsets are similar to that in QAM GCPs [2], but different in limitation of variables. The pairing difference set is the combination of that in both non-standard GCPs [7] and QAM GCPs.

The rest of this paper is organized as follows. In the next section, the definitions of GCP and GCS are introduced. We give both standard and non-standard GCPs, the constructions of the QAM GCPs in the generalised cases I-III. In Section 3, we present our main construction of non-standard 4^q-QAM GCPs and a lower bound of enumeration. An elementary proof from viewpoint of array is presented in Section 4. We conclude the paper in Section 5.

2 Preliminary

For an nonnegative integer L, a sequence of length L is a function $F(y) : \mathbb{Z}_L \to \mathbb{C}$. The *aperiodic auto-correlation* of $F(y)$ at shift τ $(1-L \leq \tau \leq L-1)$ is defined by

$$C_F(\tau) = \sum_y F(y+\tau) \cdot \overline{F(y)}, \tag{1}$$

where $\overline{F(y)}$ means the conjugate of $F(y)$, and $F(y+\tau) \cdot \overline{F(y)} = 0$ if $F(y+\tau)$ or $F(y)$ is not defined.

Definition 1. A pair of sequences $\{F(y), G(y)\}$ of length L is said to be *Golay complementary pair* (GCP) if $C_F(\tau) + C_G(\tau) = 0$ $(\forall \tau \neq 0)$. And either sequence in a GCP is called a *Golay complementary sequence* (GCS) [8].

2.1 QPSK GCP

A QPSK sequence of length 2^m can be uniquely associated to a *generalized Boolean function (GBF)* $f(x_1, x_2, \cdots, x_m) : \mathbb{Z}_2^m \to \mathbb{Z}_4$, which satisfies $F(y) = \xi^{f(x_1,x_2,\cdots,x_m)}$, where

$y=\sum_{i=1}^{m} x_i 2^{i-1}$, $\xi=\sqrt{-1}$ is a fourth primitive root of unity.

The GCPs $\{F(y), G(y)\}$ of length 2^m over QPSK were well studied by their associated GBFs $\{f(\boldsymbol{x}), g(\boldsymbol{x})\}$ in the literature, which are usually given by a GBF $f(\boldsymbol{x})$ and a pairing difference $\mu(\boldsymbol{x})$, i.e., $g(\boldsymbol{x})=f(\boldsymbol{x})+\mu(\boldsymbol{x})$. For a given $f(\boldsymbol{x})$, there exists two independent pairing difference $\mu(\boldsymbol{x})$, i.e., $\mu_A(\boldsymbol{x})$ and $\mu_B(\boldsymbol{x})$, simultaneously. We will use $\mu_A(\boldsymbol{x})$ and $\mu_B(\boldsymbol{x})$ instead of $\mu(\boldsymbol{x})$ in the following paper.

There are several constructions of GCPs over QPSK based on GBFs, such as [4, 13, 5, 6, 7]. The most typical GCPs are so called standard GCPs given in [4], which are associated with GBFs over $\mathbb{Z}_4$ given below.

Fact 2. *[4] Let π be a permutation of integers $\{1,2,\ldots,m\}$ and $c_k \in \mathbb{Z}_4 (0 \le k \le m)$. The sequence pair $\{f(\boldsymbol{x}), g(\boldsymbol{x})\}$ given by GBF*

$$f(\boldsymbol{x})=2\cdot\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)}+\sum_{k=1}^{m} c_k\cdot x_k+c_0, \tag{2}$$

and the pairing difference $\mu_A(\boldsymbol{x})=2x_{\pi(1)}$ or $\mu_B(\boldsymbol{x})=2x_{\pi(m)}$ form a GCP.

The GCPs in Fact 2 are called standard GCPs and the sequences with form (2) are called standard GCSs.

GCSs not of form (2) were found by computer search [13], and were referred to non-standard GCSs. It was explained by shared autocorrelation function of quaternary GCSs of length 8 [5] later on. The set of seed quaternary GCSs can be summarized as (a,b) ([6, Theorem 10]) and their negative reversal (a^*, b^*), i.e.,

$$\begin{cases} a(x_1,x_2,x_3)=2x_1x_2+2x_2x_3+2u_0x_3+(2u_0+2u_2)x_1, \\ b(x_1,x_2,x_3)=2x_2x_3+2x_1x_3+(2u_1+2u_2+1)x_2+(2u_1+1)x_1, \\ a^*(x_1,x_2,x_3)=a(x_1,x_2,x_3)+2x_1+2x_3+2u_2, \\ b^*(x_1,x_2,x_3)=b(x_1,x_2,x_3)+2x_1+2x_2+2u_2+2, \end{cases} \tag{3}$$

where $(u_0,u_1,u_2)\in\mathbb{Z}_2^3$.

In the following paper, we define a frequently used GBF over $\mathbb{Z}_4$ by

$$\begin{aligned} h\left(x_0,x_1,x_2,x_3,x_4\right)=&(1-x_0)\cdot a(x_1,x_2,x_3)\cdot(1-x_4)+(1-x_0)\cdot b^*(x_1,x_2,x_3)\cdot x_4 \\ &+x_0\cdot b(x_1,x_2,x_3)\cdot(1-x_4)+x_0\cdot(a^*(x_1,x_2,x_3)+2)\cdot x_4. \end{aligned} \tag{4}$$

What's more, we define "fake" variables which always equal to 0. For example, $x_ix_j=0$ and $cx_i=0$ if x_i is a "fake" variable. In the following Facts 3, 4 and Theorem 5, $x_{\pi(0)}$ and $x_{\pi(m+1)}$ are both "fake" variables.

A significant result on QPSK GCPs was given by multi-dimensional (or array) approach [7], which are associated with GBFs over $\mathbb{Z}_4$ given below.

Fact 3. *[7] Let $m\ge 1$, $n\ge 0$ be integers and $m\ge 4n-1$. Let t_k $(1\le k\le n)$ be integers satisfying $t_1\ge 0, t_k+4\le t_{k+1}$ $(k=1,2,\ldots,n-1), t_n+3\le m$. Define $\{0,1,\ldots,m\}\backslash\cup_{k=1}^{n}$ $\{t_k, t_k{+}1, t_k{+}2, t_k{+}3\}=\mathcal{K}$. Let π be a permutation of integers $\{1,2,\ldots,m\}$ satisfying*

$(\pi(t_k+2), \pi(t_k+3)) = (\pi(t_k+1)+1, \pi(t_k+1)+2)$. *Let* $c_k \in \mathbb{Z}_4 (0 \leq k \leq m)$, *where* $c_{\pi(t_k+2)} = 2c_{\pi(t_k+1)}$, $c_{\pi(t_k+1)} = 0$. *For* $1 \leq k \leq n$, *let* $h_k(x_0, x_1, x_2, x_3, x_4)$ *be of form (4), where the parameters* $(u_0, u_1, u_2) \in \mathbb{Z}_2^3$ *in (3) are chosen independently for different* k. *The sequence pair* $\{f(\boldsymbol{x}), g(\boldsymbol{x})\}$ *given by GBF*

$$f(\boldsymbol{x}) = \sum_{i \in \mathcal{K}} 2x_{\pi(i)}x_{\pi(i+1)} + \sum_{k=1}^{n} h_k\left(x_{\pi(t_k)}, x_{\pi(t_k+1)}, x_{\pi(t_k+2)}, x_{\pi(t_k+3)}, x_{\pi(t_k+4)}\right) + \sum_{k=1}^{m} c_k x_k + c_0, \tag{5}$$

and the pairing difference $\mu_A(\boldsymbol{x})$ *or* $\mu_B(\boldsymbol{x})$ *form a QPSK GCP of length* 2^{m+3n}, *where*

- $\mu_A(\boldsymbol{x}) = \begin{cases} h_1\left(1, x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}\right) - h_1\left(0, x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}\right), & (t_1 = 0), \\ 2x_{\pi(1)}, & (t_1 \neq 0); \end{cases}$

- $\mu_B(\boldsymbol{x}) = \begin{cases} h_n\left(x_{\pi(m-3)}, x_{\pi(m-2)}, x_{\pi(m-1)}, x_{\pi(m)}, 1\right) \\ \qquad - h_n\left(x_{\pi(m-3)}, x_{\pi(m-2)}, x_{\pi(m-1)}, x_{\pi(m)}, 0\right), & (t_n + 3 = m), \\ 2x_{\pi(m)}, & (t_n + 3 \neq m). \end{cases}$

In Fact 3, if $n \geq 1$, the GCPs are called non-standard GCPs and the sequences with form (5) are called non-standard GCSs. If $n = 0$, the GCPs with form (5) degenerate to standard GCPs.

2.2 4^q-QAM GCP

For any $q \geq 2$, a 4^q-QAM sequence of length 2^m can be uniquely associated to a *vectorial Generalized Boolean function (V-GBF)* $\vec{f}(x_1, x_2, \cdots, x_m) = \{f^{(p)}(x_1, x_2, \cdots, x_m) | 0 \leq p < q\} : \mathbb{Z}_2^m \to \mathbb{Z}_4$, which satisfies $F(y) = \sum_{p=0}^{q-1} 2^{q-1-p} \cdot \xi^{f^{(p)}(x_1, x_2, \cdots, x_m)}$, where $y = \sum_{i=1}^{m} x_i 2^{i-1}$.

The 4^q-QAM GCPs $\{F(y), G(y)\}$ of length 2^m were well studied by their associated V-GBFs $\{\vec{f}(\boldsymbol{x}), \vec{g}(\boldsymbol{x})\}$ in the literature. Such V-GBFs $\{\vec{f}(\boldsymbol{x}), \vec{g}(\boldsymbol{x})\}$ are usually given by

- GBF $f(\boldsymbol{x})$,
- *offset* V-GBF $\vec{s}(\boldsymbol{x}) = \left(s^{(0)}(\boldsymbol{x}) = 0, s^{(1)}(\boldsymbol{x}), \cdots, s^{(q-1)}(\boldsymbol{x})\right)$,
- either one of the two independent *pairing difference* V-GBF

$$\vec{\mu}_A(\boldsymbol{x}) = \left(\mu_A^{(0)}(\boldsymbol{x}), \mu_A^{(1)}(\boldsymbol{x}), \cdots, \mu_A^{(q-1)}(\boldsymbol{x})\right),$$

$$\vec{\mu}_B(\boldsymbol{x}) = \left(\mu_B^{(0)}(\boldsymbol{x}), \mu_B^{(1)}(\boldsymbol{x}), \cdots, \mu_B^{(q-1)}(\boldsymbol{x})\right),$$

or more clearly,

$$\begin{cases} \vec{f}(\boldsymbol{x}) = f(\boldsymbol{x}) \cdot \vec{1} + \vec{s}(\boldsymbol{x}), \\ \vec{g}(\boldsymbol{x}) = \vec{f}(\boldsymbol{x}) + \vec{\mu}_A(\boldsymbol{x}) \text{ (or } \vec{\mu}_B(\boldsymbol{x})), \end{cases} \tag{6}$$

where $\vec{1}$ denotes the q-dimensional vector $(1, 1, \cdots, 1)$. The offset V-GBFs $\vec{s}(\boldsymbol{x})$ and pairing difference V-GBFs $\vec{\mu}(\boldsymbol{x})$ in the generalized cases I-III given by Li *et al.* [12] can be represented in a general form by introducing the "fake" variables $x_{\pi(0)}$ and $x_{\pi(m+1)}$.

Fact 4. *[12] For $0 \le p \le q-1$ and $q \ge 2$, let $d_i^{(p)} \in \mathbb{Z}_4$ ($0 \le i \le 2$) satisfying $2d_0^{(p)} + d_1^{(p)} + d_2^{(p)} = 0$. Let π be a permutation of integers $\{1, 2, \ldots, m\}$. $\{\vec{f}(\boldsymbol{x}), \vec{g}(\boldsymbol{x})\}$ given by standard GCS in the form of (2), offset V-GBF $\vec{s}(\boldsymbol{x})$ and pairing difference V-GBF $\vec{\mu}_A(\boldsymbol{x})$ or $\vec{\mu}_B(\boldsymbol{x})$ form a 4^q-QAM GCP of length 2^m, where*

- $s^{(p)}(\boldsymbol{x}) = d_0^{(p)} + d_1^{(p)} x_{\pi(\omega)} + d_2^{(p)} x_{\pi(\omega+1)}, \quad (\omega \in \{0, 1, \ldots, m\})$.
- $\mu_A^{(p)}(\boldsymbol{x}) = \begin{cases} 2x_{\pi(1)} + d_1^{(p)}, & (\omega = 0), \\ 2x_{\pi(1)}, & (\omega \neq 0), \end{cases}$
- $\mu_B^{(p)}(\boldsymbol{x}) = \begin{cases} 2x_{\pi(m)} + d_2^{(p)}, & (\omega = m), \\ 2x_{\pi(m)}, & (\omega \neq m), \end{cases}$

for $0 \le p \le q-1$.

Fact 4 is more comprehensive than [12] in terms of pairing difference set. For more details, see [16].

3 Main Results

The QAM GCSs in Fact 4 are all generated from standard QPSK GCSs in Fact 2. In 2008, Li [11] declared that QAM GCSs can also be generated from non-standard QPSK GCSs and gave an example of 64-QAM Golay complementary pair. It was pointed out that " new QPSK Golay sequences lead to new QAM Golay sequences ". We will study the 4^q-QAM GCPs based on non-standard GCSs given in Fact 3 in this section, and show that offset V-GBFs $\vec{s}(\boldsymbol{x})$ and pairing difference V-GBFs $\vec{\mu}(\boldsymbol{x})$ are different from the case of the standard GCSs.

3.1 4^q-QAM GCPs Based on Non-standard GCSs

The offset V-GBFs and pairing difference V-GBFs are given for non-standard GCSs over QPSK to form GCPs over QAM in the following theorem.

Theorem 5. *Let $m \ge 1$, $n \ge 0$ and $q \ge 2$ be integers and $m \ge 4n$, t_k $(1 \le k \le n)$, π and $\mathcal{K}$ be defined the same as those in Fact 3, and $\omega \in \mathcal{K}$. Let $d_i^{(p)} \in \mathbb{Z}_4$ ($0 \le i \le 2$), and $2d_0^{(p)} + d_1^{(p)} + d_2^{(p)} = 0$. $\{\vec{f}(\boldsymbol{x}), \vec{g}(\boldsymbol{x})\}$ given by non-standard GCS $f(\boldsymbol{x})$ in (5), offset V-GBF $\vec{s}(\boldsymbol{x})$ and pairing difference V-GBF $\vec{\mu}_A(\boldsymbol{x})$ or $\vec{\mu}_B(\boldsymbol{x})$ form a 4^q-QAM GCP of length 2^m, where*

- $s^{(p)}(\boldsymbol{x}) = d_0^{(p)} + d_1^{(p)} x_{\pi(\omega)} + d_2^{(p)} x_{\pi(\omega+1)}$, $(\omega \in \mathcal{K})$.
- $\mu_A^{(p)}(\boldsymbol{x}) = \begin{cases} h_1\left(1, x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}\right) & \\ \qquad - h_1\left(0, x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}\right), & (0 = t_1); \\ 2x_{\pi(1)} + d_1^{(p)}, & (0 = \omega); \\ 2x_{\pi(1)}, & (0 \neq t_1 \text{ or } \omega). \end{cases}$

- $$\mu_B^{(p)}(\boldsymbol{x}) = \begin{cases} h_n\left(x_{\pi(m-3)}, x_{\pi(m-2)}, x_{\pi(m-1)}, x_{\pi(m)}, 1\right) \\ \qquad - h_n\left(x_{\pi(m-3)}, x_{\pi(m-2)}, x_{\pi(m-1)}, x_{\pi(m)}, 0\right), & (m = t_n+3); \\ 2x_{\pi(m)} + d_2^{(p)}, & (m = \omega); \\ 2x_{\pi(m)}, & (m \neq t_n+3 \ or \ \omega), \end{cases}$$

for $0 \le p \le q-1$.

The form of offset V-GBFs $\vec{s}(\boldsymbol{x})$ and pairing difference V-GBFs $\vec{\mu}(\boldsymbol{x})$ for non-standard GCSs cannot be straightforwardly obtained from the known offset V-GBFs and pairing difference for standard GCSs. In Theorem 5, the $s^{(p)}(\boldsymbol{x})$ in offset V-GBF $\vec{s}(\boldsymbol{x})$ share the similar form with that in Fact 4. However, the variable ω is restricted in the set $\mathcal{K}$ here, and permutation π is restricted by $(\pi(t_k+2), \pi(t_k+3)) = (\pi(t_k+1)+1, \pi(t_k+1)+2)$.

Remark 6. If $n = 0$, the 4^q-QAM GCPs in Theorem 5 degenerate into 4^q-QAM GCPs in Fact 4.

3.2 Example

Here is an example of 4^q-QAM GCP of length $2^5 = 32$ in the context of Theorem 5. Let $m = 5$, $n = 1$, $t = 0$ and π be an identity permutation. (The subscript k in t_k, h_k, a_k, b_k, a_k^*, b_k^* is ignored, since $k = 1$.) Then $\{t, t+1, t+2, t+3\} = \{0, 1, 2, 3\}$ and $\mathcal{K} = \{4, 5\}$. Let

$$\begin{cases} a(x_1, x_2, x_3) = 2x_1x_2 + 2x_2x_3, \\ b(x_1, x_2, x_3) = 2x_2x_3 + 2x_1x_3 + x_1 + x_2, \\ a^*(x_1, x_2, x_3) = 2x_1x_2 + 2x_2x_3 + 2x_1 + 2x_3, \\ b^*(x_1, x_2, x_3) = 2x_2x_3 + 2x_1x_3 + 3x_1 + 3x_2 + 2. \end{cases} \tag{7}$$

The 4^q-QAM GCPs can be generated by the following steps.

Step 1: Generate non-standard QPSK GCS by (5).

$$\begin{aligned} f(\boldsymbol{x}) = {} & 2x_1x_2 + 2x_2x_3 + 3x_2x_4 + 3x_1x_4 + 2x_4x_5 + 2x_1x_2x_4 + 2x_1x_3x_4 \\ & + c_1x_1 + 2c_1x_2 + (2 + c_4)x_4 + c_5x_5 + c_0, \end{aligned} \tag{8}$$

where $c_0, c_1, c_4, c_5 \in \mathbb{Z}_4$.

Step 2: Chose the parameter ω. ω can only be chosen from $\mathcal{K} = \{4, 5\}$.

Step 3: Calculate the offset V-GBF $\vec{s}(\boldsymbol{x})$ and pairing difference V-GBF $\vec{\mu}_A(\boldsymbol{x})$ and $\vec{\mu}_B(\boldsymbol{x})$.

Case 1: $(\omega = 4.)$ For $0 \le p \le q-1$,

$$\begin{cases} s^{(p)}(\boldsymbol{x}) = d_0^{(p)} + d_1^{(p)}x_4 + d_2^{(p)}x_5; \\ \mu_A^{(p)}(\boldsymbol{x}) = 2x_1x_4 + 2x_3x_4 + 2x_1x_3 + 2x_1x_2 + x_1 + x_2; \\ \mu_B^{(p)}(\boldsymbol{x}) = 2x_5. \end{cases} \tag{9}$$

Case 2: ($\omega = 5$.) For $0 \le p \le q-1$,

$$\begin{cases} s^{(p)}(\boldsymbol{x}) = d_0^{(p)} + d_1^{(p)} x_4 + d_2^{(p)} x_5; \\ \mu_A^{(p)}(\boldsymbol{x}) = 2x_1x_4 + 2x_3x_4 + 2x_1x_3 + 2x_1x_2 + x_1 + x_2; \\ \mu_B^{(p)}(\boldsymbol{x}) = 2x_5 + d_2^{(p)}. \end{cases} \tag{10}$$

where $d_i^{(p)} \in \mathbb{Z}_4$ ($0 \le i \le 2$), and $2d_0^{(p)} + d_1^{(p)} + d_2^{(p)} = 0$.

Step 4: The GCS $f(\boldsymbol{x})$ in (8) forms 4^q-QAM GCPs with $\vec{s}(\boldsymbol{x})$ and $\vec{\mu}_A(\boldsymbol{x})$ (or $\vec{\mu}_B(\boldsymbol{x})$) in either (9) or (10).

3.3 A Lower Bound of Enumeration

In Theorem 5, the choice of $\mathcal{K}$ will impact the possible value of non-standard QPSK GCS $f(\boldsymbol{x})$ and offset V-GBF $\vec{s}(\boldsymbol{x})$. We will specifically select a subset of $\{\vec{s}(\boldsymbol{x})\}$ denoted by $\{\vec{s}(\boldsymbol{x})\}_{\text{Sub}}$ compatible with all the possible $f(\boldsymbol{x})$. So the number of the GCSs over 4^q-QAM of length 2^m constructed in Theorems 5 denoted by $\#\{\vec{f}(\boldsymbol{x})\}$ is greater than the product of the number of the non-standard QPSK GCSs $f(\boldsymbol{x})$ and the number of the subset of compatible offsets $\vec{s}(\boldsymbol{x})$, i.e.,

$$\#\{\vec{f}(\boldsymbol{x})\} \ge \#\{f(\boldsymbol{x})\} \times \#\{\vec{s}(\boldsymbol{x})\}_{\text{Sub}}.$$

According to Fact 3, the number of the non-standard GCSs over QPSK is determined by the choice of $\{t_k | 1 \le k \le n\}$, the permutaition π, the parameters $(u_0, u_1, u_2) \in \mathbb{Z}_2^3$ for different $1 \le k \le n$, and parameters $\{c_k \in \mathbb{Z}_4 | 0 \le k \le m\}$, which range over all their $\binom{m-3n+1}{n}$, $(m-2n)!/2$, 2^{3n} and 4^{m-2n+1} allowed values respectively. (More details will be given in the extended paper.) The number of the non-standard GCSs over QPSK is given by

$$\#\{f(\boldsymbol{x})\} = 2^{2m-n+1} \binom{m-3n+1}{n} (m-2n)!, \tag{11}$$

which meets the results in [7]. Let $\{\vec{s}(\boldsymbol{x})\}_{\text{Sub}} = \{\vec{s}(\boldsymbol{x}) | 1 \le \omega \le m-1\}$. For any $f(\boldsymbol{x})$ in (5), ω has at least $m-4n-1$ choices, $\left(d_0^{(p)}, d_1^{(p)}, d_2^{(p)}\right)$ have 4^2 allowed values for each $1 \le p \le q-1$. So

$$\#\{\vec{s}(\boldsymbol{x})\}_{\text{Sub}} \ge (m-4n-1)4^{2(q-1)}, \ m > 4n+1. \tag{12}$$

Thus for $m > 4n+1$, a lower bound of the number of the GCSs over 4^q-QAM of length 2^m obtained by Theorems 5 is given:

$$\#\{\vec{f}(\boldsymbol{x})\} \ge (m-4n-1) \binom{m-3n+1}{n} 2^{2m-n+4q-3} (m-2n)! \tag{13}$$

4 A Sketch of Proof

In this section, we introduce the concept of arrays and Golay array pairs (GAPs) and show there exist mappings from Golay array pairs (GAPs) to GCPs. We give an important construction of 4^q-QAM array matrix where the pairs in each column or row form GAPs. The GCPs in Theorem 5 are directly mapped from the Golay array pairs (GAPs) in the first row and column of the array matrix. Due to the constraints of the paper length, the validity of the array matrix will be proved in extended paper.

4.1 Array and Golay Array Pair

An array of size $r_1 \times r_2 \cdots \times r_n$ is an n-variable function $F(y_1, y_2, \cdots, y_n)$ (or $F(\boldsymbol{y})$ for short) whose entries belong to $\mathbb{C}$ where $y_k \in \mathbb{Z}_{r_k}(1 \le k \le n)$. A 4^q-QAM array $F(y_1, y_2, \cdots, y_n)$ can be uniquely associated to a vectorial function $\vec{f}(y_1, y_2, \cdots, y_n) = \{f^{(p)}(y_1, y_2, \cdots, y_n)|0 \le p < q\} : \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \cdots \times \mathbb{Z}_{r_n} \to \mathbb{Z}_4$ (which is denoted as $\vec{f}(\boldsymbol{y})$ for short), satisfying $F(\boldsymbol{y}) = \sum_{p=0}^{q-1} 2^{q-1-p} \cdot \xi^{f^{(p)}(\boldsymbol{y})}$.

The *aperiodic auto-correlation* of array $F(\boldsymbol{y})$ at shift $\boldsymbol{\tau} = (\tau_1, \tau_2, \cdots \tau_n)$ $(1 - r_k \le \tau_k \le r_k - 1)$ is defined by

$$C_{\vec{f}}(\boldsymbol{\tau}) = \sum_{\boldsymbol{y}} F(\boldsymbol{y} + \boldsymbol{\tau}) \cdot \overline{F(\boldsymbol{y})},$$

where $F(\boldsymbol{y} + \boldsymbol{\tau}) \cdot \overline{F(\boldsymbol{y})} = 0$ if either $F(\boldsymbol{y} + \boldsymbol{\tau})$ or $F(\boldsymbol{y})$ is not defined.

Definition 7. A pair of arrays $\{F(\boldsymbol{y}), G(\boldsymbol{y})\}$ of size $r_1 \times r_2 \cdots \times r_n$ is said to be *Golay array pair* (GAP) if $C_{\vec{f}}(\boldsymbol{\tau}) + C_{\vec{g}}(\boldsymbol{\tau}) = 0$ $(\forall \boldsymbol{\tau} \neq \mathbf{0})$. And either array in a GAP is called a *Golay complementary array.*

For more details on the concepts and results for GAPs, see [7, 15].

Property 8. *Let $f'(\boldsymbol{y}) = \sum_{k=1}^{n} c_k y_k + c_0$ ($c_k \in \mathbb{Z}_4, 0 \le k \le n$) be an affine function from $\mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \cdots \times \mathbb{Z}_{r_n}$ to $\mathbb{Z}_4$. If a pair of q-ary arrays given by $\{\vec{f}(\boldsymbol{y}), \vec{g}(\boldsymbol{y})\}$ form a GAP, the pair of arrays given by $\left\{\vec{f}(\boldsymbol{y}) + \vec{1} \cdot f'(\boldsymbol{y}), \vec{g}(\boldsymbol{y}) + \vec{1} \cdot f'(\boldsymbol{y})\right\}$ is also a GAP.*

4.2 Relationship of GCP and GAP

For any permutation χ of $\{1, 2, \cdots, n\}$, there exists a projection from array $F(y_1, y_2, \cdots, y_n)$ of size $r_1 \times r_2 \cdots \times r_n$ to sequence $F(y)$ of length $L = \prod_{k=1}^{n} r_k$, which can be described by

$$F(y) = F(y_1, y_2, \cdots, y_n), \text{ for } y = \sum_{k=1}^{n} y_{\chi(k)} \cdot \prod_{i=0}^{k-1} r_{\chi(i)},$$

where $r_{\chi(0)} = 1$. The sequence $F(y)$ is called *evaluated* from the array $F(y_1, y_2, \cdots, y_n)$.

The aperiodic auto-correlation $C_{\vec{f}}(\tau)$ of sequence $F(y)$ can be derived from the sum of aperiodic auto-correlation $C_{\vec{f}}(\boldsymbol{\tau})$ of array $F(\boldsymbol{y})$ by restricting $\tau = \sum_{k=1}^{n} \tau_{\chi(k)} \cdot \prod_{i=0}^{k-1} r_{\chi(i)}$, i.e.,

$$C_{\vec{f}}(\tau) = \sum_{\boldsymbol{\tau} \in \mathcal{D}(\tau)} C_{\vec{f}}(\boldsymbol{\tau}),$$

where $\mathcal{D}(\tau) = \{\boldsymbol{\tau} | \tau = \sum_{k=1}^{n} \tau_{\chi(k)} \cdot \prod_{i=0}^{k-1} r_{\chi(i)}\}$. Naturally, we have the following property.

Property 9. *The sequence pair $\{F(y), G(y)\}$ of length $L = \prod_{k=1}^{n} r_k$ evaluated from the GAP $\{F(\boldsymbol{y}), G(\boldsymbol{y})\}$ of size $r_1 \times r_2 \cdots \times r_n$ form a GCP.*

Example 10. The GCP in Fact 2 is evaluatd (for the permutation χ) from the GAP of size $2 \times 2 \times \cdots \times 2$,

$$\begin{cases} f(x_1, x_2, \cdots, x_m) = 2 \cdot \sum_{k=1}^{m-1} x_k x_{k+1} + \sum_{k=1}^{m} c_k \cdot x_k + c_0, \\ g(x_1, x_2, \cdots, x_m) = f(x_1, x_2, \cdots, x_m) + x_1 \text{ or } x_m, \end{cases} \tag{14}$$

where $c_k \in \mathbb{Z}_4 (0 \le k \le m)$. The π in Fact 2 satisfy $\pi = \chi^{-1}$.

4.3 GAPs over QAM

Let $F_{i,j}(\boldsymbol{y})$ $(0 \le i, j \le 1)$ be m-dimensional arrays over 4^q-QAM, whose corresponding vectorial-function $\vec{f}_{i,j}(\boldsymbol{y}) = (f_{i,j}^{(0)}(\boldsymbol{y}), f_{i,j}^{(1)}(\boldsymbol{y}), \cdots, f_{i,j}^{(q-1)}(\boldsymbol{y}))$. The array set can be presented in a formalized matrix of order 2, i.e.,

$$\begin{pmatrix} F_{0,0}(\boldsymbol{y}) & F_{0,1}(\boldsymbol{y}) \\ F_{1,0}(\boldsymbol{y}) & F_{1,1}(\boldsymbol{y}) \end{pmatrix}.$$

The associated vectorial functions can be repesented with a set of q function matrices as $\{\widetilde{\boldsymbol{M}}^{(p)}(\boldsymbol{y}) | 0 \le q \le p-1\}$, where

$$\widetilde{\boldsymbol{M}}^{(p)}(\boldsymbol{y}) = \begin{pmatrix} f_{0,0}^{(p)}(\boldsymbol{y}) & f_{0,1}^{(p)}(\boldsymbol{y}) \\ f_{1,0}^{(p)}(\boldsymbol{y}) & f_{1,1}^{(p)}(\boldsymbol{y}) \end{pmatrix}.$$

In this paper, we are only interested in arrays of size $\underbrace{2 \times 2 \times \cdots \times 2}_{m} \times \underbrace{8 \times 8 \times \cdots \times 8}_{n}$. For convenience, define the Boolean variables $(\boldsymbol{x}, \boldsymbol{y}) = (x_1, x_2, \ldots, x_m, y_1, \ldots, y_n) \in \mathbb{Z}_2^m \times \mathbb{Z}_8^n$. For $1 \le k \le n$, denote by $a_k(y), b_k(y), a_k^*(y), b_k^*(y)$ (where $0 \le y = 4x_3 + 2x_2 + x_1 \le 7$) the sequences given in (3). For each k satisfying $0 \le k \le n$, function $h_k(x_1, y, x_2) : \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ is given by

$$\begin{aligned} h_k(x_1, y, x_2) =& (1 - x_1) \cdot a_k(y) \cdot (1 - x_2) \ + (1 - x_1) \cdot b_k^*(y) \cdot x_2 \\ &+ x_1 \cdot b_k(y) \cdot (1 - x_2) \ + x_1 \cdot (a_k^*(y) + 2) \cdot x_2. \end{aligned} \tag{15}$$

Theorem 11. *Define $\mathcal{N} = \{\sigma(1), \sigma(2), \cdots, \sigma(n)\} \subset \{0, 1, \cdots, m\}$ (where $\sigma(1) < \sigma(2) < \cdots < \sigma(n)$). Let $\omega \in \{0, 1, \cdots, m\} / \mathcal{N}$. Define $x_0 = x_{m+1} \equiv 0$ as "fake" variables. In the above context, $(F_{i,j}(\boldsymbol{y}), F_{i,1-j}(\boldsymbol{y}))$ and $(F_{i,j}(\boldsymbol{y}), F_{1-i,j}(\boldsymbol{y}))$ form GAPs, if for $0 \le p \le q-1$,*

$$\widetilde{\boldsymbol{M}}^{(p)}(\boldsymbol{x}, \boldsymbol{y}) = \mu_A^{(p)}(\boldsymbol{x}, \boldsymbol{y}) \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + \mu_B^{(p)}(\boldsymbol{x}, \boldsymbol{y}) \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + \left(f(\boldsymbol{x}, \boldsymbol{y}) + s^{(p)}(\boldsymbol{x})\right) \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \tag{16}$$

where

- $f(\boldsymbol{x},\boldsymbol{y}) = 2\cdot\sum_{k\notin\mathcal{N}} x_k x_{k+1} + \sum_{t=1}^{n} h_k(x_{\sigma(t)}, y_t, x_{\sigma(t)+1})$.
- $s^{(p)}(\boldsymbol{x}) = d_1^{(p)} x_\omega + d_2^{(p)} x_{\omega+1} + d_0^{(p)}, \quad (\omega \in \{0,1,\cdots,m\}/\mathcal{N})$.
- $\mu_A^{(p)}(\boldsymbol{x},\boldsymbol{y}) = \begin{cases} h_1(1,y_1,x_1) - h_1(0,y_1,x_1), & (0\in\mathcal{N}); \\ 2x_1 + d_1^{(p)}, & (\omega = 0); \\ 2x_1, & \textit{otherwise.} \end{cases}$
- $\mu_B^{(p)}(\boldsymbol{x},\boldsymbol{y}) = \begin{cases} h_n(x_m,y_n,1) - h_n(x_m,y_n,0), & (m\in\mathcal{N}); \\ \left(2x_m + d_2^{(p)}\right), & (\omega = m); \\ 2x_m, & \textit{otherwise.} \end{cases}$

Due to the constraints of the paper length, the proof of Theorem 11 is left in extended paper. The array pairs in first row and column in the array matrix form GAPs, which are presented in the following corollary.

Corollary 12. *The array pair over 4^q-QAM given by the following vectorial functions form GAPs.*

$$\begin{cases} \vec{f}(\boldsymbol{x},\boldsymbol{y}) = f(\boldsymbol{x},\boldsymbol{y})\cdot\vec{1} + \vec{s}(\boldsymbol{x}), \\ \vec{g}(\boldsymbol{x},\boldsymbol{y}) = \vec{f}(\boldsymbol{x},\boldsymbol{y}) + \vec{\mu}_A(\boldsymbol{x},\boldsymbol{y}) \ (or\ \vec{\mu}_B(\boldsymbol{x},\boldsymbol{y})), \end{cases} \tag{17}$$

where $\vec{s}(\boldsymbol{x}) = \left(s^{(p)}(\boldsymbol{x})|0\le p\le q-1\right)$, $\vec{\mu}_A(\boldsymbol{x},\boldsymbol{y}) = \left(\mu_A^{(p)}(\boldsymbol{x},\boldsymbol{y})|0\le p\le q-1\right)$, $\vec{\mu}_B(\boldsymbol{x},\boldsymbol{y}) = \left(\mu_B^{(p)}(\boldsymbol{x},\boldsymbol{y})|0\le p\le q-1\right)$ are given in Theorem 11.

The main result of GCPs over 4^q-QAM in Theorem5 are evaluated from Corollary 12, according to Properties 8 and 9.

5 Concluding Remarks

We proposed a construction of non-standard 4^q-QAM GCPs, which are based on weighted-sum of q non-standard QPSK GCSs in Theorem 5. As an elementary proof, we show that the 4^q-QAM GCPs is derived from 4^q-QAM GAPs. The comprehensive enumeration and proof in details will be given in an extended paper. A generalized construction of 4^q-QAM GCPs based on factorization of q[16] and non-symmetrical Gaussian integer pair (NSGIP)[14] will be introduced in our future work.

Our research amended the conjecture proposed by [11] with explicit algebraic expression. However, as GCSs over QAM given in [1] lack explicit algebraic expression, their relationship with GCSs over QAM based on non-standard GCSs and offsets is yet not clear. This may be left as an open problem.

References

[1] S. Z. Budišin and P. Spasojević. Paraunitary-based Boolean generator for QAM complementary sequences of length 2^K. *IEEE Trans. Inf. Theory*, 64(8):5938–5956, Aug. 2018.

[2] C.-Y. Chang, Y. Li, and J. Hirata. New 64-QAM Golay complementary sequences. *IEEE Trans. Inf. Theory*, 56(5):2479–2485, 2010.

[3] C. V. Chong, R. Venkataramani, and V. Tarokh. A new construction of 16-QAM Golay complementary sequences. *IEEE Trans. Inf. Theory*, 49(11):2953–2959, 2003.

[4] J. A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Trans. Inf. Theory*, 45(7):2397–2417, 1999.

[5] F. Fiedler and J. Jedwab. How do more Golay sequences arise? *IEEE Trans. Inf. Theory*, 52(9):4261–4266, 2006.

[6] F. Fiedler, J. Jedwab, and M. G. Parker. A framework for the construction of Golay sequences. *IEEE Trans. Inf. Theory*, 54(7):3114–3129, 2008.

[7] F. Fiedler, J. Jedwab, and M. G. Parker. A multi-dimensional approach to the construction and enumeration of Golay complementary sequences. *J. Combin. Theory (Series A)*, 115(5):753–776, 2008.

[8] M. J. E. Golay. Complementary series. *IRE Trans. Inf. Theory*, 7(2):82–87, 1961.

[9] C. Rößing and V. Tarokh. A construction of OFDM 16-QAM sequences having low peak powers. *IEEE Trans. Inf. Theory*, 47(5):2091–2094, 2001.

[10] H. Lee and S. W. Golomb. A new construction of 64-QAM Golay complementary sequences. *IEEE Trans. Inf. Theory*, 52(4):1663–1670, 2006.

[11] Y. Li. Comments on "A new construction of 16-QAM Golay complementary sequences" and extension for 64-QAM Golay sequences. *IEEE Trans. Inf. Theory*, 54(7):3246–3251, 2008.

[12] Y. Li. A construction of general QAM Golay complementary sequences. *IEEE Trans. Inf. Theory*, 56(11):5765–5771, 2010.

[13] Y. Li and W. B. Chu. More Golay sequences. *IEEE Trans. Inf. Theory*, 51(3):1141–1145, 2005.

[14] Z. Liu, Y. Li, and Y. L. Guan. New constructions of general QAM Golay complementary sequences. *IEEE Trans. Inf. Theory*, 59(11):7684–7692, 2013.

[15] Z. Wang, D. Ma, G. Gong, and E. Xue. New construction of complementary sequence (or array) sets and complete complementary codes. *on the second round review of IEEE Trans. Inf. Theory*, [Online]. Available: https://arxiv.org/abs/2001.04898.

[16] Z. Wang, E. Xue, and G. Gong. New Constructions of Complementary Sequence Pairs over 4^q-QAM. [Online]. Available: https://arxiv.org/abs/2003.03459.