Complex Orthogonal Designs with Forbidden 2×2 Submatrices

Yuan Li and Haibin Kan

Abstract

Complex orthogonal designs (CODs) are used to construct space-time block codes. COD $\mathcal{O}_z$ with parameter $[p, n, k]$ is a $p \times n$ matrix, where nonzero entries are filled by $\pm z_i$ or $\pm z_i^*$, $i = 1, 2, \ldots, k$, such that $\mathcal{O}_z^H \mathcal{O}_z = (|z_1|^2 + |z_2|^2 + \ldots + |z_k|^2) I_{n \times n}$. Define $\mathcal{O}_z$ an M-type COD if and only if $\mathcal{O}_z$ does not contain submatrix $\begin{pmatrix} \pm z_j & 0 \\ 0 & \pm z_j^* \end{pmatrix}$ or $\begin{pmatrix} \pm z_j^* & 0 \\ 0 & \pm z_j \end{pmatrix}$. It is already known that, all CODs with maximal rate, i.e., maximal k/p, are of M-type.

In this paper, we determine all achievable parameters $[p, n, k]$ of M-type COD, as well as all their possible structures. The existence of parameters is proved by explicit-form constructions. New M-type CODs with parameters $[p, n, k] = [\binom{n}{w-1} + \binom{n}{w+1}, n, \binom{n}{w}]$, for $0 \leq w \leq n$, are constructed, which demonstrate the possibility of sacrificing code rate to reduce decoding delay. It's worth mentioning that all maximal rate, minimal delay CODs are contained in our constructions, and their uniqueness under equivalence operation of all optimal CODs is proved.

1 Introduction

Space-time block codes have been widely investigated for wireless communication systems with multiple transmit and receive antennas. Since the pioneering work by Alamouti [7] in 1998, and the work by Tarokh et al. [23], [24], orthogonal designs have become an effective technique for the design of space-time block codes (STBC). The importance of this class of codes comes from the fact that they achieve full diversity and have the fast maximum-likelihood (ML) decoding.

A complex orthogonal design (COD) $\mathcal{O}_z[p, n, k]$ is an $p \times n$ matrix, and each entry is filled by $\pm z_i$ or $\pm z_i^*$, $i = 1, 2, \ldots, k$, such that $\mathcal{O}_z^H \mathcal{O}_z = \sum_{i=1}^{n} |z_i|^2 I_n$, where H is the Hermitian transpose and I_n is the $n \times n$ identity matrix. Under this definition, the designs are said to be combinatorial, in the sense that there is no linear processing in each entry. When linear combination of variables are allowed, we call it generalized complex orthogonal design (GCOD).

Code rate k/p and decoding delay p are the two most important criteria of complex orthogonal space-time block codes. One important problem is, given n, determine the tight upper bound of code rate, which is called maximal rate problem. Another is, given n, determine the tight lower bound of decoding delay p when code rate k/p reaches the maximal, which is called minimal delay problem.

For combinatorial CODs, where linear combination is not allowed, Liang determined for a COD with $n = 2m$ or $2m-1$, the maximal possible rate is $\frac{m+1}{2m}$ [14]. Liang gave an algorithm in [14] to generate such CODs with rate $\frac{m+1}{2m}$, which shows that this bound is tight. In [16], Yuan et al. simplifies Liang's proof on the upper bound of code rate slightly. The minimal delay problem are solved by Adams et al. In [5], lower bound $\binom{2m}{m-1}$ of decoding delay is proved for any $n = 2m$ or $2m-1$. In [6], Adams et al. prove that when $n \equiv 2 \pmod 4$, decoding delay p is lowered bound by $2\binom{2m}{m-1}$.

Besides some scattered constructions for relatively small number of antennas n [27], [23], [20], several general methods to construct complex orthogonal designs have been proposed. Liang's algorithmic construction in [14] achieves the maximal rate for all n, acheives the minimal delay when $n \equiv 1, 2, 3 \pmod 4$. But when $n \equiv 0 \pmod 4$, the delay is twice of the minimal delay. In [21], a different algorithmic method to generate complex orthogonal is proposed, which has the same code rate and decoding delay as Liang's construction. In [17], a closed-form iterative construction of complex orthogonal designs was proposed, which achieves both the maximal rate and minimal delay.

For GCOD, which allows linear combination in each entry, little is known about the rate and delay. In [15], they proved that there does not exist rate 1 GCOD when $n \geq 3$. In [26], Wang and Xia proved an upper bound $4/5$ of the code rate for GCODs without equal weight condition, and an upper bound $3/4$ with equal weight condition when $n \geq 3$. And this result is the best as far as we know.

The unfortunate property of COD is that for $n = 2m$ or $2m-1$ transmit antennas, the codes with maximal rate $(m+1)/(2m)$ has minimal decoding delay $\binom{2m}{m-1}$(with exception $n = 2 \pmod 4$ where it is $2\binom{2m}{m-1}$). For example, when $n = 14$, the minimal delay for a code with maximal rate is 6006! Therefore, it's meaningful to construct CODs with smaller decoding delay by sacrificing code rate and investigate the tradeoff between code rate and decoding delay. For example, in [3], Adams et al. considered a class of CODs with rate $\frac{1}{2}$ and proved a lower bound on delay.

In this paper, by restricting to a specific type of CODs which contains no submatrices $\begin{pmatrix} \pm z_j & 0 \\ 0 & \pm z_j^* \end{pmatrix}$ or $\begin{pmatrix} \pm z_j^* & 0 \\ 0 & \pm z_j \end{pmatrix}$, which are called M-type CODs in the paper, we consider the most general problem that determining what parameters $[p, n, k]$ are achievable. Not only all achievable parameters are determined, but also all their possible structures are also proved. It should be noticed that all CODs with maximal rate are of M-type, and thus it is not a very strict restriction.

The organization of our paper is as follows. In section 2, we we introduce the notions which will be used. In section 3, we review some basic definition and some known results about CODs. In section 4, we present our explicit-form constructions. In section 5, we prove our constructions in section 4 consist of all M-type CODs, up to equivalence operation and simple catenation operation. In section 5, we give out the conclusions.

2 Notations

In this section, we introduce some basic notions, which will be used in the sequel.

$\mathbb{C}$ denotes the field of complex numbers, $\mathbb{R}$ the field of real numbers and $\mathbb{F}_2$ the field with two elements. Adding over $\mathbb{F}_2$ is denoted by $\oplus$ to avoid ambiguity. All vectors are assumed to be column vectors. For any field $\mathbb{F}$, denoted by $\mathbb{F}^n$ and $M_{m\times n}(\mathbb{F})$ the set of all n-dimensional vectors in $\mathbb{F}$ and the set of all $m \times n$ matrices in $\mathbb{F}$, respectively. For any vector $x \in \mathbb{F}^n$, denote by x^T the transpose of x. For any matrix $A \in M_{m\times n}(\mathbb{C})$, denote by A^T the transpose of A and by A^H the conjugate transpose of A. Denote by

$$A(i_1, i_2, \ldots, i_p; j_1, j_2, \ldots, j_q) \text{ and } A(s_1, \ldots, s_2; t_1, \ldots, t_2)$$

the submatrix consisting of i_1^{th}, i_2^{th}, ..., i_p^{th} rows and the j_1^{th}, j_2^{th}, ..., j_q^{th} columns of A, and the submatrix consisting of the s_1^{th}, $(s_1+1)^{\text{th}}$, ..., s_2^{th} rows and the t_1^{th}, $(t_1+1)^{\text{th}}$, ..., t_2^{th} columns of A, where $s_1 < s_2$ and $t_1 < t_2$, respectively. We use $A(i,j)$ for the (i,j) element of the matrix A. In this paper, rows and variables are often indexed by vectors in $\mathbb{F}_n^2$.

For convenience, let $e_i \in \mathbb{F}_2^n$ be the vector with i^{th} bit occupied by 1 and the others 0, i.e., $e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i})$ and let $e = e_1 \oplus e_2 \oplus \ldots \oplus e_n$, i.e., $e = (1, 1, \ldots, 1)_2$.

The weight of a vector in $\mathbb{F}_2^n$ is defined as the number of ones in n bits, i.e., $\text{wt}(\alpha) = \sum_{i=1}^{n} \alpha(i)$. Furthermore, $\text{wt}_{s,t}(\alpha)$ is defined as the sum of s^{th} bit to t^{th} bit, i.e.,

$$\text{wt}_{s,t}(\alpha) = \alpha(s) + \alpha(s+1) + \cdots + \alpha(t) = \sum_{i=s}^{t} \alpha(i).$$

In abuse of notation, we denote by $z[j]$ the complex variable z_j, up to negation and conjugation, i.e., $z[j] \in \{z_j, -z_j, z_j^*, -z_j^*\}$. Note that the same notation $z[j]$ may represent different elements in the same paragraph.

3 Definitions and Some Known Results

Definition 3.1. *A $[p, n, k]$ complex orthogonal design $\mathcal{O}_z$ is a $p \times n$ rectangular matrix whose nonzero entries are*

$$z_1, z_2, \ldots, z_k, -z_1, -z_2, \ldots, -z_k$$

or their conjugates

$$z_1^*, z_2^*, \ldots, z_k^*, -z_1^*, -z_2^*, \ldots, -z_k^*,$$

where $z_1, z_2, \ldots, z_k$ are indeterminates over $\mathbb{C}$, such that

$$\mathcal{O}_z^H \mathcal{O}_z = (|z_1|^2 + |z_2|^2 + \cdots + |z_k|^2) I_{n\times n}.$$

k/p is called the code rate of $\mathcal{O}_z$, and p is called the decoding delay of $\mathcal{O}_z$.

A matrix is called an Alamouti 2×2 if it matches the following form

$$\begin{pmatrix} z_i & z_j \\ -z_j^* & z_i^* \end{pmatrix}, \tag{1}$$

up to negation or conjugation of z_i or z_j. We say two rows share an Alamout 2×2 if and only if the intersection of the two rows and some two columns form an Alamouti 2×2.

Definition 3.2. *The equivalence operations performed on any COD are defined as follows.*

1) Rearrange the order the rows("row permutation").

2) Rearrange the order the columns ("column permutation").

3) Conjugate all instances of certain variable ("instance conjugation").

4) Negate all instances of certain variable ("instance negation").

5) Change the index of all instances of certain variable ("instance renaming").

6) Multiply any row by -1, ("row negation").

7) Multiply any column by -1, ("column negation").

It's not difficult to verify that, given a COD $\mathcal{O}_z[p, n, k]$, after arbitrary equivalence operations, we will obtain another COD $\mathcal{O}'_z[p, n, k]$. And we say COD $\mathcal{O}_z$ and $\mathcal{O}'_z$ are the same under equivalence operations.

Following the definition in [14], define an $(n_1, n_2) - \mathcal{B}_j$ form by

$$\begin{aligned}
\mathcal{B}_j &= \begin{pmatrix} z_j I_{n_1} & \mathcal{M}_1 \\ -\mathcal{M}_1^H & z_j^* I_{n_2} \end{pmatrix} \\
&= \left(\begin{array}{cccc|cccc} z_j & 0 & \cdots & 0 & & & & \\ 0 & z_j & \cdots & 0 & & & & \\ \vdots & \vdots & \ddots & \vdots & & \mathcal{M}_j & & \\ 0 & 0 & \cdots & z_j & & & & \\ \hline & & & & z_j^* & 0 & \cdots & 0 \\ & -\mathcal{M}_j^H & & & 0 & z_j^* & \cdots & 0 \\ & & & & \vdots & \vdots & \ddots & \vdots \\ & & & & 0 & 0 & \cdots & z_j^* \end{array}\right),
\end{aligned} \tag{2}$$

where $n_1 + n_2 = n$. And we call it $\mathcal{B}_j$ form for short.

Definition 3.3. *[5] We say COD $\mathcal{O}_z$ is in $\mathcal{B}_j$ form if the submatrix $\mathcal{B}_j$ can be created from $\mathcal{O}_z$ through equivalence operations except for column permutation. Equivalently, $\mathcal{O}_z$ is in $\mathcal{B}_j$ form if every row of $\mathcal{B}_j$ appears within the rows of $\mathcal{O}_z$, up to possible conjugations of all instances of z_i and possible factors of -1.*

It is proved that [5] that COD $\mathcal{O}_z$ is in some $\mathcal{B}_j$ form if and only if one row in $\mathcal{O}_z$ matches one row of $\mathcal{B}_j$ up to signs and conjugations.

In [14], Liang proved the upper bound $\frac{m+1}{2m}$ of code rate $\frac{k}{p}$ for any $n = 2m$ or $2m - 1$, and obtained the necessary and sufficient condition to reach the maximal rate.

Theorem 3.4. *Let $n = 2m$ or $2m - 1$. The rate of COD $\mathcal{O}_z[p, n, k]$ is upper bounded by $\frac{m+1}{2m}$, i.e., $\frac{k}{p} \leq \frac{m+1}{2m}$.*

This bound is achieved if and only if for all $i = 1, 2, \ldots, k$, $\mathcal{B}_j$ is an $(m, m-1) - \mathcal{B}_j$ or $(m-1, m) - \mathcal{B}_j$ form and there are no zero entries in $\mathcal{M}_j$, when $n = 2m - 1$; $\mathcal{B}_j$ is an $(m, m) - \mathcal{B}_j$ form and there are no zero entries in $\mathcal{M}_j$, when $n = 2m$

The lower bound on the decoding delay when code rate reaches the maximal is completely solved by Adams et al. in [5] and [6].

Theorem 3.5. *Let $n = 2m$ or $2m-1$. For COD $\mathcal{O}_z[p,n,k]$, if the rate reaches the maximal, i.e., $\frac{k}{p} = \frac{m+1}{2m}$, the delay, i.e., p, is lower bounded by $\binom{2m}{m-1}$ when $n \equiv 0,1,3 \pmod 4$; by $2\binom{2m}{m-1}$ when $n \equiv 2 \pmod 4$.*

The technique in proving the lower bound $\binom{2m}{m-1}$ is the observation and definition of zero pattern, which is a vector in $\mathbb{F}_2^n$ defined with respect to one row where the i^{th} bit is 0 if and only if the element on column i is 0. For example, when

$$\mathcal{O}_z = \begin{pmatrix} z_1 & z_2 & z_3 \\ -z_2^* & z_1^* & 0 \\ -z_3^* & 0 & z_1^* \\ 0 & z_3^* & -z_2^* \end{pmatrix}, \tag{3}$$

the first row has zero pattern $(1,1,1)$, the second $(1,1,0)$, the third $(1,0,1)$, the fourth $(0,1,1)$.

Next, we present some new definitions.

Definition 3.6. *COD $\mathcal{O}_z[p,n,k]$ is an M-type COD if it does not contain submatrix*

$$\begin{pmatrix} \pm z_j & 0 \\ 0 & \pm z_j^* \end{pmatrix} \text{ or } \begin{pmatrix} \pm z_j^* & 0 \\ 0 & \pm z_j \end{pmatrix},$$

where $1 \le j \le k$.

In other words, COD $\mathcal{O}_z[p,n,k]$ is of M-type if for all $1 \le j \le k$, there is no zero entry in $\mathcal{M}_j$ of its $\mathcal{B}_j$ form. By Theorem 3.4, we can see all maximal-rate CODs are in M-type.

Definition 3.7. *COD $\mathcal{O}_z[p,n,k]$ is called atomic if and only if there does not exist a COD which is a submatrix of $\mathcal{O}_z$ consisting of some (not all) rows of $\mathcal{O}_z$.*

Formally, $\mathcal{O}_z[p,n,k]$ is atomic if and only if for any integers $1 \le q \le p-1, 1 \le i_1 < i_2 < \cdots\ i_q \le p$, $\mathcal{O}_z(i_1, i_2, \ldots, i_q; 1, \ldots, n)$ is a not COD. Otherwise, $\mathcal{O}_z[p,n,k]$ is called non-atomic.

For an atomic COD $\mathcal{O}_z[p,n,k]$, given any $1 \le s,t \le k$, there exist $j_1 = s, j_2, \ldots, j_{m-1}, j_m = t$ such that $\mathcal{B}_{j_1}$ and $\mathcal{B}_{j_2}$ share some common rows, $\mathcal{B}_{j_2}$ and $\mathcal{B}_{j_3}$ share some common rows, ..., $\mathcal{B}_{j_{m-1}}$ and $\mathcal{B}_{j_m}$ share some common rows. This condition is also sufficient for a COD to be atomic.

For COD $\mathcal{O}_z$, assume one row is in some atomic COD $\mathcal{O}_z'$ which consists of some rows of $\mathcal{O}_z$. If one variable is in $\mathcal{O}_z'$, then all rows containing this variable is in $\mathcal{O}_z'$. Repeat this procedure until no more rows are added. Finally, atomic COD $\mathcal{O}_z'$ is obtained. By the above algorithm, we can see COD $\mathcal{O}_z$ can be decomposed into atomic ones in a unique way.

For example, let $\mathcal{O}_z$ consists of the first two columns of (3), i.e.,

$$\mathcal{O}_z = \begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \\ -z_3^* & 0 \\ 0 & z_3^* \end{pmatrix}. \tag{4}$$

Then $\mathcal{O}_z$ can be decomposed into two atomic CODs

$$\begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \end{pmatrix} \text{ and } \begin{pmatrix} -z_3^* & 0 \\ 0 & z_3^* \end{pmatrix}.$$

On the contrary to the decomposition of COD, given two (or more) CODs with parameters $\mathcal{O}_1[p_1, n, k_1]$ and $\mathcal{O}_2[p_2, n, k_2]$, we can construct a new COD with parameter $[p_1 + p_2, n, k_1 + k_2]$ by simply catenating them, i.e., $\begin{pmatrix} \mathcal{O}_1 \\ \mathcal{O}_2 \end{pmatrix}$, and renaming certain variables of $\mathcal{O}_1$ and $\mathcal{O}_2$ to avoid conflicts if necessary. We call it catenation operation.

4 Explicit-form Constructions

In this section, we present explicit-form constructions of M-type CODs. The basic idea is first to construct a basic COD with rate 1/2 and parameters $[2^{n+1}, n, 2^n]$, which are based on combinatorial methods by using vectors in $\mathbb{F}_2^{n+1}$. Then, by choosing submatrices from the basic COD, we obtain CODs with paramters

$$[p, n, k] = [\binom{n}{w-1} + \binom{n}{w+1}, n, \binom{n}{w}],$$

where $-1 \leq w \leq n+1$. Note that, when $n \not\equiv 0 \pmod 4$, all maximal-rate, minimal-delay CODs are contained in the above constructions.

Next, we consider $n \equiv 0 \pmod 4$. By padding an extra column on our basic COD, we obtain COD with parameter $[2^n, n, 2^{n-1}]$. Again, by choosing submatrices from the basic COD, we obtain CODs with parameters $[\binom{n}{n/2+1}, n, \binom{n-1}{n/2-1}]$, which contains the codes with maximal rate and minimal decoding delay.

Theorem 4.1. *Let $\mathcal{G}_n$ be $2^{n+1} \times n$ matrix, where rows are indexed by vectors in $\mathbb{F}_2^{n+1}$ and columns are indexed by $1, 2, \ldots, n$. For all $\alpha \in \mathbb{F}_2^{n+1}, 1 \leq i \leq n$,*

- *if $\alpha(i) = 0$, then $\mathcal{G}_n(\alpha, i) = 0$,*
- *if $\alpha(i) = 1$ and $\alpha(n+1) = 0$, then $\mathcal{G}_n(\alpha, i) = (-1)^{\theta(\alpha,i)} z_{\varphi(\alpha,i)}$,*
- *if $\alpha(i) = 1$ and $\alpha(n+1) = 1$, then $\mathcal{G}_n(\alpha, i) = (-1)^{\theta(\alpha,i)} z^*_{\varphi(\alpha,i)}$,*

where

$$\theta(\alpha, i) = \begin{cases} wt_{i,n+1}(\alpha) + \frac{n-i}{2}, & \text{if } n-i \text{ is even}, \\ wt_{i,n+1}(\alpha) + \frac{n-i-1}{2} + \alpha(n+1), & \text{if } n-i \text{ is odd}, \end{cases} \tag{5}$$

and

$$\begin{aligned} \varphi(\alpha, i) &= \alpha \oplus \alpha(n+1)e \oplus e_i \\ &= (\alpha(1) \oplus \alpha(n+1), \ldots, \alpha(i) \oplus \alpha(n+1) \oplus 1, \ldots, \\ &\quad \alpha(n+1) \oplus \alpha(n+1)). \end{aligned}$$

Then $\mathcal{G}_n$ is a COD with parameter $[2^{n+1}, n, 2^n]$.

Proof. It is sufficient to prove 1) every variable, up to negation or conjugation, appears exactly once in each column; 2) any two different columns are orthogonal.

Since for fixed i, $\varphi(\alpha, i)$ takes nonzero values on 2^n different vectors $\alpha \in \mathbb{F}_2^{n+1}, \alpha(i) = 1$. To prove 1), we only need to show φ is a surjective, i.e. $\alpha \neq \beta \Rightarrow \varphi(\alpha, i) \neq \varphi(\beta, i)$. Suppose to the contrary that there exists α and β where $\alpha \neq \beta$, $\alpha(i) = \beta(i) = 1$ and $\varphi(\alpha, i) = \varphi(\beta, i)$. Expanding $\varphi(\alpha, i) = \varphi(\beta, i)$ by definition, we have

$$\alpha \oplus \alpha(n+1)e \oplus e_i = \beta \oplus \beta(n+1)e \oplus e_i,$$

which is equivalent to

$$\alpha \oplus \beta = (\alpha(n+1) \oplus \beta(n+1))e.$$

If $\alpha(n+1) = \beta(n+1)$, then $\alpha \oplus \beta = (\alpha(n+1) \oplus \beta(n+1))e = 0 \Rightarrow \alpha = \beta$, which is contradicted with $\alpha \neq \beta$. If $\alpha(n+1) \neq \beta(n+1)$, then $\alpha \oplus \beta = (\alpha(n+1) \oplus \beta(n+1))e = e$, which is contradicted with $\alpha(i) = \beta(i) = 1$.

To prove any two different columns are orthogonal, it is sufficient to show that, every pair of nonzero entries in the same row are in an Alamouti 2×2.

Let columns $1 \leq i < j \leq n$ and $\alpha \in \mathbb{F}_2^{n+1}$ be any row, satisfying $\alpha(i) = \alpha(j) = 1$. Let $\gamma = \varphi(\alpha, i)$, $\delta = \varphi(\alpha, j)$. Since every variable appears exactly once in each column, we assume $z[\delta]$ appears in the β^{th} row in i^{th} column, i.e., $\varphi(\beta, i) = \gamma$.

By the assumption that $z[\delta]$ appears in $\mathcal{G}_n(\beta, i)$, we have $\varphi(\beta, i) = \varphi(\alpha, j)$, i.e.,

$$\alpha \oplus \alpha(n+1)e \oplus e_j = \beta \oplus \beta(n+1)e \oplus e_i,$$

which implies

$$\begin{aligned} \beta &= \alpha \oplus \alpha(n+1)e \oplus e_j \oplus \beta(n+1)e \oplus e(i) \\ &= \alpha \oplus (\alpha(n+1) \oplus \beta(n+1))e \oplus e_i \oplus e_j. \end{aligned} \tag{6}$$

Noting that φ takes nonzero value on (α, i), (α, j) and (β, i), we have $\alpha(i) = \alpha(j) = \beta(j) = 1$. Considering i^{th} value in equality (6), we conclude $\alpha(n+1) \oplus \beta(n+1) = 1$. Thus,

$$\alpha \oplus \beta = e \oplus e_i \oplus e_j. \tag{7}$$

Taking $\beta = \alpha \oplus e \oplus e_i \oplus e_j$ into $\varphi(\beta, j)$, we have

$$\begin{aligned} \varphi(\beta, j) &= \beta \oplus \beta(n+1)e \oplus e_j \\ &= \alpha \oplus \alpha(n+1)e \oplus e_j \oplus \beta(n+1)e \oplus e_i \oplus \beta(n+1)e \oplus e_j \\ &= \alpha \oplus \alpha(n+1)e \oplus e_i \\ &= \varphi(\alpha, i). \end{aligned}$$

Therefore, submatrix $\mathcal{G}_n(\alpha, \beta; i, j)$ could be written in either of the two following forms

$$\begin{pmatrix} (-1)^{\theta(\alpha,i)} z_\gamma & (-1)^{\theta(\alpha,j)} z_\delta \\ (-1)^{\theta(\beta,i)} z_\delta^* & (-1)^{\theta(\beta,j)} z_\gamma^* \end{pmatrix}$$

or

$$\begin{pmatrix} (-1)^{\theta(\alpha,i)} z_\gamma^* & (-1)^{\theta(\alpha,j)} z_\delta^* \\ (-1)^{\theta(\beta,i)} z_\delta & (-1)^{\theta(\beta,j)} z_\gamma \end{pmatrix}.$$

Now we calculate $\theta(\alpha,i)+\theta(\alpha,j)+\theta(\beta,i)+\theta(\beta,j)$ to check whether it is an Alamouti 2×2. According to the parity of $n-i$ and $n-j$, discussions are divided into four cases.

When both $n-i$ and $n-j$ are evens,

$$\begin{aligned}
&\theta(\alpha,i)+\theta(\alpha,j)+\theta(\beta,i)+\theta(\beta,j)\\
\equiv&\,\mathrm{wt}_{i,n+1}(\alpha)+\frac{n-i}{2}+\mathrm{wt}_{j,n+1}(\alpha)+\frac{n-j}{2}+\\
&\,\mathrm{wt}_{i,n+1}(\beta)+\frac{n-i}{2}+\mathrm{wt}_{j,n+1}(\beta)+\frac{n-j}{2} && \text{by (5)}\\
\equiv&\,\mathrm{wt}_{i,n+1}(\alpha\oplus\beta)+\mathrm{wt}_{j,n+1}(\alpha\oplus\beta)\\
\equiv&\,(n-i)+(n-j)+1 && \text{by (7)}\\
\equiv&\,1 \pmod 2.
\end{aligned}$$

When $n-i$ is odd and $n-j$ is even,

$$\begin{aligned}
&\theta(\alpha,i)+\theta(\alpha,j)+\theta(\beta,i)+\theta(\beta,j)\\
\equiv&\,\mathrm{wt}_{i,n+1}(\alpha)+\frac{n-i-1}{2}+\alpha(n+1)+\mathrm{wt}_{j,n+1}(\alpha)+\frac{n-j}{2}+\\
&\,\mathrm{wt}_{i,n+1}(\beta)+\frac{n-i-1}{2}+\beta(n+1)+\mathrm{wt}_{j,n+1}(\beta)+\frac{n-j}{2} && \text{by (5)}\\
\equiv&\,\mathrm{wt}_{i,n+1}(\alpha\oplus\beta)+\mathrm{wt}_{j,n+1}(\alpha\oplus\beta)+(\alpha(n+1)\oplus\beta(n+1))\\
\equiv&\,(n-i)+(n-j)+1+1 && \text{by (7)}\\
\equiv&1 \pmod 2.
\end{aligned}$$

When $n-i$ is even and $n-j$ is odd, it's similar with the above case.
When both $n-i$ and $n-j$ are odds,

$$\begin{aligned}
&\theta(\alpha,i)+\theta(\alpha,j)+\theta(\beta,i)+\theta(\beta,j)\\
\equiv&\,\mathrm{wt}_{i,n+1}(\alpha)+\frac{n-i-1}{2}+\alpha(n+1)+\mathrm{wt}_{j,n+1}(\alpha)+\\
&\,\frac{n-j-1}{2}+\alpha(n+1)+\mathrm{wt}_{i,n+1}(\beta)+\frac{n-i-1}{2}+\\
&\,\beta(n+1)+\mathrm{wt}_{j,n+1}(\beta)+\frac{n-j-1}{2}+\beta(n+1) && \text{by (5)}\\
\equiv&\,\mathrm{wt}_{i,n+1}(\alpha\oplus\beta)+\mathrm{wt}_{j,n+1}(\alpha\oplus\beta)\\
\equiv&\,(n-i)+(n-j)+1 && \text{by (7)}\\
\equiv&1 \pmod 2.
\end{aligned}$$

Therefore,

$$(-1)^{\theta(\alpha,i)}z_\gamma^*(-1)^{\theta(\alpha,j)}z_\delta+(-1)^{\theta(\beta,i)}z_\delta(-1)^{\theta(\beta,j)}z_\gamma^*=0$$

holds and the submatrix $\mathcal{G}_n(\alpha,\beta;i,j)$ is an Alamouti 2×2, which implies column i and column j are orthogonal. The proof is complete. □

By taking out some submatrices form $\mathcal{G}_n$, we can get a series of atomic M-type CODs.

Theorem 4.2. *Given n, for arbitrary integer $-1 \leq w \leq n+1$, let*

$$\mathcal{G}_n^w = \mathcal{G}_n(\alpha_1, \ldots, \alpha_{\binom{n}{w+1}}, \beta_1, \ldots, \beta_{\binom{n}{n-w+1}}; 1 \sim n),$$

where α_i are all vectors in $\mathbb{F}_2^{n+1}$ with weight $w+1$ and the $(n+1)^{th}$ bit 0, β_i are all vectors in $\mathbb{F}_2^{n+1}$ with weight $n-w+2$ and the $(n+1)^{th}$ bit 1. Then $\mathcal{G}_n^w$ is a COD with parameter $[\binom{n}{w+1} + \binom{n}{w-1}, n, \binom{n}{w}]$.

Proof. Since $\mathcal{G}_n^w$ is a submatrix of the orthogonal design $\mathcal{G}_n$, it's sufficient to prove that if some variable exists on one column of $\mathcal{G}_n^w$ then it exists on every column of $\mathcal{G}_n^w$. We will show that all variables with subscript weight w exist on each column of $\mathcal{G}_n^w$.

For any $\alpha \in \mathbb{F}_2^{n+1}$ such that $\alpha(n+1) = 0, \alpha(i) = 1$ for some $1 \leq i \leq n$, as $\mathrm{wt}(\varphi(\alpha, i)) = \mathrm{wt}(\alpha \oplus e_i) = \mathrm{wt}(\alpha) - 1$, then $\mathrm{wt}(\varphi(\alpha, i)) = w$ if and only if $\mathrm{wt}(s) = w + 1$.

For any $\alpha \in \mathbb{F}_2^{n+1}$ such that $\alpha(n+1) = 1$, and $\alpha(i) = 1$ for some $1 \leq i \leq n$, as $\mathrm{wt}(\varphi(\alpha, i)) = \mathrm{wt}(\alpha \oplus e_i \oplus e) = n + 2 - \mathrm{wt}(\alpha)$, then $\mathrm{wt}(\varphi(\alpha, i)) = w$ if and only if $\mathrm{wt}(\alpha) = n - w + 2$.

Finally, there are $\binom{n}{w+1} + \binom{n}{n-w+1} = \binom{n}{w+1} + \binom{n}{w-1}$ rows taken and $\binom{n}{w}$ different variables in it. The proof is complete. □

Notice that, in the above constructions, $\mathcal{G}_n^{-1} = (0, 0, \ldots, 0)$ is a trivial COD with rate 0 and delay 1.

For fixed number of antennas n, the code rate

$$\frac{\binom{n}{m}}{\binom{n}{m+1} + \binom{n}{m-1}} = \left(\frac{n-m}{m+1} + \frac{m}{n-m+1}\right)^{-1}$$

is an increasing function of m when $-1 \leq m \leq \lfloor \frac{n}{2} \rfloor$, as well as the decoding delay $\binom{n}{m}$. Since the decoding delay $\binom{n}{m}$ grows very fast when m is increasing, the sacrifice in rate might be worth the trade-off for a smaller decoding delay in practice.

For example, let $n = 14$, $m = 0, 1, \ldots, 7$ respectively, we obtain codes with the following parameters with rate decreasing and delay incresing.

Table 1: Code rate and delay for $n = 14$

m	k	rate $= k/p$	delay $= p$
0	1	0.071	14
1	14	0.152	92
2	91	0.241	378
3	364	0.333	1092
4	1001	0.423	2366
5	2002	0.500	4004
6	3003	0.553	5434
7	3432	0.571	6006

Like the Alamouti 2×2 in [7], certain CODs enjoy a property known as transceiver signal linearization, which can facilitate decoding. This linearization allows the code to be backward compatible with existing signal processing techniques and standards, and allows for the design of low complexity interference

suppressing filters and channel equalizers [19]. It has been shown that a complex orthogonal design can achieve transceiver signal linearization if and only if each row in the code has either all conjugated entries or all non-conjugated entries [19], which is called conjugation separated. Note that $\mathcal{G}_n$ and $\mathcal{G}_n^w$ are all conjugation separated and thus satisfy the transceiver signal linearization property.

When $n \equiv 0 \pmod 4$, it's possible to pad an extra column on $\mathcal{G}_{n-1}$ to obtain a new COD.

Theorem 4.3. *For positive integer $n = 2m, m$ even, let $\mathcal{Q}_n = (\mathcal{G}_{n-1}, \mathcal{H}_n)$, where $\mathcal{H}_n(\alpha) = \alpha(n)(-1)^{\psi(\alpha)} z_{\alpha \oplus e_n}$, for all $\alpha \in \mathbb{F}_2^n$ and $\psi(\alpha) = \sum_{i=1}^{m} \alpha(2i)$. Then $\mathcal{Q}_n$ is a COD with parameter $[2^n, n, 2^{n-1}]$.*

Proof. From Theorem 4.1, we claim columns in $\mathcal{G}_{n-1}$ are pairwise orthogonal. By proving $\mathcal{H}_n$ is orthogonal to the other columns, we can complete the proof. It's obvious that each variable exists on $\mathcal{H}_n$ only once. It only remains to prove any two nonzero elements(one is on $\mathcal{H}_n$) in the same row are in an Alamouti 2×2.

Consider column $1 \leq i \leq n-1$ and column n. For row $\alpha \in \mathbb{F}_2^n$ and $\alpha(i) = \alpha(n) = 1$, $\mathcal{Q}_n(\alpha, i) = (-1)^{\theta(\alpha,i)} z^*_{\varphi(\alpha,i)}$ and $\mathcal{Q}_n(\alpha, n) = (-1)^{\psi(\alpha)} z_{\alpha \oplus e_n}$. Since each variable exists in $\mathcal{H}_n$, there exists an integer $\beta \in \mathbb{F}_2^n, \beta(n) = 1$ such that $|\mathcal{Q}_n(\beta, n)| = |\mathcal{Q}_n(\alpha, i)|^*$, which is

$$\beta \oplus e_n = \alpha \oplus \alpha(n)e \oplus e_i.$$

Noting that $\alpha(n) = 1$, thus,

$$\beta = \alpha \oplus e \oplus e_i \oplus e_n. \tag{8}$$

which implies $\beta(i) = \beta(n) = 1$. Now, we calculate the subscript of the variable in $\mathcal{Q}_n(\beta, i)$.

$$\begin{aligned} \varphi(\beta, i) &= \beta \oplus \beta(n)e \oplus e_i \\ &= \alpha \oplus e \oplus e_i \oplus e_n \oplus e \oplus e_i \\ &= \alpha \oplus e_n, \end{aligned}$$

which is equal to the subscript of variable in $\mathcal{Q}_n(\alpha, n)$. Therefore, the submatrix $\mathcal{Q}_n(\alpha, \beta; i, n)$ could be written as follows

$$\begin{pmatrix} (-1)^{\theta(\alpha,i)} z^*_\gamma & (-1)^{\psi(\alpha)} z_\delta \\ (-1)^{\theta(\beta,i)} z^*_\delta & (-1)^{\psi(\beta)} z_\gamma, \end{pmatrix},$$

where $\gamma = \alpha \oplus e_i \oplus e_n$ and $\delta = \alpha \oplus e_n$. Let's check the signs to verify whether it's an Alamouti 2×2.

When $(n-1)-i$ is even, i.e., i is odd,

$$\begin{aligned}
&\theta(\alpha,i)+\psi(\alpha)+\theta(\beta,i)+\psi(\beta)\\
\equiv&\,\mathrm{wt}_{i,n}(\alpha)+\frac{(n-1)-i}{2}+\sum_{k=0}^{m}\alpha(2k)+\\
&\,\mathrm{wt}_{i,n}(\beta)+\frac{(n-1)-i}{2}+\sum_{k=1}^{m}\beta(2k) && \text{by definition}\\
\equiv&\,\mathrm{wt}_{i,n}(\alpha\oplus\beta)+\sum_{k=1}^{m}(\alpha(2k)\oplus\beta(2k))\\
\equiv&\,(n-i-1)+(m-1) && \text{by (8)}\\
\equiv&\,1 \pmod 2.
\end{aligned}$$

When $(n-1)-i$ is odd, i.e., i is even,

$$\begin{aligned}
&\theta(\alpha,i)+\psi(\alpha)+\theta(\beta,i)+\psi(\beta)\\
\equiv&\,\mathrm{wt}_{i,n}(\alpha)+\frac{(n-1)-i-1}{2}+\alpha(n)+\sum_{k=1}^{m}\alpha(2k)+\\
&\,\mathrm{wt}_{i,n}(\beta)+\frac{(n-1)-i-1}{2}+\beta(n)+\sum_{k=1}^{m}\beta(2k) && \text{by definition}\\
\equiv&\,\mathrm{wt}_{i,n}(\alpha\oplus\beta)+(\alpha\oplus\beta)(n)+\sum_{k=1}^{m}(\alpha(2k)\oplus\beta(2k))\\
\equiv&\,(n-i-1)+0+(m-2) && \text{by (8)}\\
\equiv&\,1 \pmod 2.
\end{aligned}$$

Therefore,

$$(-1)^{\theta(\alpha,i)}z_\gamma(-1)^{\psi(\alpha)}z_\delta+(-1)^{\theta(\beta,i)}z_\delta(-1)^{\psi(\beta)}z_\gamma=0$$

holds and the submatrix $\mathcal{Q}_n(\alpha,\beta;i,n)$ an Alamouti 2×2, which implies column i and column n are orthogonal. The proof is complete. □

Similar with the idea in Theorem 5.8, by taking out some submatrices of $\mathcal{Q}_n$, we can obtain new ones.

Theorem 4.4. *For positive integer $n=2m, m$ even, let*

$$\mathcal{Q}_n^m=\mathcal{Q}_n(\alpha_1,\ldots,\alpha_{\binom{n}{m+1}};1\sim n),$$

where α_i are all vectors in $\mathbb{F}_2^n$ with weight $m+1$. Then $\mathcal{Q}_n^m$ is a COD with parameter $[\binom{n}{m+1},n,\binom{n-1}{m}]$.

Proof. From Theorem 4.3, we know $\mathcal{Q}_n$ is orthogonal. Now we will prove that every variable with subscript weight m exists on each column, which implies $\mathcal{Q}_n^m$ is a COD.

For $\alpha\in\mathbb{F}_2^n,\alpha(n)=0,1\le i\le n-1$ and $\alpha(i)=1$, since $\mathrm{wt}(\varphi(\alpha,i))=\mathrm{wt}(\alpha\oplus e_i)=\mathrm{wt}(\alpha)-1$, then $\mathrm{wt}(\varphi(\alpha,i))=m$ if and only if $\mathrm{wt}(\alpha)=m+1$.

For $\alpha \in \mathbb{F}_2^n, \alpha(n) = 1, 1 \leq i \leq n-1$ and $\alpha(i) = 1$, since $\mathrm{wt}(\varphi(\alpha, i)) = \mathrm{wt}(\alpha \oplus e_i \oplus e) = n + 1 - \mathrm{wt}(\alpha)$, then $\mathrm{wt}(\varphi(\alpha, i)) = m$ if and only if $\mathrm{wt}(\alpha) = n + 1 - m = m + 1$.

For the last column, since $\mathcal{H}_n(\alpha) = (-1)^{\psi(\alpha)} z_{\alpha \oplus e_n}$ for $\alpha(n) = 1$, it's easy to see if $\mathrm{wt}(\alpha) = m + 1$, then $\mathrm{wt}(\psi(\alpha)) = 2m$ and vice versa. Therefore, the proof is complete. □

It's worth noticing that, for a given row, there are both conjugated and non-conjugated nonzero entries in $\mathcal{Q}_n$ and $\mathcal{Q}_n^w$, which violets the transceiver signal linearization property.

In [4], Adams et al. proved that when $n \equiv 1, 2, 3 \pmod 4$, maximal rate CODS with transceiver linearization can achieve the minimal delay, and when $n \equiv 0 \pmod 4$, it can not. Our explicit-form constrictions are consist with their results.

The CODs constructed by Liang in [14], and by Su and Xia in [20] is exactly $\mathcal{G}_n^m$, which achieves maximal rate and minimal delay when $n \not\equiv 0 \pmod 4$. The closed-form constructions in [17] are exactly $\mathcal{G}_n^m$ and $\mathcal{Q}_n^m$, and therefore achieve maximal rate and minimal delay for any n. The constructions in [3] by Adams et al. have rate $1/2$ and delay 2^{m-1} or 2^m, depending on the parity of n modulo 8. Those CODs do not belong to M-type, and have smaller decoding delay compared to $\mathcal{G}_n^w$ with rate $1/2$.

5 Structures of Atomic M-type CODs

In [6], it is proved that in a COD with parameter $[\binom{2m}{m-1}, n, \binom{2m-1}{m-1}]$ when $n = 2m$ or $2m-1$, row α and row β share an Alamout 2×2 over column i and j if and only if the zero pattern of row α and row β are simultaneously nonzero exactly in columns i and j and never simultaneously zero or nonzero in any other column. In fact, it can be generalized for M-type COD as follows.

Lemma 5.1. *For M-type COD $\mathcal{O}_z[p, n, k]$, $\mathcal{O}_z(\alpha, i)$ and $\mathcal{O}_z(\beta, j)$ are the same, up to signs, implies that the zero pattern of row α and that of row β are different only at column i and column j; $\mathcal{O}_z(\alpha, i)$ and $\mathcal{O}_z(\beta, j)$ are conjugated, up to signs, implies that the zero pattern of row α and that of row β are the same only at column i and column j.*

Proof. Without loss of generality, assume $\mathcal{O}_z(\alpha, i) = z[1]$ and $\mathcal{O}_z(\beta, j) = z[1]$, where $z[1]$ represents an arbitrary element in $\{z_1, -z_1, z_1^*, -z_1^*\}$. Through some column permutation, say $\pi \in \Sigma_n$, where Σ_n is the set of all permutations on

$\{1, 2, \ldots, n\}$, we can transform $\mathcal{O}_z$ into $\mathcal{B}_1$ form, where

$$\begin{aligned}\mathcal{B}_1 &= \begin{pmatrix} z_1 I_{n_1} & \mathcal{M}_1 \\ -\mathcal{M}_1^H & z_1^* I_{n-n_1} \end{pmatrix} \\ &= \left(\begin{array}{cccc|cccc} z_1 & 0 & \cdots & 0 & & & & \\ 0 & z_1 & \cdots & 0 & & & & \\ \vdots & \vdots & \ddots & \vdots & & \mathcal{M}_1 & & \\ 0 & 0 & \cdots & z_1 & & & & \\ \hline & & & & z_1^* & 0 & \cdots & 0 \\ & -\mathcal{M}_1^H & & & 0 & z_1^* & \cdots & 0 \\ & & & & \vdots & \vdots & \ddots & \vdots \\ & & & & 0 & 0 & \cdots & z_1^* \end{array}\right), \end{aligned} \tag{9}$$

and $\mathcal{M}_1$ contains no zero entry.

When $|\mathcal{O}_z(\alpha, i)| = |\mathcal{O}_z(\beta, j)|$, we know row α and row β are both in the upper or lower part of $\mathcal{B}_1$ form. We can see that row α and row β have the same zero pattern except for column $\pi(i)$ and $\pi(j)$ after column permutation, which implies that row α and row β have the same zero pattern except for column $\pi^{-1}(\pi(i)) = i$ and $\pi^{-1}(\pi(j)) = j$ before column permutation.

When $|\mathcal{O}_z(\alpha, i)| = |\mathcal{O}_z(\beta, j)|^*$, we know row α and row β are in different parts (upper or lower) of $\mathcal{B}_1$ form. We can see that the zero patterns of row α and row β are all different except for column $\pi(i)$ and $\pi(j)$ after column permutation, which implies the zero patterns of row α and row β are all different except for column $\pi^{-1}(\pi(i)) = i$ and $\pi^{-1}(\pi(j)) = j$ before column permutation. □

The next lemma states that in an M-type COD, the existence of one zero pattern implies the existence of some other zero patterns, which will be used to prove the lower bound of decoding delay p for M-type COD.

Lemma 5.2. *Let $\mathcal{O}_z[p, n, k]$ be an M-type COD. If one zero pattern of some row is $\alpha \in \mathbb{F}_2^n$, then for any $1 \le i \ne j \le n$, there exists one row with zero pattern $\beta \in \mathbb{F}_2^n$, such that $\beta(i) = \alpha(j), \beta(j) = \alpha(i)$ and $\beta(l) = \alpha(l)$ for all $l \ne i, j$.*

Furthermore, for any $1 \le i \ne j \le n$ such that $\alpha(i) = \alpha(j) = 1$, there exists one row with zero pattern $\beta \in \mathbb{F}_2^n$, such that $\beta = \alpha \oplus e_i \oplus e_j \oplus e$.

Proof. **For the first part:** as when $\alpha(i) = \alpha(j)$, the conclusion is trivial, we assume $\alpha(i) = 1$ and $\alpha(j) = 0$. And, without loss of generality, assume the variable on that row in column i is $z[1]$. Through column permutation π satisfying $\pi(i) = 1, \pi(j) = 2$ and $\pi(\alpha) = (1, \underbrace{0, \ldots, 0}_{n-\mathrm{wt}(\alpha)}, 1, \ldots, 1)$, we can make this row the first row in $\mathcal{B}_1$ form.

Recall $\mathcal{B}_1$ form (9), we know the zero pattern of the second row is different from $\pi(\alpha)$ only in column 1 and 2, which implies that it's different from α only in column $\pi^{-1}(1) = i$ and $\pi^{-1}(2) = j$ before column permutation.

For the second part: Without loss of generality, assume the variable on that row in column i is $z[1]$. Through column permutation π such that $\pi(i) = 1, \pi(j) = n - \mathrm{wt}(\alpha) + 2$ and $\pi(\alpha) = (1, \underbrace{0, \ldots, 0}_{n-\mathrm{wt}(\alpha)}, 1, \ldots, 1)$, we can make this row the first row in $\mathcal{B}_1$ form after column permutation. Recall $\mathcal{B}_1$ form (9),

we know the zero pattern of the first row of the lower part is the same as $\pi(\alpha)$ only in column 1 and $n-\mathrm{wt}(\alpha)+2$, which implies that it's only the same as α in column $\pi^{-1}(1)=i$ and $\pi^{-1}(n-\mathrm{wt}(\alpha)+2)=j$ before column permutation. □

Next lemma gives an lower bound of the decoding delay p for M-type COD when n and the number of nonzero entries in some row are given.

Lemma 5.3. *Let $\mathcal{O}_z[p,n,k]$ be an M-type COD. If one row in $\mathcal{O}_z$ contains $w+1$ nonzero entries, then $p \geq \binom{n}{w-1}+\binom{n}{w+1}$ when $n \neq 2w$; and $p \geq \binom{n}{w-1}$ when $n=2w$.*

Furthermore, all zero patterns with weight $w+1$ or $n-w+1$ exists in $\mathcal{O}_z$.

Proof. According to the condition, assume that one row in $\mathcal{O}_z$ has zero pattern $\alpha \in \mathbb{F}_2^n$ such that $\mathrm{wt}(\alpha)=w+1$. Then for any zero pattern $\beta \in \mathbb{F}_2^n$ with $\mathrm{wt}(\beta)=w+1$, there exists a permutation $\pi \in \Sigma_n$ such that $\pi(\alpha)=\beta$. Since any permutation is a product of transpositions, then π can be written as the product of transpositions. According to Lemma 5.2, we claim there exists one row in $\mathcal{O}_z$ with zero pattern $\beta=\pi(\alpha)$.

Again, by Lemma 5.2, the existence of zero pattern α implies one row with zero pattern β such that $\mathrm{wt}(\beta)=n+2-\mathrm{wt}(\alpha)=n-w+1$. By similar arguments in the last paragraph, we claim all zero patterns with weight $n-w+1$ exist. When $w+1 \neq n-w+1 \Leftrightarrow n \neq 2w$, we know p is lower bounded by the number of all zero patterns with weight $w+1$ and $n-w+1$, i.e., $p \geq \binom{n}{w+1}+\binom{n}{n-w+1}$. When $w+1=n-w+1 \Leftrightarrow n=2w$, we know p is lower bounded by the number of all zero patterns with weight $w+1$, i.e., $p \geq \binom{n}{w+1}=\binom{n}{w-1}$. □

For M-type COD, besides the lower bound, we can say more about the decoding delay p, as the following lemma reveals.

Lemma 5.4. *Let $\mathcal{O}_z[p,n,k]$ be an atomic M-type COD. If one row in $\mathcal{O}_z$ contains $w+1$ nonzero entries, then p is a multiple of $\binom{n}{w-1}+\binom{n}{w+1}$ when $n \neq 2w$; and p is a multiple of $\binom{n}{w-1}$ when $n=2w$.*

Proof. At first, we will show, for an atomic M-type COD $\mathcal{O}_z[p,n,k]$, if one row contains $w+1$ nonzero entries, then each row contains $w+1$ or $n-w+1$ nonzero entries. Since $\mathcal{O}_z$ is atomic, then, for any pair of $1 \leq s \neq t \leq k$, there exists $j_1=s, j_2, \ldots, j_m=t$ such that $\mathcal{B}_{j_1}$ and $\mathcal{B}_{j_2}$ share some common rows, $\mathcal{B}_{j_2}$ and $\mathcal{B}_{j_3}$ share some common rows, ..., $\mathcal{B}_{j_{m-1}}$ and $\mathcal{B}_{j_m}$ share some common rows. Note that, in some $\mathcal{B}_j$ form of M-type COD, if one row contains $w+1$ nonzero entries, then all rows in $\mathcal{B}_j$ contains $w+1$ or $n-w+1$ nonzero entries. As s and t are taken arbitrarily, we claim every row of $\mathcal{O}_z[p,n,k]$ contains $w+1$ or $n-w+1$ nonzero entries.

Assume that zero pattern α appears with maximal times t, say, row $r_1, \ldots, r_t$ have zero pattern α. For any i satisfying $\alpha(i)=1$, there exists a column permutation π on $\mathcal{O}_z$ such that $\pi(i)=1$ and $\pi(\alpha)=(1,\underbrace{0,\ldots,0}_{n-w-1},1,\ldots,1)$. Therefore, r_i is in $\mathcal{B}_{j_i}$ form, where $z[j_i]$ appears in the first column of row r_i after column permutation π. Since $z[j_i]$ appears in the same column, $z[j_1], \ldots, z[j_t]$ are all different, and thus form $\mathcal{B}_{j_i}$ are mutually disjointed.

Now, we will show all zero patterns with weight $w+1$ exist t times. Recall $\mathcal{B}_j$ form (9), we claim there are t different rows with zero pattern β, where β is obtained by exchanging the value on i^{th} and j^{th} of α with any $\alpha(i) \oplus \alpha(j)=1$.

Since any permutation can be written as the product of transpositions, repeat this procedure, we know all zero patterns with weight $w+1$ exists at least t times. By the maximality of t, we claim all zero patterns with weight $w+1$ exists t times.

Finally, we will show all zero patterns with weight $n-w+1$ exist t times. For any $j, \alpha(j)=1$, recall $\mathcal{B}_j$ form (9), we claim there are t different rows with zero pattern $\beta = \alpha \oplus e_i \oplus e_j \oplus e$. Following similar argument of the above paragraph, we claim all zero patterns with weight $n-w+1$ exists t times.

Therefore, we have $p = t\left(\binom{n}{w-1} + \binom{n}{w+1}\right)$ when $n \neq 2w$; and $p = t\binom{n}{w-1}$ when $n = 2w$, where t is a positive integer. □

Next three lemmas are about the structure of COD $\mathcal{G}_n^w$ and $\mathcal{Q}_n^m$, and they will be used in the proof of Theorem 5.8.

Lemma 5.5. *For $\alpha \in \mathbb{F}_2^{n+1}, \alpha(n+1)=0$ and $1 \leq i \leq n$, $z[\alpha]$ is the variable with smallest index on row α_i of $\mathcal{G}_n$, where $\alpha_i = \alpha \oplus e_i \oplus \alpha(i)e$, if and only if*

$$\alpha(i) = \alpha(i+1) = \ldots = \alpha(n) = 0, \tag{10}$$

or

$$\alpha(1) = \alpha(2) = \ldots = \alpha(i) = 1. \tag{11}$$

Proof. By the definition of $\mathcal{G}_n^w$, we know that for all j satisfying $\alpha_i(j) = 1 \Leftrightarrow \alpha(i) \oplus \alpha(j) = 1$, $\mathcal{G}_n^w(\alpha_i, j) = z[\beta]$, where $\beta = \alpha_i \oplus e_j \oplus \alpha_i(n+1)e = \alpha \oplus e_i \oplus \alpha(i)e \oplus e_j \oplus \alpha(i)e = \alpha \oplus e_i \oplus e_j$.

Therefore, if $\alpha(i)=0$, for any $j, \alpha(j)=1$, $\alpha \oplus e_i \oplus e_j > \alpha$ if and only $j < i \Rightarrow \alpha(i) = \alpha(i+1) = \ldots = \alpha(n) = 0$; if $\alpha(i)=1$, for any $\alpha(j)=0$, $\alpha \oplus e_i \oplus e_j > \alpha$ if and only if $j > i \Rightarrow \alpha(1) = \alpha(2) = \ldots = \alpha(i) = 1$. The proof is complete. □

Lemma 5.6. *For $\alpha \in \mathbb{F}_2^{n+1}, \alpha(1) = \ldots = \alpha(s-1) = 1, \alpha(s) = 0, \alpha(t) = 1, \alpha(t+1) = \ldots = \alpha(n+1) = 0$ and $1 \leq s < t \leq n$, the smallest index of variables in $\mathcal{B}_\alpha$ form of $\mathcal{G}_n$ is $\alpha \oplus e_s \oplus e_t$.*

Proof. We prove it by calculating the indexes of all variables in $\mathcal{B}_\alpha$ form directly. By the definition of $\mathcal{G}_n$, we know $z[\alpha]$ is in $\mathcal{G}_n(\alpha_i, i), i = 1, 2, \ldots, n$, where $\alpha_i = \alpha \oplus e_i \oplus \alpha(i)e$. For $\alpha_i(j) = 1 \Leftrightarrow \alpha(i) \oplus \alpha(j) = 1$, $\mathcal{G}_n(\alpha_i, j) = z[\beta]$, where $\beta = \alpha_i \oplus e_j \oplus \alpha_i(n+1)e = \alpha \oplus e_i \oplus \alpha(i)e \oplus e_j \oplus \alpha(i)e = \alpha \oplus e_i \oplus e_j$.

For what i, j satisfying $\alpha(i) \oplus \alpha(j) = 1$, value $\alpha \oplus e_i \oplus e_j$ reaches the minimal? Without loss of generality, assume $\alpha(i) = 0$ and $\alpha(j) = 1$. It's easy to see that i should be as small as possible and j should be as big as possible. Therefore, $i = s$ and $j = t$, and $\alpha \oplus e_s \oplus e_t$ is the smallest index of variables in $\mathcal{B}_\alpha$ form of $\mathcal{G}_n$. □

Lemma 5.7. *For $n = 2m$ or $2m-1$, CODs $\mathcal{G}_n^w$, $-1 \leq w \leq n+1$, are all atomic. And when $n = 2m$, m even, COD $\mathcal{Q}_n^m$ is atomic.*

Proof. If $n \neq 2w$, $\mathcal{G}_n^w$ has parameter $[\binom{n}{w-1} + \binom{n}{w+1}, n, \binom{n}{w}]$. By Lemma 5.3, we know p is minimal, and therefore $\mathcal{G}_n^w$ is atomic. It's similar to prove $\mathcal{Q}_n^m$ is atomic, for $n = 2m$, m even.

For $n = 2m$, COD $\mathcal{G}_n^m$, assume that there is an atomic COD $\mathcal{O}_z$ consisting of some rows of $\mathcal{G}_n^m$. Take one $\alpha \in \mathbb{F}_2^{n+1}$, $\mathrm{wt}(\alpha) = m+1$ and $\alpha(n+1) = 0$, such that

$z[\alpha]$ appears in $\mathcal{O}_z$. By the definition of $\mathcal{G}_n^m$, $z[\alpha]$ appears in $\mathcal{G}_n^m(\alpha_i, i)$, where $\alpha_i = \alpha \oplus e_i \oplus \alpha(i)e$. For any j, satisfying $\alpha_i(j) = 1 \Leftrightarrow \alpha(i) \oplus \alpha(j) = 1$, $\mathcal{G}_n^m(\alpha_i, j)$ contains the variable with index $\alpha_i \oplus e_j \oplus \alpha_i(n+1)e = \alpha \oplus e_i \oplus \alpha(i)e \oplus e_j \oplus \alpha(i)e = \alpha \oplus e_i \oplus e_j$. Thus $z[\alpha \oplus e_i \oplus e_j]$ should exist in $\mathcal{O}_z$. Since i and j are taken arbitrary if $\alpha(i) \oplus \alpha(j) = 1$ is satisfied, by repeating this procedure, we claim all variables with index weight $\mathrm{wt}(\alpha) = m + 1$ appears in $\mathcal{O}_z$. Therefore $\mathcal{O}_z = \mathcal{G}_n^m$, and the proof is complete. □

The next theorem is our main result, which determines the parameters as well as the structures of most atomic M-type CODs.

Theorem 5.8. *Let $\mathcal{O}_z[p, n, k]$ be an atomic COD, with some row containing $w + 1$ nonzero entries, and $n \neq 2w$. Then, $[p, n, k] = [\binom{n}{w-1} + \binom{n}{w+1}, n, \binom{n}{w}]$ and $\mathcal{O}_z$ is the same as $\mathcal{G}_n^w$ under equivalence operation.*

Proof. We first present an example to illustrate our proof idea. For some atomic COD $\mathcal{O}_z$, with $n = 3$ and $w = 2$, we will show how to prove it is the same as

$$\mathcal{G}_3^2 = \begin{pmatrix} -z_{(0,1,1)} & z_{(1,0,1)} & z_{(1,1,0)} \\ -z^*_{(1,0,1)} & -z^*_{(0,1,1)} & 0 \\ -z^*_{(1,1,0)} & 0 & -z^*_{(0,1,1)} \\ 0 & z^*_{(1,1,0)} & -z^*_{(1,0,1)} \end{pmatrix}.$$

For convenience, we denote $z_{(1,1,0)}$ by z_1, $z_{(1,0,1)}$ by z_2, $z_{(0,1,1)}$ by z_3.

Since $w = 2$, there is at least one row of $\mathcal{O}_z$ which contains 3 nonzero entries. Without loss of generality, we denote it by

$$\begin{pmatrix} -z_3 & z_2 & z_1 \end{pmatrix}.$$

It can be achieved by instance renaming, instance conjugation and instance negation.

Recalling $\mathcal{B}_1$ form, we claim there exists one row of $\mathcal{O}_z$ matches $(\pm z_1^*, 0, \bigstar)$. At first, we can use row negation to make sure $\pm z_1^*$ takes the same sign as that of $\mathcal{G}_n^w$, which is "$-$". By orthogonality, the first row shares an Alamouti 2×2 with this row, which is $\begin{pmatrix} -z_3 & z_1 \\ -z_1^* & \bigstar \end{pmatrix}$. Thus, $\bigstar$ should be $-z_3^*$. Now we have determined two rows of $\mathcal{O}_z$ as follows

$$\begin{pmatrix} -z_3 & z_2 & z_1 \\ -z_1^* & 0 & -z_3^* \end{pmatrix}.$$

Recalling $\mathcal{B}_1$ form again, there must exist one row of $\mathcal{O}_z$ matches $(0, \pm z_1^*, \bigstar)$. At first, we can use row negation to make sure $\pm z_1^*$ takes the same sign as that of $\mathcal{G}_n^w$, which is "$+$". By orthogonality, the first row shares an Alamouti 2×2 with this row, which is $\begin{pmatrix} z_2 & z_1 \\ z_1^* & \bigstar \end{pmatrix}$. Thus, $\bigstar$ should be $-z_2^*$. Now, we have determined three rows of $\mathcal{O}_z$ as follows

$$\begin{pmatrix} -z_3 & z_2 & z_1 \\ -z_1^* & 0 & -z_3^* \\ 0 & z_1^* & -z_2^* \end{pmatrix}.$$

Recalling $\mathcal{B}_2$ form, there must exist one row of $\mathcal{O}_z$ matches $(\pm z_2^*, \bigstar, 0)$. At first, we can use row negation to make sure $\pm z_1^*$ takes the same sign as that of

$\mathcal{G}_n^w$, which is "$-$". By orthogonality, the first row shares an Alamouti 2×2 with this row, which is $\begin{pmatrix} -z_3 & z_2 \\ -z_2^* & \bigstar \end{pmatrix}$, which implies $\bigstar$ should be $-z_3^*$. Now, we have

$$\begin{pmatrix} -z_3 & z_2 & z_1 \\ -z_1^* & 0 & -z_3^* \\ 0 & z_1^* & -z_2^* \\ -z_2^* & -z_3^* & 0 \end{pmatrix},$$

which is already a COD. Since $\mathcal{O}_z$ is atomic, we claim $[p,n,k]=[4,3,3]$ and it is the same as $\mathcal{G}_3^2$ under equivalence operation.

Applying the above method, for a general $\mathcal{O}_z[p,n,k]$ with some row containing $w+1$ nonzero entries, $n\neq 2w$, we will prove that, using equivalence operation, we can transform $\mathcal{O}_z$ to $\mathcal{G}_n^w$ row by row in a specific order.

We reorder the rows in $\mathcal{G}_n^w$ first by order of the smallest index of the variables on that row in increasing, then by the order of the row index in increasing. We will use induction to prove that, $\mathcal{O}_z$ is the same as $\mathcal{G}_n^w$ under equivalence operation, and the induction parameter is the reordered rows of $\mathcal{G}_n^w$.

Induction basis: For the first row of $\mathcal{G}_n^w$, say row $\beta\in\mathbb{F}_2^{n+1}$. In $\mathcal{G}_n^w$, find one row with the zero pattern $(\beta(1),\beta(2),\ldots,\beta(n))$. Note that Lemma 5.3 guarantees the existence of this row. Since all variables exist for the first time, we can use instance renaming, instance conjugation and instance negation to make this row the same as the corresponding row of $\mathcal{G}_n^w$.

Induction step: For variable index $\beta\in\mathbb{F}_2^{n+1}, \beta(n+1)=0$ and row $\beta_i\Rightarrow \mathcal{G}_n^w(\beta_i,i)=z[\beta]$, where $\beta_i=\beta\oplus e_i\oplus\beta(i)e$. Assume that there exists an equivalence operation on $\mathcal{O}_z$ such that some rows of $\mathcal{O}_z$ are the same as rows of $\mathcal{G}_n^w$ which either has the smallest index less than β or the smallest index β and its row index less than β, we will show it is true after row β_i in $\mathcal{G}_n^w$ is added.

We claim $z[\beta]$ already exists in former induction steps. Otherwise, β should have the smallest index of all variables, and Lemma 5.6 implies β is unique and thus already appears on the first row in the induction step. Therefore, by Lemma 5.3, we know that there exists one row of $\mathcal{O}_z$ having the same zero pattern as row β_i of $\mathcal{G}_n^w$ with the corresponding position occupied $z[\beta]$. Since $z[\beta]$ already exists, whether $z[\beta]$ takes conjugation is already determined by the zero pattern $(\beta_i(1),\beta_i(2),\ldots,\beta_i(n))$. Thus, we can use row negation to make sure $z[\beta]$ takes the same sign the same as $\mathcal{G}_n^w(\beta_i,i)$. We will show that for all the other nonzero entries on this row of $\mathcal{O}_z$,

- either the variable exists for the first time, which implies we can use instance renaming, instance conjugation and instance negation to make it the same as the corresponding one in $\mathcal{G}_n^w$,
- or it's uniquely determined, including sign and conjugation, by the orthogonality of $\mathcal{O}_z$.

For any $j\neq i, \beta_i(j)=1\Leftrightarrow \beta(i)\oplus\beta(j)=1$, let's consider the entry on β_i^{th} row and j^{th} column of $\mathcal{O}_z$. By assumption that $z[\beta]$ is the smallest-index variable in row β_i, we know from Lemma 5.5, either

$$\beta(i)=\beta(i+1)=\ldots=\beta(n)=0, \tag{12}$$

or

$$\beta(1) = \beta(2) = \ldots = \beta(i) = 1 \tag{13}$$

holds. We will discuss it in the following four cases separately.

Case 1: $\beta(i) = \beta(i+1) = \ldots = \beta(n) = 0, \beta(j) = 1$ **and** $\beta(l) = 0$ **for some** $1 \leq l < j$**.** Let $\mathcal{G}_n^w(\beta_j, l) = z[\gamma]$, where $\beta_j = \beta \oplus e_j \oplus e$. We have

$$\begin{aligned} \gamma &= \beta_j \oplus e_l \oplus \beta_j(n+1)e \\ &= \beta \oplus e_j \oplus e \oplus e_l \oplus e \\ &= \beta \oplus e_j \oplus e_l. \end{aligned}$$

Since $\beta(l) = 0, \beta(j) = 1$ and $l < j$, we have $\gamma < \beta$, which implies row β_j is already determined. By the orthogonality of $\mathcal{O}_z$, submatrix

$$\mathcal{O}_z(\beta_i, \beta_j; i, j) = \begin{pmatrix} z[\beta] & \bigstar \\ z[\gamma] & z[\beta] \end{pmatrix}$$

should be an Alamouti 2×2. Thus $\bigstar$ should be $z[\gamma]$ and its conjugation and sign are uniquely determined by the other three entries.

Case 2: $\beta(i) = \beta(i+1) = \ldots = \beta(n) = 0$ **and** $\beta(1) = \beta(2) = \ldots = \beta(j) = 1$**.** Let $\mathcal{G}_n^w(\beta_i, j) = z[\gamma]$, where $\beta_i = \beta \oplus e_i$. Thus $\gamma = \beta_i \oplus e_j \oplus \beta_i(n+1) = \beta \oplus e_i \oplus e_j$.

To prove $z[\gamma]$ exists for the first time, it's sufficient to show that there are determined rows with no zero pattern matches one in $\mathcal{B}_\gamma$ form. By Lemma 5.6, we know that $z[\beta]$ is the smallest index variable in B_γ form of $\mathcal{G}_n^w$, adding the fact that $\beta_j = \beta \oplus e_j \oplus e > \beta_i$, which implies that $z[\gamma]$ exists for the first time. Therefore, we can use instance renaming, instance conjugation and instance negation to make $\mathcal{O}_z(\alpha_i, j)$ the same as $\mathcal{G}_n^w(\alpha_i, j)$.

Case 3: $\beta(1) = \beta(2) = \ldots = \beta(i) = 1, \beta(j) = 0$ **and** $\beta(l) = 1$ **for some** $l > j$**.** Let $\mathcal{G}_n^w(\beta_j, l) = z[\gamma]$, where $\beta_j = \beta \oplus e_j$. We have $\gamma = \beta_j \oplus e_l \oplus \beta_j(n+1)e = \beta \oplus e_j \oplus e_l$. Since $\beta(l) = 1, \beta(j) = 0$ and $l > j$, we have $\gamma < \beta$, which implies row β_j is already determined. Following the same argument in **Case 1**, we know $\mathcal{O}_z(\beta_j, j)$ is uniquely determined.

Case 4: $\beta(1) = \beta(2) = \ldots = \beta(i) = 1, \beta(j) = 0$ **and** $\beta(j) = \beta(j+1) = \ldots = \beta(n) = 0$**.** Let $\mathcal{G}_n^w(\beta_j, j) = z[\gamma]$, where $\beta_j = \beta \oplus e_j$. We have $\gamma = \beta_j \oplus e_j \oplus \beta_j(n+1)e = \beta \oplus e_j \oplus e_j = \beta$. Note that $\beta_j = \beta \oplus e_j$ and $\beta_i = \beta \oplus e_i \oplus e$, which implies $\beta_j < \beta_i$. Therefore, row β_j in $\mathcal{O}_z$ is determined. Following the same argument in **Case 1**, we know element in $\mathcal{O}_z(\beta_i, j)$ is uniquely determined. □

It is worth noting that the equivalence operations used in transform $\mathcal{O}_z$ to $\mathcal{G}_n^w$ does not contain column negations. This property will be used in the sequel.

Theorem 5.8 does not consider the case when $n = 2w$. To cover the final case, we need the following lemma first, which states when $n \equiv 2 \pmod 4$, COD with parameter $[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$ does not exist. It should be noticed that this result is first proved in [6]. However, based on our explicit construction, we present a different proof here.

Lemma 5.9. *When $n = 2m$, m odd, there does not exist COD with parameter $[p, n, k] = [\binom{n}{m-1}, n, \binom{n-1}{m-1}]$.*

Proof. Assume to the contrary that there exists COD $\mathcal{O}_z[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$. By deleting the last column of $\mathcal{O}_z$, we obtain a COD with parameter $[\binom{n}{m-1}, n-1, \binom{n-1}{m-1}]$. By Theorem 5.8, it is equivalent to $\mathcal{G}^m_{n-1}$. Thus, by padding a column $\mathcal{H}$ to $\mathcal{G}^m_{n-1}$, we can obtain a COD with parameter $[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$. Now, we will show it is impossible.

By Lemma 5.3, we know the zero pattern of $\mathcal{O}_z$ is unique. By Lemma 5.1, we know which variable should be in $\mathcal{H}(\alpha)$ is uniquely determined by the zero pattern of this row. Set $\mathcal{H}(\alpha) = \alpha(n+1)\phi(\alpha)z_{\alpha\oplus e_n}$, where $\phi(\alpha) \in \{-1, 1\}$. It is easy to verify that, for arbitrary $1 \le i \le n-1$, $\mathcal{O}_z(\alpha, i)$ and $\mathcal{H}(\alpha)$ are contained in the following Alamouti

$$\begin{pmatrix} (-1)^{\theta(\alpha,i)} z^*_{\varphi(\alpha,i)} & \phi(\alpha) z_{\alpha\oplus e_n} \\ (-1)^{\theta(\beta,i)} z^*_{\varphi(\beta,i)} & \phi(\beta) z_{\beta\oplus e_n}, \end{pmatrix}$$

where $\alpha \oplus \beta = e \oplus e_i \oplus e_n$. A direct computation will verify $\varphi(\alpha, i) = \beta \oplus e_n$ and $\varphi(\beta, i) = \alpha \oplus e_n$. Thus, setting $\mathcal{H}(\alpha) = \alpha(n+1)\phi(\alpha)z_{\alpha\oplus e_n}$ is valid.

Calculating $\theta(\alpha, i) + \theta(\beta, i)$ by definition, we know that when i is odd, $\theta(\alpha, i) + \theta(\beta, i) \equiv 0 \pmod 2$; when i is even, $\theta(\alpha, i) + \theta(\beta, i) \equiv 1 \pmod 2$. Therefore, when i is odd, we have $\phi(\alpha) = -\phi(\alpha \oplus e_i \oplus e_n)$; when i is even, we have $\phi(\alpha) = \phi(\alpha \oplus e_i \oplus e_n)$. Next, we will show a contradiction by calculating the relationship between $\phi(\underbrace{0, 0, \ldots, 0}_{m-1}, \underbrace{1, 1, \ldots, 1}_{m}, 0)$ and $\phi(1, 0, \ldots, 1, 0)$ in two ways.

Way 1: Let $\alpha = \bigoplus_{i=m}^{2m-1} e_i = (\underbrace{0, 0, \ldots, 0}_{m-1}, \underbrace{1, 1, \ldots, 1}_{m}, 0)$ initially. And let $i = 2m-2l+1, l = 1, 2, \ldots, \frac{m+1}{2}$ and $i = 2l, l = 1, 2, \ldots, \frac{m-1}{2}$. Finally, we obtain the relationship between $\phi(\alpha)$ and $\phi(\alpha \bigoplus_{i=1}^{\frac{m-1}{2}} (e_{2l} \oplus e_{2m-2l+1}) \oplus e_m \oplus e \oplus e_n) = \phi(\bigoplus_{i=1}^{m} e_{2l-1}) = \phi(1, 0, 1, 0, \ldots, 0, 1)$. Since $\phi(\alpha) = -\phi(\alpha \oplus e_i \oplus e)$ if and only if i is odd, we claim

$$\phi(\underbrace{0, 0, \ldots, 0}_{m-1}, \underbrace{1, 1, \ldots, 1}_{m}, 0) = (-1)^{\frac{m+1}{2}} \phi(1, 0, \ldots, 1, 0). \tag{14}$$

Way 2: Let $\alpha = \bigoplus_{i=m}^{2m} e_i = (\underbrace{0, 0, \ldots, 0}_{m-1}, \underbrace{1, 1, \ldots, 1}_{m}, 0)$ initially. And let $i = 2m-2l, l = 1, 2, \ldots, \frac{m-1}{2}$ and $i = 2l-1, l = 1, 2, \ldots, \frac{m-1}{2}$. Finally, we obtain the relationship between $\phi(\alpha)$ and $\phi(\alpha \bigoplus_{i=1}^{\frac{m-1}{2}} (e_{2l-1} \oplus e_{2m-2l})) = \phi(1, 0, \ldots, 1, 0)$. Since $\phi(\alpha) = -\phi(\alpha \oplus e_i \oplus e)$ if and only if i is odd, we claim

$$\phi(\underbrace{0, 0, \ldots, 0}_{m-1}, \underbrace{1, 1, \ldots, 1}_{m}, 0) = (-1)^{\frac{m-1}{2}} \phi(1, 0, \ldots, 1, 0), \tag{15}$$

which is contradicted with (14)!

Therefore, it's impossible to pad an extra column to $\mathcal{G}^m_{2m-1}$ to obtain a $[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$ a COD, and thus COD with parameter $[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$ does not exist. □

Now, we are ready to prove the final case. Along with Theorem 5.8, we have determined the parameters and structures of all atomic CODs.

Theorem 5.10. *When $n = 2m$, let $\mathcal{O}_z[p, n, k]$ be an atomic COD with some row containing $m + 1$ nonzero entries. Then $[p, n, k] = [\binom{n}{m-1}, n, \binom{n-1}{m-1}]$ or $[2\binom{n}{m-1}, n, 2\binom{n-1}{m-1}]$.*

When $[p, n, k] = [2\binom{n}{m-1}, n, 2\binom{n-1}{m-1}]$, $\mathcal{O}_z$ is the same as $\mathcal{G}_{2m}^m$ under equivalence operation. When $[p, n, k] = [\binom{n}{m-1}, n, \binom{n-1}{m-1}]$, $\mathcal{O}_z$ is the same as $\mathcal{Q}_{2m}^m$ under equivalence operation and m is even.

Proof. By deleting the last column of $\mathcal{O}_z[p, n, k]$, we obtain a COD, say $\mathcal{O}'_z$, with parameter $[p, n-1, k]$. By Theorem 5.8 and the fact that no column negation is used, we know $\mathcal{O}'_z$ is the same as the catenation of t CODs $\mathcal{G}_{n-1}^m$ under equivalence operation, which are denoted by $\mathcal{O}_z^{(1)}, \mathcal{O}_z^{(2)}, \ldots, \mathcal{O}_z^{(t)}$. And we denote the last column by by $\mathcal{H}_z^{(1)}, \mathcal{H}_z^{(2)}, \ldots, \mathcal{H}_z^{(t)}$, where $\mathcal{H}_z^{(i)}$ and $\mathcal{O}_z^{(i)}$ are in the same rows of $\mathcal{O}_z$. For the convenience of description, we denote the row of $\mathcal{O}_z$ by $\alpha^{(i)} \in \mathbb{F}_2^n$, and denote the variable index of $\mathcal{O}_z$ by $\beta^{(i)} \in \mathbb{F}_2^n, i = 1, 2, \ldots, t$.

Let's consider padding the last column. For some variable $\beta^{(1)}$, recalling Lemma 5.1 and the fact that zero patterns of $\mathcal{G}_n^w$ do not repeat, we know that it might be in row $\alpha^{(i)}$ of $\mathcal{O}_z$ for some $1 \le i \le t$ and α is uniquely determined.

If $\mathcal{O}_z(\alpha^{(1)}, n) = z[\beta^{(1)}]$, then $z[\beta^{(1)}]$ and other variables $z[\gamma^{(1)}]$ on this row should be in an Alamouti 2×2, which implies those $z[\gamma^{(1)}]$ are in $\mathcal{H}_z^{(1)}$. Repeating this procedure, we can prove all variables in $\mathcal{O}_z^{(1)}$ are in $\mathcal{H}_z^{(1)}$, because $\mathcal{O}_z^{(1)}$ is atomic. Therefore, $(\mathcal{O}_z^{(1)}, \mathcal{H}_z^{(1)})$ is a COD. Since $\mathcal{O}_z$ is atomic, we claim $t = 1$. By Lemma 5.9, we know m is even. Since the above procedure indicates the last column is uniquely determined, we claim atomic COD with parameter $[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$ is unique under equivalence operation, which implies $\mathcal{O}_z$ is equivalent to $\mathcal{Q}_{2m}^m$.

If $\mathcal{O}_z(\alpha^{(1)}, n) = z[\beta^{(i)}]$ for some $2 \le i \le t$, without loss of generality, letting $i = 2$, then $z[\beta^{(2)}]$ and other variable $z[\gamma^{(1)}]$ on this row should be in an Alamouti 2×2, which implies that those $z[\gamma^{(1)}]$ are in $\mathcal{H}_z^{(2)}$. Repeating this procedure, we can prove all variables in $\mathcal{O}_z^{(1)}$ appear in $\mathcal{H}_z^{(2)}$ and all variables in $\mathcal{O}_z^{(2)}$ appear in $\mathcal{H}_z^{(1)}$, because both $\mathcal{O}_z^{(1)}$ and $\mathcal{O}_z^{(2)}$ are atomic. Therefore,

$$\begin{pmatrix} \mathcal{O}_z^{(1)} & \mathcal{H}_z^{(1)} \\ \mathcal{O}_z^{(2)} & \mathcal{H}_z^{(2)} \end{pmatrix}$$

is a COD. Since $\mathcal{O}_z$ is atomic, we claim $t = 2$. From the above procedure, we know $\mathcal{H}_z^{(1)}$ and $\mathcal{H}_z^{(2)}$ are uniquely determined. Therefore, atomic COD with parameter $[2\binom{n}{m-1}, n, 2\binom{n-1}{m-1}]$ is unique under equivalence operation, which implies $\mathcal{O}_z$ is equivalent to $\mathcal{G}_{2m}^m$. □

6 Conclusion

Theorem 6.1. *Given positive integers p, n, k, M-type COD $\mathcal{O}_z[p, n, k]$ exists if and only if there exist nonnegative integers $t_{-1}, t_0, \ldots, t_{\lceil \frac{n}{2} \rceil}$ such that*

$$p = \sum_{i=-1}^{\lceil \frac{n}{2} \rceil} t_i \left(\binom{n}{i-1} + \binom{n}{i+1} \right) \text{ and } k = \sum_{i=-1}^{\lceil \frac{n}{2} \rceil} t_i \binom{n}{i},$$

when $n \equiv 1, 2, 3 \pmod 4$,

$$p = \sum_{i=-1}^{\frac{n}{2}-1} t_i \left(\binom{n}{i-1} + \binom{n}{i+1} \right) + t_{\frac{n}{2}} \binom{n}{\frac{n}{2}-1}$$

and

$$k = \sum_{i=-1}^{\frac{n}{2}-1} t_i \binom{n-1}{i-1} + t_{\frac{n}{2}} \binom{n-1}{\frac{n}{2}-1},$$

when $n \equiv 0 \pmod 4$.

Proof. **For the "if" direction:** When $n \equiv 1, 2, 3 \pmod 4$, assume that

$$p = \sum_{i=-1}^{\lceil \frac{n}{2} \rceil} t_i \left(\binom{n}{i-1} + \binom{n}{i+1} \right) \text{ and } k = \sum_{i=-1}^{\lceil \frac{n}{2} \rceil} t_i \binom{n}{i}.$$

We can construct a COD achieving parameter $[p, n, k]$ by simply catenating t_i atomic CODs $\mathcal{G}_n^i[\binom{n}{i-1} + \binom{n}{i+1}, n, \binom{n}{i}]$, $i = -1, 0, \ldots, \lceil \frac{n}{2} \rceil$.

When $n \equiv 0 \pmod 4$, assume that

$$p = \sum_{i=-1}^{\frac{n}{2}-1} t_i \left(\binom{n}{i-1} + \binom{n}{i+1} \right) + t_{\frac{n}{2}} \binom{n}{\frac{n}{2}-1}$$

and

$$k = \sum_{i=-1}^{\frac{n}{2}-1} t_i \binom{n-1}{i-1} + t_{\frac{n}{2}} \binom{n-1}{\frac{n}{2}-1}.$$

We can construct a COD achieving parameter $[p, n, k]$ by simply catenating t_i atomic CODs $\mathcal{G}_n^i[\binom{n}{i-1} + \binom{n}{i+1}, n, \binom{n}{i}]$, $i = -1, 0, \ldots, \frac{n}{2} - 1$, and $t_{\frac{n}{2}}$ atomic CODs $\mathcal{Q}_n^{n/2}[\binom{n}{\frac{n}{2}-1}, n, \binom{n-1}{\frac{n}{2}-1}]$.

For the "only if" direction: Decompose COD $\mathcal{O}_z$ into atomic ones. By Theorem 5.8 and Theorem 5.10, we know that all atomic CODs have parameter $[\binom{n}{i-1} + \binom{n}{i+1}, n, \binom{n}{i}]$ for $i = -1, 0, \ldots, \lceil \frac{n}{2} \rceil$, or $[\binom{n}{n/2-1}, n, \binom{n-1}{n/2-1}]$ when $n \equiv 0 \pmod 4$.

Say, when $n \not\equiv 0 \pmod 4$, there are t_i atomic CODs with parameter $[\binom{n}{i-1} + \binom{n}{i+1}, n, \binom{n}{i}]$, $i = -1, 0, \ldots, \lceil \frac{n}{2} \rceil$. When $n \equiv 0 \pmod 4$, there are there are t_i atomic CODs have parameter $[\binom{n}{i-1} + \binom{n}{i+1}, n, \binom{n}{i}]$, $i = -1, 0, \ldots, n/2 - 1$, $t''_{n/2}$ atomic CODS with parameter $[2\binom{n}{n/2-1}, n, 2\binom{n-1}{n/2-1}]$ and $t'_{n/2}$ atomic CODs with parameter $[\binom{n}{n/2-1}, n, \binom{n-1}{n/2-1}]$. Finally, let $t_{n/2} = 2t''_{n/2} + t'_{n/2}$. The proof is complete. □

The following corollary characterizes all possible structures of M-type COD, which has similar proof with Theorem 6.1. And thus the proof is omitted.

Corollary 6.2. *Let $\mathcal{O}_z[p, n, k]$ be an M-type COD. Then $\mathcal{O}_z$ is equivalent to the catenation of t_i times $\mathcal{G}_n^i$, $i = -1, 0, \ldots, \lceil \frac{n}{2} \rceil$, for some $t_{-1}, t_0, \ldots, t_{\lceil \frac{n}{2} \rceil}$ satisfying*

$$p = \sum_{i=-1}^{\lceil \frac{n}{2} \rceil} t_i \left(\binom{n}{i-1} + \binom{n}{i+1} \right)$$

and

$$k = \sum_{i=-1}^{\lceil \frac{n}{2} \rceil} t_i \binom{n}{i},$$

when $n \equiv 1, 2, 3 \pmod 4$*;* $\mathcal{O}_z$ *is equivalent to the catenation of* t_i *times* $\mathcal{G}_n^i$*,* $i = -1, 0, \ldots, \frac{n}{2}$ *and* $t'_{\frac{n}{2}}$ *times* $\mathcal{Q}_n^m$*, for some* $t_{-1}, t_0, \ldots, t_{\frac{n}{2}}$ *and* $t'_{\frac{n}{2}}$ *satisfying*

$$p = \sum_{i=-1}^{\frac{n}{2}} t_i \left(\binom{n}{i-1} + \binom{n}{i+1} \right) + t'_{\frac{n}{2}} \binom{n}{\frac{n}{2}-1}$$

and

$$k = \sum_{i=-1}^{\frac{n}{2}} t_i \binom{n-1}{i-1} + t'_{\frac{n}{2}} \binom{n-1}{\frac{n}{2}-1},$$

when $n \equiv 0 \pmod 4$*.*

Since all optimal CODs, which achieves both the maximal rate and minimal delay, have parameters $[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$ when $n \equiv 0, 1, 3 \pmod 4$; have parameter $[\binom{n}{m-1}, n, \binom{n-1}{m-1}]$ when $n \equiv 2 \pmod 4$. And they are proved to be in M-type. We can obtain the following corollary directly.

Corollary 6.3. *Let* $n = 2m$ *or* $2m-1$*. When* $n \equiv 1, 2, 3 \pmod 4$*, all maximal-rate, minimal-delay CODs are the same as* $\mathcal{G}_n^m$ *under equivalence operation; when* $n \equiv 0 \pmod 4$*, all maximal-rate, minimal-delay CODs are the same as* $\mathcal{Q}_n^m$ *under equivalence operation.*

The uniqueness under equivalence operation of optimal COD for $n \equiv 0, 1, 3 \pmod 4$ is already proved in [3] by showing that all such CODs with optimal parameters can be transformed in to a standard form. The uniqueness for the case $n \equiv 2 \pmod 4$ is proved for the first time.

In [4], three facts are proved

1) For $n = 2m-1$, let $\mathcal{O}_z$ be a maximal rate, minimal delay COD. Then, $\mathcal{O}_z$ is equivalent to a COD that is conjugation-separated.

2) For $n = 2m$, let $\mathcal{O}_z$ be a maximal rate COD with decoding delay $\binom{2m}{m-1}$. Then no arrangement of $\mathcal{O}_z$ is conjugation-separated.

3) It is possible to construct a maximum rate COD with any even number of columns that simultaneously achieves conjugation-separation and decoding delay $2\binom{2m}{m-1}$.

By Theorem 5.8, a $[\binom{2m}{m-1}, 2m-1, \binom{2m-1}{m-1}]$ COD is equivalent to $\mathcal{G}_n^m$, which conjugation-separated. Thus, 1) is true. By Theorem 5.10, we know COD $\mathcal{O}_z[\binom{2m}{m-1}, 2m, \binom{2m-1}{m-1}]$ is equivalent to $\mathcal{Q}_n^m$. Therefore, to prove 2), it's sufficient to show $\mathcal{Q}_n^m$ isn't equivalent to a conjugation-separated COD. By the constructions of $\mathcal{G}_n^m$, 3) is true.

7 Acknowledgment

We are immensely grateful to Chen Yuan for deciding the signs in Theorem 4.1.

References

[1] J. F. Adams, "Vector fields on spheres," Ann. Math., vol. 75, no. 2, pp. 603-632, 1962.

[2] J. F. Adams, P. D. Lax, and R. S. Phillips, "On matrices whose real linear combinations are nonsingular," in Proc. Amer. Math. Soc., vol. 16, 1965, pp. 318-322.

[3] S. S. Adams, J. Davis, N. Karst, M. K. Murugan, B. Lee, M. Crawford, C. Greeley, "Novel classes of minimal delay and low PAPR rate 1/2 complex orthogonal designs," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 2254-2262, Apr. 2011.

[4] S. S. Adams, N. Karst, M. K. Murugan and T. A. Wysocki, "On transceiver signal linearization and the decoding delay of maximum rate complex orthogonal space-time block codes," IEEE Trans. Inf. Theory, vol. 57, no. 6, pp. 3618-3621, Jun. 2011.

[5] S. S. Adams, N. Karst, and J. Pollack, "The minimum decoding delay of maximum rate complex orthogonal space-time block codes," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2677-2684, Aug. 2007.

[6] S. S. Adams, N. Karst, M. K. Murugan., "The final case of the decoding delay problem for maximum rate complex orthogonal designs," IEEE Trans. Inf. Theory, vol. 56, no. 1, pp. 103-122, Jan. 2010.

[7] S. Alamouti, "A simple transmit diversity technique for wireless communications," IEEE J. Select. Areas Commun., vol. 16, pp. 1451-1458, Oct. 1998.

[8] A. V. Geramite and N. J. Pullman, "Orthogonal Designs: Quadratic Forms and Hadamard Matrices (Lecture Notes in Pure and Applied Mathematics)," New York: Marcel Dekker, vol. 43, 1979.

[9] R. L. Graham, D. E. Knuth and O. Patashnik, "Concrete Mathematics: A Foundation for Computer Science," 2nd Edition, Pearson Education, 1994.

[10] R. A. Horn and C. R. Johnson, "Topics in Matrix Analysis," Cambridge, U.K.: Cambridge Univ. Press, 1991.

[11] M. Z. A. Khan, B. S. Rajan, "A generalization of some existence results on orthogonal designs for STBCs," IEEE Trans. Inf. Theory, vol. 50, no. 1, Jan. 2004.

[12] H. Kan and H. Shen, "A counterexample for the open problem on the minimal delays of orthogonal designs with maximal rates," IEEE Trans. Inf. Theory, vol. 51, no. 1, pp. 355-359, Jan. 2005.

[13] H. Kan and H. Shen, "Lower bounds on the minimal delay of complex orthogonal designs with maximal rats," IEEE Trans. Commun., vol. 54, no. 3, pp. 383-388, Mar. 2006.

[14] X-B. Liang, "Orthogonal designs with maximal rates," IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2468-2503, Oct. 2003.

[15] X-B. Liang, and X-G Xia, "On the nonexistence of rate-one generalized complex orthogonal designs," IEEE Trans. Inf. Theory, vol.49, no.11, pp.2984-2989, Nov. 2003.

[16] Y. Li, H. Kan, C. Yuan and H. Ma, "The maximal rates and minimal decoding delay of more general complex orthogonal designs," Science in China, Series F: Information Sciences 2010, pp. 1826-1832.

[17] K. Lu, S. Fu, and X. G. Xia, "Closed-form designs of complex orthogonal space-time block codes of rates (k+1)/(2k) for 2k-1 or 2k transmit antennas," IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4340-4347, Dec. 2005.

[18] S. K. Mohammed, B. S. Rajan and A. Chockalingam, "On the maximal rate of non-square STBCs from complex orthogonal designs," in Proc. IEEE Global Telecommun. Conf. (GLOBECOM '07), Nov. 2007, pp. 1709-1713.

[19] W. Su, S. N. Batalama, and D. A. Pados, "On orthogonal space-time block codes and transceiver signal linearization," IEEE Commun. Lett. vol. 8, no. 60, pp. 458-460, Feb. 2004.

[20] W. Su and X.-G. Xia, "Two generalized complex orthogonal space-time block codes of rates 7/11 and 3/5 for 5 and 6 transmit antennas", IEEE Trans. Inf. Theory, vol. 69, no. 1, pp. 313 - 316, Jan. 2002.

[21] W. Su, X.-G. Xia, and K. J. R. Lui, "A systematic design of high-rate complex orthogonal space-time block codes," IEEE Commun. Lett. vol. 8, no. 6, pp. 380-382, Jun. 2004.

[22] J. Seberry, S. A. Spence, and T. A. Wysocki, "A construction technique for generalized complex orthogonal designs and applications to wireless communications," Linear Algebra and its Applications 405 (2005) 163-167.

[23] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," IEEE Trans. Inf. Theory, vol. 45, no. 5, pp. 1456-1467, July 1999.

[24] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Correction to 'Space-time block codes from orthogonal designs,"' IEEE Trans. Inf. Theory, vol. 46, no. 1, Jan. 2000.

[25] L. C. Tran, T. A. Wysocki, J. Seberry, A. Mertins and S. S. Adams, "Novel constructions of improved square complex orthogonal designs for eight transmit antennas," IEEE Trans. Inf. Theory, vol. 55, no. 10, Oct. 2009.

[26] H. Wang and X-G. Xia, "Upper bounds of rates of complex orthogonal space-time block codes," IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2788-2796, Oct. 2003.

[27] W. Su, X.-G. Xia, "Two generalized complex orthogonal space-time block codes of rate 7/11 and 3/5 for 5 and 6 transmit antennas," IEEE Trans. Inf. Theory, vol. 49, pp. 313-316, Jan. 2003.