國立交通大學

應用數學系

碩士論文

權重為3 的最優避免衝突碼

Optimal Conflict-avoiding Codes of Even Length and Weight 3

研究生：林逸軒

指導教授：傅恆霖 教授

中華民國九十九年六月

權重為 3 的最優避免衝突碼

研究生：林逸軒　　　　指導教授：傅恆霖 教授

國立交通大學

應用數學系

摘要

如果一個集合 $C \subseteq (Z_2)^n$ 的全部向量都是漢明權重為 k，且在 C 裡任意兩個向量的循環移動距離至少為 2k-2，則我們稱此集合 C 是一個長度為 n 且權重為 k 的衝突避免碼。在本論文中，我們用某些類型的數列，得到了建構長度為 n = 4m (m 為奇數)且權重為 3 的最優避免衝突碼的方法。再加上一些已知結果，我們完全解決了如何建構長度為偶數且權重為 3 的最優避免衝突碼的問題。

Optimal Conflict-avoiding Codes of Even Length and Weight 3

Student: Yi-Hean Lin
Department of Applied Mathematics
National Chiao Tung University
Hsinchu, Taiwan 30050

Advisor: Hung-Lin Fu
Department of Applied Mathematics
National Chiao Tung University
Hsinchu, Taiwan 30050

Abstract

A conflict-avoiding code of length n and weight k is defined as a set $C \subseteq \mathbb{Z}_2^n$ of binary vectors, called codewords, all of Hamming weight k such that the distance of arbitrary cyclic shifts of two distinct codewords in C is at least $2k-2$. In this thesis, we obtain direct constructions for optimal conflict-avoiding codes of length $n = 4m$ where m is odd and weight 3 by using certain types of sequences which are newly constructed. As a consequence (with known results), we have completely settled the problem of constructing optimal conflict-avoiding codes of even length and weight 3.

誌謝

首先，我最想要感謝的人，就是我的指導教授 傅恆霖老師。在這些日子裡，不論在課業上、論文的寫作上都給予很多的指導與關心。也謝謝老師鼓勵並且支持我繼續打排球，讓我能在碩士期間繼續打球。更重要的是在待人處事方面，老師也常常分享他的生活經歷，並且提出許多精闢的見解，讓我受益良多。

同時也非常感謝系上的所有老師，在我求學的這段期間對我的教導與鼓勵，不僅解決了我在課業上的問題與煩惱，也讓我學習到許多課本以外的知識。在所有老師和系上助理小姐的關心與照顧下，讓我感受到了應數大家庭的溫馨與和樂融融。

再來，我要謝謝學長姐們的幫助，特別是貓頭學長。貓頭學長是個很會照顧人的學長，當有問題請教學長，他會非常熱心、不厭其煩的把他所知道的都跟你說，並且給出許多有用的意見。也要感謝常常幫助我的賓賓學長、惠蘭學姊、小貓學長、Robin 學長、敏筠學姊、智懷學長、舜婷、阿草、瑞毅、彥琳、小育、還有許多應數所的同學、交大應數系男排與系女排的所有人，沒有你們的加油打氣與陪伴，相信我的研究生活不會如此多采多姿。謝謝大家在這段時間的照顧，讓我擁有很多很美好的回憶。

最後，我要感謝我最親愛的家人，因為有你們的支持與鼓勵，讓我能無憂慮的情況下，全心全力的完成學業。

Contents

1 Introduction

Protocol sequences for a multiple-access channel (collision channel) without feedback have been investigated by many researchers [3, 5, 6, 8, 12, 13]. In such a multiple-access channel model (see [1] and [7]), the time axis is partitioned into slots whose duration corresponds to the transmission time for one packet and all users are supposed to have slot synchronization, but no other synchronization is assumed. In a particular slot, if none of the users is sending a packet (in which case it is said that each user "sends" the silence symbol), then the channel output in that slot is the silence symbol. If exactly one user is sending a packet in a particular slot, then the packet is transmitted successfully and the channel output in that slot is this packet value q, a prime power. If more than one users are sending packets in a particular slot simultaneously, then there is a conflict and the channel output in that slot is the collision symbol (see Fig. 1).

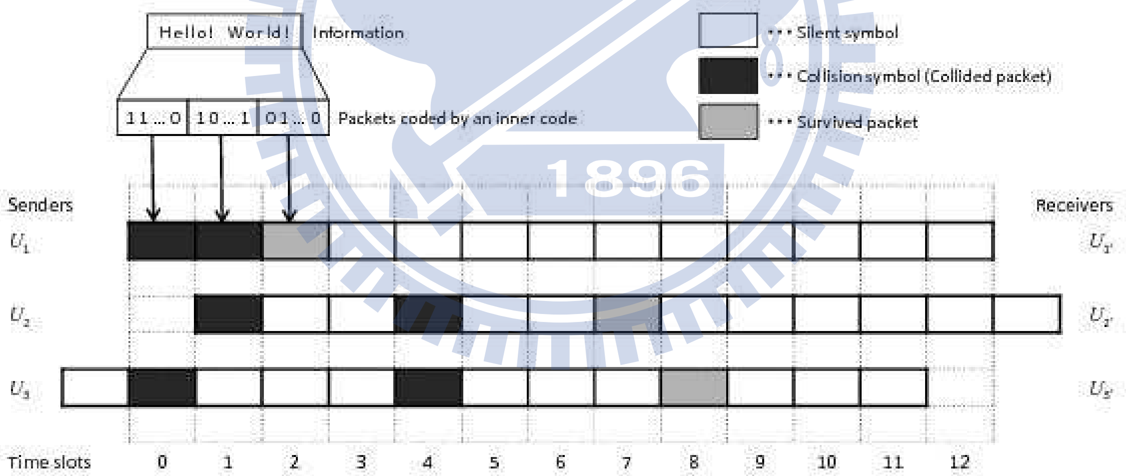

Figure 1: A multiple-access channel model

Each user, say user i, is statically assigned a protocol sequence, which is a binary sequence $x_i = (x_{i,0}, x_{i,1}, \ldots, x_{i,n-1})$ of length n that controls his sending of packets in the following manner: When user i becomes active (after some period of inactivity), he sends a packet (or silence symbol) in the jth slot ($0 \leq j \leq n-1$) of this activity if $x_{i,j} = 1$ (or $x_{i,j} = 0$). User i continues to use the protocol sequence periodically in this manner until there are no more packets to be sent, and after that the user must remain inactive for at least $n-1$ slots. Those silent slots enable the receiver to synchronize the session of user i without any assumption other than slot synchronization, which is a major difference from the synchronizing technique of optical orthogonal codes.

If the protocol sequence x_i has nonzero components, then user i sends w packets in each frame of n slots, where his protocol sequence appears. The set $\mathcal{C} = \{x_1, x_2, \ldots, x_N\}$ of N binary sequences is said to be an (N, k, n, σ) *protocol sequence set* if any $x_i \in \mathcal{C}$ is of length n and has the property that at least σ successful packet transmissions in a frame are guaranteed for each active user, provided that at most k out of N users are active. Our interest is $\sigma = 1$.

An $(N, k, n, 1)$ protocol sequence set is called a *conflict-avoiding code*(CAC) of length n for k active users. A *conflict-avoiding code* of length n for k active users can be viewed as an $(n, k, 1)$ optical orthogonal code without the autocorrelation property, which implies that the maximum size of a conflict-avoiding code should be larger than that of an optical orthogonal code with the same parameters, i.e., larger than $\lfloor (n-1)/\{k(k-1)\} \rfloor$. For the definition and some results of optical orthogonal codes, see [2] and references therein.

Before we introduce the terminologies, an example is presented. Let x, y and z be codewords of length 13 corresponding to the channel model mentioned in Figure 1, see Figure 2.

x = (1 1 1 0 0 0 0 0 0 0 0 0 0)

y = (1 0 0 1 0 0 1 0 0 0 0 0 0)

z = (0 1 0 0 0 1 0 0 0 1 0 0 0)

Figure 2: vector representations (codewords)

Because all users have been assigned just one slot at the same period and three slots for each user, a CAC of weight 3 permit three users to use the code. Figure 2 shows that there are survived packets for all of them.

On the other hand, if three codewords are in Figure 3, then no survived packet for x'.

We will see why this happens in the followings.

z' = (1 0 0 0 0 1 0 0 0 1 0 0)

x' = (1 1 0 0 1 0 0 0 0 0 0 0)

y' = (1 0 0 0 0 1 1 0 0 0 0 0)

Figure 3: Failure situation

In a mathematical description, a *conflict-avoiding code* of length n for k active users is a set $\mathcal{C} \subseteq \{0,1\}^n$ of binary vectors, or *codewords*, all of Hamming weight k, such that the Hamming distance between arbitrary cyclic shifts of distinct codewords is at least $2k-2$. The support $\text{supp}(x)$ of a codeword x is the set of indices of its nonzero positions. In what follows, for convenience, we shall use $\text{supp}(x)$ to represent the codeword x.

For a k-subset A of $\mathbb{Z}_n$, we define the multiset of $k(k-1)$ difference set of A by

$$\Delta(A) = \{i - j \pmod n : i, j \in A, i \neq j\}.$$

A *conflict-avoiding code* of length n and weight k can be defined as a collection $\mathcal{C}$ of k-subsets, called *codewords*, of $\mathbb{Z}_n$ satisfying the condition

$$\Delta(A) \cap \Delta(B) = \emptyset \text{ for any } A, B \in \mathcal{C} \text{ with } A \neq B.$$

Two codewords are said to be *equivalent* if $\Delta(A) = \Delta(B)$.

In fact, we usually consider $0 \in A$ for every codeword A in a *conflict-avoiding code* (CAC). Since for any codeword A in a CAC of length n, the elements of $\Delta(A)$ are symmetric with respect to $n/2$, we henceforth consider the halved difference set defined by

$$\Delta_2(A) = \{i : i \in \Delta(A), 1 \leq i \leq n/2\}$$

instead of $\Delta(A)$. We also use the notation $\Delta_2(\mathcal{C})$ to denote $\cup_{A\in\mathcal{C}}\Delta_2(A)$.

Example 1.1. *Suppose that* $A = \{0, 20, 40\}$, $B = \{0, 6, 12\}$ *and* $C = \{0, 1, 22\}$ *are codewords of a conflict-avoiding code of length* 60*. In this case,*

$$\begin{array}{ll} \Delta(A) = \{20, 20, 20, 40, 40, 40\}, & \Delta_2(A) = \{20\}, \\ \Delta(B) = \{6, 6, 12, 48, 54, 54\}, & \Delta_2(B) = \{6, 12\}, \\ \Delta(C) = \{1, 22, 23, 37, 38, 59\}, & \Delta_2(C) = \{1, 22, 23\}. \end{array}$$

we denote the class of all the CACs of length n and weight k by $\mathrm{CAC}(n,k)$.

For some $i,t\in\mathbb{Z}_n$, a codeword A of weight k is said to be *equi-difference* (or *centered* when $k=3$) if it has the form

$$A=\{t,i+t,\ldots,(k-1)i+t\}\pmod{n}.$$

and a code $\mathcal{C}\in\mathrm{CAC}(n,k)$ is called an *equi-difference* code (or *centered* code when $k=3$)if every codeword in $\mathcal{C}$ is equi-difference.

The maximum size of some codes in $\mathrm{CAC}(n,k)$ is denoted by $M(n,k)$, i.e.,

$$M(n,k)=\max\{|\mathcal{C}|:\mathcal{C}\in\mathrm{CAC}(n,k)\}.$$

A code $\mathcal{C}\in\mathrm{CAC}(n,k)$ is said to be *optimal* if $|\mathcal{C}|=M(n,k)$. Similarly, the maximum size of equi-difference codes is defined in a similar manner to $M(n,k)$ by follows:

$$M^e(n,k)=\max\{|\mathcal{C}|:\mathcal{C}\in\mathrm{CAC}^e(n,k)\},$$

where $\mathrm{CAC}^e(n,k)$ is the subclass consisting of all the equi-difference codes in $\mathrm{CAC}^e(n,k)$.In this thesis, we focus on $\mathrm{CAC}(n,k)$ only.Moreover, only the case $k=3$ is treated. In what follow, $\mathrm{CAC}(n,3)$ and $M(n,3)$ are simply written as $\mathrm{CAC}(n)$ and $M(n)$, respectively.

Levenshtein and Tonchev [6] derived the following upper bound on $M(n)$:

$$M(n)\le\frac{n+1}{4}, \tag{1.1}$$

and further proved that

$$M(n)=\frac{n-2}{4}\quad\text{if } n\equiv 2\pmod{4}.$$

Jimbo et al. [4] improved the Levenshtein's bound (1.1) for the case $n\equiv 0\pmod 4$ by using linear programming.

Theorem 1.2 (Jimbo et al. [4]). *Let $n = 4t$. Then*

$$M(n) \le \begin{cases} 7n/32, & \text{if } t \equiv 0 \pmod{8}, \\ (7n+4)/32, & \text{if } t \equiv 1 \pmod{8}, \\ (7n-24)/32, & \text{if } t \equiv 2, 10 \pmod{24}, \\ (7n+12)/32, & \text{if } t \equiv 3 \pmod{24}, \\ (7n-16)/32, & \text{if } t \equiv 4, 20 \pmod{24}, \\ (7n-12)/32, & \text{if } t \equiv 5, 13 \pmod{24}, \\ (7n-8)/32, & \text{if } t \equiv 6 \pmod{8}, \\ (7n-4)/32, & \text{if } t \equiv 7 \pmod{8}, \\ (7n-20)/32, & \text{if } t \equiv 11, 19 \pmod{24}, \\ (7n+16)/32, & \text{if } t \equiv 12 \pmod{24}, \\ (7n+8)/32, & \text{if } t \equiv 18 \pmod{24}, \\ (7n+20)/32, & \text{if } t \equiv 21 \pmod{24}. \end{cases}$$

Here let us review briefly the linear programming problem formulated by Jimbo et al. [4]. Partition integers not exceeding $n/2$ into the following three subsets.

$$O = \{i : i \equiv 1 \pmod{2},\ 1 \le i \le n/2\},$$

$$E = \{i : i \equiv 2 \pmod{4},\ 1 \le i \le n/2\},$$

$$D = \{i : i \equiv 0 \pmod{4},\ 1 \le i \le n/2\}.$$

The integers belonging to O are odd, those belonging to E are said to be *singly even* and those belonging to D are said to be *doubly even*. Then it is easy to see that any codeword can be categorized as in Lemmas 1.3 and 1.4 according to the composition of its halved difference set.

Lemma 1.3 ([4]). *Any centered codeword $A \in \mathcal{C}$ such that $\Delta_2(A) = \{i, j\}$, where $j = 2i$ if $i \in [1, n/4]$, and $j = n - 2i$ if $i \in (n/4, n/2)$ and $i \ne n/3$, belongs to one of the following three types:*

(i) *$i \in O$ and $j \in E$,*

(ii) *$i \in E$ and $j \in D$,*

(iii) *$i, j \in D$.*

Lemma 1.4 ([4]). *Any non-centered codeword $A \in \mathcal{C}$ such that $\Delta_2(A) = \{i, j, k\}$ belongs to one of the following four types:*

(iv) *two of i, j and k are in O and one is in E,*

(v) *two of* i, j *and* k *are in* O *and one is in* D*,*

(vi) *two of* i, j *and* k *are in* E *and one is in* D*,*

(vii) $i, j, k \in D$*.*

After the fashion of [4], we also use the notations C_o, C_e and C_d to denote the sets of centered codewords of types (i), (ii) and (iii) categorized in Lemma 1.3, and N_{oe}, N_{od}, N_e and N_d to denote the sets of non-centered codewords of types (iv), (v), (vi) and (vii) categorized in Lemma 1.4, respectively. For convenience, we treat the centered codewords $\{0, n/3, 2n/3\}$ and $\{0, n/4, n/2\}$ separately from C_o, C_e and C_d, and define the following parameters.

$$\alpha = \begin{cases} 1 & \text{if } \{0, n/3, 2n/3\} \in \mathcal{C}, \\ 0 & \text{otherwise,} \end{cases}$$

$$\beta = \begin{cases} 1 & \text{if } \{0, n/4, n/2\} \in \mathcal{C}, \\ 0 & \text{otherwize.} \end{cases}$$

Then it follows that

$$C_o \cup C_e \cup C_d \cup N_{oe} \cup N_{od} \cup N_e \cup N_d$$
$$= \mathcal{C} \setminus \{\{0, n/3, 2n/3\}, \{0, n/4, n/2\}\}$$

and

$$|\mathcal{C}| = s\alpha + \beta + |C_o| + |C_e| + |C_d| + |N_{oe}| + |N_{od}| + |N_e| + |N_d|, \tag{1.2}$$

where the parameter s accounts for the centered codeword $\{0, n/3, 2n/3\}$, i.e., $s = 1$ if $n \equiv 0 \pmod 3$, otherwise $s = 0$.

An upper bound on $M(n = 4t)$ of Theorem 1.2 can be obtained by maximizing (1.2) subject to

$$\begin{aligned} & k_1\beta + |C_o| + 2|N_{oe}| + 2|N_{od}| \le \frac{n}{4}, \\ & k_2\beta + |C_o| + |C_e| + |N_{oe}| + 2|N_e| \le \left\lceil \frac{n}{8} \right\rceil, \\ & s\alpha + k_3\beta + |C_e| + 2|C_d| \\ & \qquad + |N_{od}| + |N_e| + 3|N_d| \le \left\lfloor \frac{n}{8} \right\rfloor, \\ & |C_o| \le \left\lfloor \frac{n}{8} \right\rfloor, \ \alpha \le 1, \ \beta \le 1, \end{aligned} \tag{1.3}$$

where

$$(1.4) \qquad (s, k_1, k_2, k_3) = \begin{cases} (1,0,0,2) & \text{if } t \equiv 0 \pmod{12}, \\ (1,0,1,1) & \text{if } t \equiv 6 \pmod{12}, \\ (0,0,1,1) & \text{if } t \equiv 2, 10 \pmod{12}, \\ (0,0,0,2) & \text{if } t \equiv 4, 8 \pmod{12}, \\ (0,1,1,0) & \text{if } t \equiv 1, 5 \pmod{6}, \\ (1,1,1,0) & \text{if } t \equiv 3 \pmod{6}. \end{cases}$$

For the conditions (1.3) and (1.4), see Section 2 of [4]. The technique for solving the LP probelm is also demonstrated in [4] (and [9]).

In [4] Jimbo et al. further proved that the upper bounds in Theorem 1.2 are strict if $t \equiv 2 \pmod{4}$, i.e., $n \equiv 8 \pmod{16}$ [4, Theorem 3.1].

Recently, Mishima et al. [9] showed that with two exceptions, the equality in Theorem 1.2 holds for $t \equiv 0 \pmod{4}$, i.e., $n \equiv 0 \pmod{16}$.

Theorem 1.5 (Mishima et al. [9]). *Let $n = 16m$. The maximum size $M(n)$ of a code $\mathcal{C} \in \mathrm{CAC}(n)$ is*

$$M(n) = \begin{cases} 7n/32, & \text{if } m \equiv 0 \pmod{2}, \\ (7n-16)/32, & \text{if } m \equiv 1, 5 \pmod{6}, \\ (7n+16)/32, & \text{if } m \equiv 3 \pmod{6}. \end{cases}$$

with the exceptions $M(48) = 10$ and $M(64) = 13$.

It now turns out that for even n, the case for which the strictness of the upper bound on $M(n)$ remains unsettled is $n \equiv 4 \pmod{8}$. Our objective is to determine the exact values of $M(n)$ completely for all even n by proving the strictness of Theorem 1.2 for the remaining cases, i.e., by proving the following theorem.

Theorem 1.6. *Let $n = 8m + 4$. Then*

$$M(n) = \begin{cases} (7n+4)/32, & \text{if } m \equiv 0 \pmod{4}, \\ (7n+12)/32, & \text{if } m \equiv 1 \pmod{12}, \\ (7n-12)/32, & \text{if } m \equiv 2, 6 \pmod{12}, \\ (7n-4)/32, & \text{if } m \equiv 3 \pmod{4}, \\ (7n-20)/32, & \text{if } m \equiv 5, 9 \pmod{12}, \\ (7n+20)/32, & \text{if } m \equiv 10 \pmod{12}. \end{cases}$$

As for odd n, which is not treated in this thesis, the necessary and sufficient condition to satisfy $M(n) = (n-1)/4$ or $(n+1)/4$ can be found in [10], but known results on $M(n)$ for odd n are very few so far.

2 Odd sequences with doubly even integers latently

Mishima et al. [9] used Skolem type sequences effectively in the proof of Theorem 1.5 and with those sequences, they also gave a simpler proof of Theorem 3.1 in [4] than the original one. Unfortunately, the Skolem type sequences used in [9] to prove the strictiness of the upper bound on $M(n)$ is not valid for our present target case $n \equiv 4 \pmod 8$. So, we define here a new sequence with a certain property and provide several series of those sequences that are needed for our constructions of optimal codes in CAC(n).

Definition 2.1. *For positive integers k and n, let K be a k-subset of $\{1, 2, \ldots, n\}$ and F be a $2k$-subset of the $2n$ odd integers $\{1, 3, \ldots, 4n-1\}$. A K-extended odd sequence of order n and defect F with doubly even integers latently, denoted by K-ext $\mathcal{O}_n$ of defect F for short, is a collection of $n-k$ ordered pairs of odd integers*

$$\{(a_i, b_i) : b_i - a_i = 4i \text{ or } b_i + a_i = 4i, i \in \{1, 2, \ldots, n\} \setminus K\}$$

with

$$\bigcup_{\substack{i=1 \\ i \notin K}}^{n} \{a_i, b_i\} = \{1, 3, \ldots, 4n-1\} \setminus F.$$

If $K = \{t\}$, a K-ext $\mathcal{O}_n$ of defect F is simply denoted as t-ext $\mathcal{O}_n$ of defect F, and if $K = \emptyset$, it is denoted just as $\mathcal{O}_n$.

Example 2.2. (1) An $\mathcal{O}_4$:

$\{(7, 11), (5, 13), (3, 9), (1, 15)\}$.

(2) A 2-ext $\mathcal{O}_5$ of defect $\{13, 19\}$:

$\{(7, 11), (3, 9), (1, 17), (5, 15)\}$.

(3) A $\{2, 3\}$-ext $\mathcal{O}_8$ of defect $\{3, 5, 29, 31\}$:

$\{(23, 27), (9, 25), (1, 19), (11, 13), (7, 21), (15, 17)\}$.

Lemma 2.3. *There exists an $\mathcal{O}_n$ if $n \equiv 0, 1 \pmod 4$.*

Proof. The proof is devided into two cases.

(i) The case $n \equiv 0 \pmod 4$. Put doubly even integers in $[4, 4n]$ as follows:

$$4 \text{ in } (3n-3, 3n+1);$$

$$8+8i \text{ in } (2n-7-4i, 2n+1+4i),\ 0 \le i \le n/4-2;$$

$$12+8i \text{ in } (2n-5-4i, 2n+7+4i),\ 0 \le i \le n/4-2;$$

$$2n \text{ in } (3, 2n+3);$$

$$4n-8-4i \text{ in } (5+2i, 4n-3-2i),\ 0 \le i \le n/2-3;$$

$$4n-4 \text{ in } (2n-3, 2n-1);$$

$$4n \text{ in } (1, 4n-1).$$

Then the set of the above n pairs is a partition of $\{1, 3, \ldots, 4n-1\}$, which means that it is an $\mathcal{O}_n$,

(ii) The case $n \equiv 1 \pmod 4$. Note that the case (i) guarantees the existence of an $\mathcal{O}_{n-1}$ for $n \ge 5$. Metamorphose the pair $(3, 2(n-1)+3)$ in the $\mathcal{O}_{n-1}$ together with $\{4n-3, 4n-1\}$ into the following two pairs so that $2(n-1)$ and $4n$ can be there latently.

$$2n-2 \text{ in } (2n+1, 4n-1);$$

$$4n \text{ in } (3, 4n-3).$$

Then the remaining $n-2$ pairs in the $\mathcal{O}_{n-1}$ and the above two pairs form an $\mathcal{O}_n$ for $n \ge 5$. If $n = 1$, it is trivial that $\{(1, 3)\}$ is the $\mathcal{O}_1$. ∎

Example 2.4. (1) An $\mathcal{O}_{12}$:

$\{(33, 37), (17, 25), (19, 31), (13, 29), (15, 35), (3, 27),$

$(11, 39), (9, 41), (7, 43), (5, 45), (21, 23), (1, 47)\}.$

(2) An $\mathcal{O}_{13}$:

$\mathcal{O}_{12} \setminus \{(3, 27)\} \bigcup \{(3, 49), (27, 51)\}.$

Lemma 2.5. *There exists an n-ext* $\mathcal{O}_n$ *of defect* F *if*

(1) $n \equiv 0 \pmod 4$ *and* $F \in \{\{2n-1, 2n+1\}, \{4n-7, 4n-1\}.$

(2) $n \equiv 2 \pmod 4$, $n \ge 6$ *and* $F = \{2n-3, 2n+7\}$, *and*

(3) $n \equiv 3 \pmod 4$ *and* $F \in \{\{2n-1, 2n+5\}, \{4n-13, 4n-3\}, \{4n-5, 4n-3\}\}.$

Proof. (1) The case $n \equiv 0 \pmod 4$ and $F = \{2n-1, 2n+1\}$. If $n \geq 8$, put doubly even integers as follows:

$$4 \text{ in } (3n-5, 3n-1);$$

$$8+8i \text{ in } (2n-3-4i, 2n+5+4i),\ 0 \leq i \leq n/2-2;$$

$$12+8i \text{ in } (2n-9-4i, 2n+3+4i),\ 0 \leq i \leq n/4-3;$$

$$2n-4 \text{ in } (1, 2n-5);$$

$$4n-4-8i \text{ in } (3+4i, 4n-1-4i),\ 0 \leq i \leq n/4-1.$$

If $n = 4$, we have $\{(11,15),(3,5),(1,13)\}$ as a 4-ext $\mathcal{O}_4$ of defect $\{7,9\}$.

The case $n \equiv 0 \pmod 4$ and $F = \{4n-7, 4n-1\}$. Put doubly even integers as follows:

$$4 \text{ in } (n-1, n+3);$$

$$8+8i \text{ in } (2n-1-4i, 2n+7+4i),\ 0 \leq i \leq n/4-2;$$

$$12+8i \text{ in } (2n-11-4i, 2n+1+4i),\ 0 \leq i \leq n/2-3;$$

$$4n-8-8i \text{ in } (3+4i, 4n-5-4i),\ 0 \leq i \leq n/4-2;$$

$$2n \text{ in } (2n-3, 4n-3);$$

$$4n-4 \text{ in } (2n-7, 2n+3).$$

(2) The case $n \equiv 2 \pmod 4$. Put doubly even integers as follows:

$$4 \text{ in } (n+1, n+5);$$

$$8+8i \text{ in } (2n+3-4i, 2n+11+4i),\ 0 \leq i \leq (n-2)/4-1;$$

$$12+8i \text{ in } (2n-7-4i, 2n+5+4i),\ 0 \leq i \leq n/2-2;$$

$$4n-8-8i \text{ in } (7+4i, 4n-1-4i),\ 0 \leq i \leq (n-2)/4-2;$$

$$2n+4 \text{ in } (3, 2n+1).$$

(3) The case $n \equiv 3 \pmod 4$ and $F = \{2n-1, 2n+5\}$. From the case (2), there does exist an $(n-1)$-ext $\mathcal{O}_{n-1}$ of defect $\{2n-5, 2n+5\}$ for $n \geq 7$. Assemble the pair $(3, 2(n-1)+1)$ in the $(n-1)$-ext $\mathcal{O}_{n-1}$ and $\{2n-5, 2n+5, 4n-3, 4n-1\}$ into the following two pairs

$$2(n-1)+4 \text{ in } (2n-5, 4n-3);$$

$$4n-4 \text{ in } (3, 4n-1).$$

Then together with the remaining pairs in the $(n-1)$-ext $\mathcal{O}_{n-1}$, an n-ext $\mathcal{O}_n$ of defect $\{2n-1, 2n+5\}$ can be obtained for $n \geq 7$. If $n = 3$, we have $\{(3,7),(1,9)\}$ as a 3-ext $\mathcal{O}_3$ of defect $\{5, 11\}$.

The case $n \equiv 3 \pmod 4$ and $F = \{4n-13, 4n-3\}$. If $n \geq 11$, put doubly even integers as follows:

$$4 \text{ in } (n-4, n);$$

$$8 \text{ in } (4n-9, 4n-1);$$

$$12+8i \text{ in } (2n-9-4i, 2n+3+4i),\ 0 \leq i \leq (n-1)/2-2;$$

$$16+8i \text{ in } (2n-11-4i, 2n+5+4i),\ 0 \leq i \leq (n-3)/4-3;$$

$$4n-20-8i \text{ in } (3+4i, 4n-17-4i),\ 0 \leq i \leq (n-3)/4-2;$$

$$2n-6 \text{ in } (2n+1, 4n-5);$$

$$4n-12 \text{ in } (2n-7, 2n-5);$$

$$4n-4 \text{ in } (2n-3, 2n-1).$$

If $n = 7$, we have $\{(9,13),(11,19),(5,17),(7,23),(1,21),(3,27)\}$ as a 7-ext $\mathcal{O}_7$ of defect $\{15, 25\}$.

The case $n \equiv 3 \pmod 4$ and $F = \{4n-5, 4n-3\}$. If $n \geq 7$, put doubly even integers as follows:

$$4 \text{ in } (3n-4, 3n);$$

$$8+8i \text{ in } (2n-9-4i, 2n-1+4i),\ 0 \leq i \leq (n-3)/4-1;$$

$$12+8i \text{ in } (2n-7-4i, 2n+5+4i),\ 0 \leq i \leq (n-1)/2-3;$$

$$4n-12-8i \text{ in } (5+4i, 4n-7-4i),\ 0 \leq i \leq (n-3)/4-2;$$

$$2n+2 \text{ in } (1, 2n+1);$$

$$4n-8 \text{ in } (2n-5, 2n-3);$$

$$4n-4 \text{ in } (3, 4n-1).$$

If $n = 3$, we have $\{(1,5),(3,11)\}$ as a 3-ext $\mathcal{O}_3$ of defect $\{7, 9\}$. ∎

Example 2.6. (1) A 8-ext $\mathcal{O}_8$ of defect $\{15, 17\}$:

$\{(19,23),(13,21),(1,11),(9,25),(7,27),(5,29),(3,31)\}$.

A 8-ext $\mathcal{O}_8$ of defect $\{25, 31\}$:

$\{(7, 11), (15, 23), (5, 17), (13, 29), (1, 21), (3, 27), (9, 19)\}$.

(2) A 10-ext $\mathcal{O}_{10}$ of defect $\{17, 27\}$:

$\{(11, 15), (23, 31), (13, 25), (19, 35), (9, 29), (3, 21), (5, 33), (7, 39), (1, 37)\}$.

(3) A 11-ext $\mathcal{O}_{11}$ of defect $\{31, 41\}$:

$\{(7, 11), (35, 43), (13, 25), (23, 39), (9, 29), (3, 27), (5, 33), (15, 17), (1, 37), (19, 21)\}$.

A 11-ext $\mathcal{O}_{11}$ of defect $\{39, 41\}$:

$\{(29, 33), (13, 21), (15, 27), (9, 25), (11, 31), (1, 23), (7, 35), (5, 37), (17, 19), (3, 43)\}$.

Lemma 2.7. *There exists a 2-ext $\mathcal{O}_n$ of defect F if*

(1) $n \equiv 0 \pmod 4$ *and* $F = \{4n-5, 4n-3\}$,

(2) $n \equiv 1 \pmod 4$, $n \geq 5$ *and* $F = \{4n-7, 4n-1\}$, *and*

(3) $n \equiv 2, 3 \pmod 4$ *and* $F = \{4n-3, 4n-1\}$.

Proof. (1) The case $n \equiv 0 \pmod 4$. If $n \geq 8$, put doubly even integers as follows:

$$4 \text{ in } (3n-11, 3n-7);$$

$$12+8i \text{ in } (2n-11-4i, 2n+1+4i),\ 0 \leq i \leq n/4-3;$$

$$16+8i \text{ in } (2n-9-4i, 2n+7+4i),\ 0 \leq i \leq n/2-4;$$

$$4n-12-8i \text{ in } (5+4i, 4n-7-4i),\ 0 \leq i \leq n/4-2;$$

$$2n-4 \text{ in } (3, 2n-1);$$

$$4n-8 \text{ in } (2n-5, 2n-3);$$

$$4n-4 \text{ in } (2n-7, 2n+3);$$

$$4n \text{ in } (1, 4n-1).$$

If $n = 4$, $\{(1, 5), (3, 15), (7, 9)\}$ is a 2-ext $\mathcal{O}_4$ of defect $\{11, 13\}$.

(2) The case $n \equiv 1 \pmod 4$. If $n \geq 9$, we first construct the 2-ext $\mathcal{O}_{n-1}$ of defect $\{4(n-1)-5, 4(n-1)-3\}$ according to the construction for the case (1). Next, metamorphose the pair $(3, 2(n-1)-1)$ in the 2-ext $\mathcal{O}_{n-1}$ with $\{4n-9, 4n-3\}$ into the following two pairs so that $2(n-1)-4$ and $4n$ can be there latently.

$$2n-6 \text{ in } (2n-3, 4n-9);$$

$$4n \text{ in } (3, 4n-3).$$

Then together with the remaining pairs in the 2-ext $\mathcal{O}_{n-1}$, we have a 2-ext $\mathcal{O}_n$ of defect $\{4n-7, 4n-1\}$.If $n = 5$, $\{(7,11),(3,9),(1,17),(5,15)\}$ is a 2-ext $\mathcal{O}_5$ of defect $\{13, 19\}$.

(3) The case $n \equiv 2 \pmod 4$. If $n \geq 10$, put doubly even integers as follows:

$$4 \text{ in } (3n-3, 3n+1);$$

$$12+8i \text{ in } (2n-11-4i, 2n+1+4i),\ 0 \leq i \leq n/2-3;$$

$$16+8i \text{ in } (2n-9-4i, 2n+7+4i),\ 0 \leq i \leq (n-2)/4-3;$$

$$4n-16-8i \text{ in } (11+4i, 4n-5-4i),\ 0 \leq i \leq (n-2)/4-2;$$

$$2n-4 \text{ in } (3, 2n-1);$$

$$4n-8 \text{ in } (2n-5, 2n-3);$$

$$4n-4 \text{ in } (2n-7, 2n+3);$$

$$4n \text{ in } (7, 4n-7).$$

If $n = 6$, $\{(7,11),(5,17),(3,13),(1,19),(9,15)\}$ is a 2-ext $\mathcal{O}_6$ of defect $\{21, 23\}$. If $n = 2$, $\{(1,3)\}$ is a 2-ext $\mathcal{O}_2$ of defect $\{5, 7\}$.

The case $n \equiv 3 \pmod 4$. If $n \geq 7$, put doubly even integers as follows:

$$4 \text{ in } (n-2, n+2);$$

$$12+8i \text{ in } (2n-5-4i, 2n+7+4i),\ 0 \leq i \leq (n-3)/4-2;$$

$$16+8i \text{ in } (2n-11-4i, 2n+5+4i),\ 0 \leq i \leq (n-1)/2-3;$$

$$4n-8-8i \text{ in } (1+4i, 4n-7-4i),\ 0 \leq i \leq (n-3)/4-1;$$

$$2n-2 \text{ in } (2n-3, 4n-5);$$

$$4n-4 \text{ in } (2n-7, 2n+3);$$

$$4n \text{ in } (2n-1, 2n+1).$$

If $n = 3$, $\{(1,3),(5,7)\}$ is a 2-ext $\mathcal{O}_3$ of defect $\{9, 11\}$. ∎

Example 2.8. (1) A 2-ext $\mathcal{O}_8$ of defect $\{27, 29\}$:

$\{(13, 17), (3, 15), (7, 23), (5, 25), (11, 13), (9, 19), (1, 31)\}$.

(2) A 2-ext $\mathcal{O}_9$ of defect $\{29, 35\}$:

2-ext $\mathcal{O}_8 \backslash \{(3, 15)\} \cup \bigcup \{(15, 27), (3, 33)\}$.

(3) A 2-ext $\mathcal{O}_{10}$ of defect $\{37, 39\}$:

$\{(27, 31), (9, 21), (3, 19), (5, 25), (11, 35), (1, 29), (15, 17), (13, 23), (7, 33)\}$.

A 2-ext $\mathcal{O}_{11}$ of defect $\{41, 43\}$:

$\{(9, 13), (17, 29), (11, 27), (19, 39), (7, 31), (5, 33), (3, 35), (1, 37), (15, 25), (21, 23)\}$.

Lemma 2.9. *There exists a 3-ext $\mathcal{O}_n$ of defect F if*

(1) $n \equiv 0, 1 \pmod 4$, $n \geq 4$ *and* $F = \{1, 3\}$, *and*

(2) $n \equiv 2, 3 \pmod 4$, $n \geq 3$ *and* $F = \{3, 5\}$.

Proof. (1) The case $n \equiv 0 \pmod 4$. If $n \geq 8$, put doubly even integers as follows:

$$4 \text{ in } (3n + 1, 3n + 5);$$

$$8 \text{ in } (2n + 3, 2n + 11);$$

$$16 + 8i \text{ in } (2n - 11 - 4i, 2n + 5 + 4i),\ 0 \leq i \leq n/4 - 2;$$

$$20 + 8i \text{ in } (2n - 5 - 4i, 2n + 15 + 4i),\ 0 \leq i \leq n/2 - 4;$$

$$4n - 8 - 8i \text{ in } (5 + 4i, 4n - 3 - 4i),\ 0 \leq i \leq n/4 - 3;$$

$$2n + 8 \text{ in } (7, 2n + 1);$$

$$4n - 4 \text{ in } (2n - 3, 2n - 1);$$

$$4n \text{ in } (2n - 7, 2n + 7).$$

If $n = 4$, $\{(9, 13), (7, 15), (5, 11)\}$ is a 3-ext $\mathcal{O}_4$ of defect $\{1, 3\}$.

The case $n \equiv 1 \pmod 4$. If $n \geq 9$, put doubly even integers as follows:

$$4 \text{ in } (3n, 3n+4);$$

$$8 \text{ in } (2n-3, 2n+5);$$

$$16+8i \text{ in } (2n-5-4i, 2n+11+4i),\ 0 \leq i \leq (n-1)/2-3;$$

$$20+8i \text{ in } (2n-11-4i, 2n+9+4i),\ 0 \leq i \leq (n-1)/4-3;$$

$$4n-8-8i \text{ in } (7+4i, 4n-1-4i),\ 0 \leq i \leq (n-1)/4-2;$$

$$2n+2 \text{ in } (5, 2n+7);$$

$$4n-4 \text{ in } (2n-7, 2n+3);$$

$$4n \text{ in } (2n-1, 2n+1).$$

If $n = 5$, $\{(13,17),(11,19),(7,9),(5,15)\}$ is a 3-ext $\mathcal{O}_5$ of defect $\{1,3\}$.

(2) The case $n \equiv 2 \pmod 4$. If $n \geq 10$, put doubly even integers as follows:

$$4 \text{ in } (3n+1, 3n+5);$$

$$8 \text{ in } (2n+1, 2n+9);$$

$$16+8i \text{ in } (2n-9-4i, 2n+7+4i),\ 0 \leq i \leq (n-2)/4-2;$$

$$20+8i \text{ in } (2n-7-4i, 2n+13+4i),\ 0 \leq i \leq n/2-4;$$

$$4n-8-8i \text{ in } (7+4i, 4n-1-4i),\ 0 \leq i \leq (n-2)/4-2;$$

$$2n+4 \text{ in } (1, 2n+3);$$

$$4n-4 \text{ in } (2n-3, 2n-1);$$

$$4n \text{ in } (2n-5, 2n+5).$$

If $n = 6$, $\{(19,23),(13,21),(1,15),(9,11),(7,17)\}$ is a 3-ext $\mathcal{O}_6$ of defect $\{3,5\}$.

The case $n \equiv 3 \pmod 4$. If $n \geq 7$, put doubly even integers as follows:

$$4 \text{ in } (3n+2, 3n+6);$$

$$8 \text{ in } (2n-3, 2n+5);$$

$$16+8i \text{ in } (2n-5-4i, 2n+11+4i),\ 0 \leq i \leq (n-1)/2-3;$$

$$20+8i \text{ in } (2n-11-4i, 2n+9+4i),\ 0 \leq i \leq (n-3)/4-2;$$

$$4n-8-8i \text{ in } (7+4i, 4n-1-4i),\ 0 \leq i \leq (n-3)/4-1;$$

$$2n+6 \text{ in } (1, 2n+7);$$

$$4n-4 \text{ in } (2n-7, 2n+3);$$

$$4n \text{ in } (2n-1, 2n+1).$$

If $n = 3$, $\{(7,11),(1,9)\}$ is a 3-ext $\mathcal{O}_3$ of defect $\{3,5\}$. ∎

Lemma 2.10. *There exists a* $\{2,3\}$*-ext* $\mathcal{O}_n$ *of defect* F *if*

(1) $n \equiv 0, 1 \pmod 4$, $n \geq 8$ *and* $F = \{3, 5, 4n-3, 4n-1\}$, *and*

(2) $n \equiv 2, 3 \pmod 4$, $n \geq 7$ *and* $F = \{1, 3, 4n-3, 4n-1\}$.

Proof. (1) The case $n \equiv 0 \pmod 4$. If $n \geq 8$, put doubly even integers as follows:

$$4 \text{ in } (3n-1, 3n+3);$$

$$16+8i \text{ in } (2n-7-4i, 2n+9+4i),\ 0 \leq i \leq n/2-4;$$

$$20+8i \text{ in } (2n-13-4i, 2n+7+4i),\ 0 \leq i \leq n/4-3;$$

$$4n-12-8i \text{ in } (7+4i, 4n-5-4i),\ 0 \leq i \leq n/4-3;$$

$$2n+4 \text{ in } (1, 2n+3);$$

$$4n-8 \text{ in } (2n-5, 2n-3);$$

$$4n-4 \text{ in } (2n-9, 2n+5);$$

$$4n \text{ in } (2n-1, 2n+1).$$

The case $n \equiv 1 \pmod 4$. If $n \geq 9$, put doubly even integers as follows:

$$4 \text{ in } (3n, 3n+4);$$

$$16+8i \text{ in } (2n-11-4i, 2n+5+4i),\ 0 \leq i \leq (n-1)/4-2;$$

$$20+8i \text{ in } (2n-9-4i, 2n+11+4i),\ 0 \leq i \leq (n-1)/2-4;$$

$$4n-12-8i \text{ in } (7+4i, 4n-5-4i),\ 0 \leq i \leq (n-1)/4-3;$$

$$2n+6 \text{ in } (1, 2n+7);$$

$$4n-8 \text{ in } (2n-5, 2n-3);$$

$$4n-4 \text{ in } (2n-7, 2n+3);$$

$$4n \text{ in } (2n-1, 2n+1).$$

(2) The case $n \equiv 2 \pmod 4$. If $n \geq 10$, put doubly even integers as follows:

$$4 \text{ in } (3n+1, 3n+5);$$

$$16+8i \text{ in } (2n-7-4i, 2n+9+4i),\ 0 \leq i \leq n/2-4;$$

$$20+8i \text{ in } (2n-13-4i, 2n+7+4i),\ 0 \leq i \leq (n-2)/4-2;$$

$$4n-12-8i \text{ in } (7+4i, 4n-5-4i),\ 0 \leq i \leq (n-2)/4-3;$$

$$2n+8 \text{ in } (5, 2n+3);$$

$$4n-8 \text{ in } (2n-5, 2n-3);$$

$$4n-4 \text{ in } (2n-9, 2n+5);$$

$$4n \text{ in } (2n-1, 2n+1).$$

The case $n \equiv 3 \pmod 4$. If $n \geq 7$, put doubly even integers as follows:

$$4 \text{ in } (3n-2, 3n+2);$$

$$16+8i \text{ in } (2n-11-4i, 2n+5+4i),\ 0 \leq i \leq (n-3)/4-2;$$

$$20+8i \text{ in } (2n-9-4i, 2n+11+4i),\ 0 \leq i \leq (n-1)/2-4;$$

$$4n-12-8i \text{ in } (7+4i, 4n-5-4i),\ 0 \leq i \leq (n-3)/4-2;$$

$$2n+2 \text{ in } (5, 2n+7);$$

$$4n-8 \text{ in } (2n-5, 2n-3);$$

$$4n-4 \text{ in } (2n-7, 2n+3);$$

$$4n \text{ in } (2n-1, 2n+1).$$

∎

3 Constructions for optimal CACs

We will now present direct constructions for optimal codes in CAC($n = 8m + 4$), which will eventually prove Theorem 1.6. The constructions are given for the following nine subcases, respectively.

(1) $m \equiv 0, 4 \pmod{16}$,

(2) $m \equiv 8, 12 \pmod{16}$,

(3) $m \equiv 1 \pmod{12}$,

(4) $m \equiv 5, 9 \pmod{12}$,

(5) $m \equiv 2, 6, 18, 38 \pmod{48}$,

(6) $m \equiv 14, 26, 30, 42 \pmod{48}$,

(7) $m \equiv 22, 34 \pmod{48}$,

(8) $m \equiv 10, 46 \pmod{48}$, and

(9) $m \equiv 3 \pmod{4}$.

For reference, we list in Table 1 the sizes of subsets of codewords produced by our direct constructions, which indeed meet the upper bounds on $M(n)$ of Theorem 1.6.

Table 1: Sizes of subsets of codewords for an optimal code in CAC($n = 8m + 4$)

m	α	β	$\lvert C_o\rvert$	$\lvert C_d\rvert$	$\lvert N_{od}\rvert$	$\lvert C\rvert$
$0 \pmod{4}$	0	1	$(n-4)/8$	$(n-4)/32$	$(n-4)/16$	$(7n+4)/32$
$1 \pmod{12}$	1	1	$(n-4)/8-1$	$(n-12)/32$	$(n+4)/16$	$(7n+12)/32$
$2, 6 \pmod{12}$	0	1	$(n-4)/8$	$(n-20)/32-1$	$(n+12)/16$	$(7n-12)/32$
$3 \pmod{4}$	0	1	$(n-4)/8$	$(n-28)/32$	$(n+4)/16$	$(7n-4)/32$
$5, 9 \pmod{12}$	0	1	$(n-4)/8$	$(n-12)/32-2$	$(n+4)/16+1$	$(7n-20)/32$
$10 \pmod{12}$	1	1	$(n-4)/8$	$(n-20)/32$	$(n-4)/16$	$(7n+20)/32$

Construction 3.1. The case $m \equiv 0, 4 \pmod{16}$, i.e., $n \equiv 4, 36 \pmod{128}$. Let C_o be the set of the following $(n-4)/8$ centered codewords:

$$\{0, n/2+1-2i, n+2-4i\},\ 1 \le i \le (n-4)/8, \tag{3.5}$$

and let C_d be the set of the following $(n-4)/32$ centered codewords:

$$\{0, n/4+3-4i, n/2+6-8i\},\ 1 \le i \le (n-4)/32. \tag{3.6}$$

Then it is easy to verify that

$\Delta_2(C_o) = \{2i-1 : (n+4)/8+1 \le i \le n/4\} \cup \{4i-2 : (n+4)/8+1 \le i \le n/4\}$

$\Delta_2(C_d) = \{4i : (n+28)/32+1 \le i \le (n-4)/16\} \cup \{8i : (n+28)/32+1 \le i \le (n-4)/16\}$.

Next, let N_{od} be the set of the following $(n-4)/16$ non-centered codewords:

$$\{0, n/4+2-4i, n/2+2-8i\},\ 1 \le i \le (n-4)/32; \tag{3.7}$$

$$\{0, a_i, b_i\} \text{ or } \{0, a_i, a_i+b_i\},\ 1 \le i \le (n-4)/32, \tag{3.8}$$

where $\{(a_i, b_i) : 1 \le i \le (n-4)/32\}$ is an $\mathcal{O}_{(n-4)/32}$. The choice between $\{0, a_i, b_i\}$ or $\{0, a_i, a_i+b_i\}$ depends on how a_i and b_i give rise to $4i$, i.e., if $b_i - a_i = 4i$, take $\{0, a_i, b_i\}$, and if $b_i + a_i = 4i$, take $\{0, a_i, a_i+b_i\}$. Then

$$\Delta_2(N_{od}) = \{2i-1 : 1 \le i \le (n-4)/8-1,\ i \ne (n+12)/16\}$$
$$\cup \{4i : 1 \le i \le (n-4)/32\} \cup \{8i-4 : (n+28)/32 \le i \le (n-4)/16\}.$$

Note that since $(n-4)/32 \equiv 0, 1 \pmod 4$ holds, Lemma 2.3 guarantees the existence of an $\mathcal{O}_{(n-4)/32}$.

Counting the number of codewords in the resulting code $\mathcal{C}$, we have

$$|\mathcal{C}| = \beta + |C_o| + |C_d| + |N_{od}| = 1 + \frac{n-4}{8} + \frac{n-4}{32} + \frac{n-4}{16} = \frac{7n+4}{32}.$$

Example 3.2. When $m = 16$, i.e., $n = 132$, $\alpha = 0$, $\beta = 1$,

$C_o = \{\{0, 65, 130\}, \{0, 63, 126\}, \{0, 61, 122\}, \{0, 59, 118\}, \{0, 57, 114\}, \{0, 55, 110\},$
$\{0, 53, 106\}, \{0, 51, 102\}, \{0, 49, 98\}, \{0, 47, 94\}, \{0, 45, 90\}, \{0, 43, 86\},$
$\{0, 41, 82\}, \{0, 39, 78\}, \{0, 37, 74\}, \{0, 35, 70\}\},$

$C_d = \{\{0, 32, 60\}, \{0, 28, 56\}, \{0, 24, 48\}, \{0, 20, 40\}\},$

$N_{od} = \{\{0, 31, 60\}, \{0, 27, 52\}, \{0, 23, 44\}, \{0, 19, 36\},$
$\{0, 11, 15\}, \{0, 3, 8\}, \{0, 1, 13\}, \{0, 7, 16\}\}.$

Construction 3.3. The case $m \equiv 8, 12 \pmod{16}$, i.e., $n \equiv 68, 100 \pmod{128}$. Let C_o be the set of $\{0, n/4-2, n/2-4\}$ and (3.5) for $1 \le i \le (n-4)/8-1$, C_d be the set of (3.6) just as it is, and N_{od} be the set of $\{0, n/4+2, n/2-6\}$,

(3.9) $$\{0, n/4+4-8i, n/2+2-16i\},\ 1 \le i \le \lfloor (n-4)/64 \rfloor;$$

(3.10) $$\{0, n/4+2-8i, n/2-6-16i\},\ 1 \le i \le \lceil (n-4)/64 \rceil - 1;$$

and (3.8) with an $((n+28)/32)$-ext $\mathcal{O}_{(n+28)/32}$ of defect

$$F = \begin{cases} \{(n-4)/8-1, (n+4)/8\} & \text{if } m \equiv 8 \pmod{16}, \\ \{(n-4)/8-3, (n+4)/8+2\} & \text{if } m \equiv 12 \pmod{16}. \end{cases}$$

Note that since $(n+28)/32 \equiv 3, 0 \pmod 4$, Lemma 2.5(3) and (1) assure the existence of the required odd sequences. Then we have $|\mathcal{C}| = (7n+4)/32$. Since the verification of $\Delta_2(\mathcal{C})$ is strightforward, we leave it to the reader.

Construction 3.4. The case $m \equiv 1 \pmod{12}$ and $m \ge 13$, i.e., $n \equiv 12 \pmod{96}$ and $n \ge 108$. Let C_o be the set of $\{0, n/6+1, n/3+2\}$ and (3.5) for $2 \le i \le (n-4)/8$ except $i = n/12+1$, and C_d be the set of the following $(n-12)/32$ centered codewords:

(3.11) $$\{0, n/4+1-4i, n/2+2-8i\},\ 1 \le i \le (n-12)/32.$$

Further let N_{od} be the set of

$$\{0, n/6-1, n/2-2\},\ \{0, n/4-2, n/2-1\},\ \{0, 2, c\},$$

where

$$c = \begin{cases} (n+4)/8+1 & \text{if } m \equiv 1, 37 \pmod{96}, \\ (n+4)/16+2 & \text{if } m \equiv 13 \pmod{96}, \\ (n-4)/8 & \text{if } m \equiv 25 \pmod{96}, \end{cases}$$

and

(3.12) $$\{0,\ n/4-4i, n/2-2-8i\},\ 1 \le i \le (n-12)/32-1,\ i \ne (n-12)/48,$$

and (3.8) for $1 \le i \le (n-12)/32$, where $\{(a_i, b_i) : 1 \le i \le (n-12)/32\}$ is an $\mathcal{O}_{(n-12)/32}$ if $m \equiv 1, 37 \pmod{96}$, and an $(n+20)/32$-ext $\mathcal{O}_{(n+20)/32}$ of defect

$$F = \begin{cases} \{(n+4)/16, (n+4)/16+2\} & \text{if } m \equiv 13 \pmod{96}, \\ \{(n-4)/8-2, (n-4)/8\} & \text{if } m \equiv 25 \pmod{96}. \end{cases}$$

It is easy to see that Lemmas 2.3, 2.5(1) and 2.5(3) guarantee the existence of the respective required sequences.

Counting the number of codewords in the resulting code $\mathcal{C}$, we have

$$|\mathcal{C}| = \alpha + \beta + |C_o| + |C_d| + |N_{od}| = 1 + 1 + \left(\frac{n-4}{8} - 1\right) + \frac{n-12}{32} + \frac{n+4}{16} = \frac{7n+12}{32}.$$

Construction 3.5. The case $m \equiv 5, 9 \pmod{12}$ and $m \geq 21$, i.e., $n \equiv 44, 76 \pmod{96}$ and $n \geq 172$. Let C_o be the set of $\{0, 6, 12\}$ and (3.5) for $1 \leq i \leq (n-4)/8$ and $i \neq 2$, and C_d be the set of (3.11) for $1 \leq i \leq (n-12)/32 - 2$. Further let N_{od} be the set of

$$\{0, c, n/2-2\}, \ \{0, 3, n/4+1\}, \ \{0, 8, n/4+13\},$$

(3.12) for $1 \leq i \leq (n-12)/32 - 1$, and (3.8) for $1 \leq i \leq (n+20)/32 + 1$ and $i \neq 2, 3$, where $c = 1$ or 5 depending on $m \equiv 5, 17, 21, 33 \pmod{48}$ or $m \equiv 9, 29, 41, 45 \pmod{48}$ respectively, and $\{(a_i, b_i) : 1 \leq i \leq (n+20)/32 + 1, \ i \neq 2, 3\}$ is a $\{2,3\}$-ext $\mathcal{O}_{(n+20)/32+1}$ of defect $\{c, 3, (n+4)/8+3, (n+4)/8+5\}$ whose existence is guaranteed by Lemma 2.10.

Counting the number of codewords in the resulting code $\mathcal{C}$, we have

$$|\mathcal{C}| = \beta + |C_o| + |C_d| + |N_{od}| = 1 + \frac{n-4}{8} + \left(\frac{n-12}{32} - 2\right) + \frac{n+4}{16} + 1 = \frac{7n-20}{32}.$$

Construction 3.6. The case $m \equiv 2, 6, 18, 38 \pmod{48}$ and $m \geq 6$, i.e., $n \equiv 20, 52, 148, 308 \pmod{384}$ and $n \geq 52$. Let C_o be the set of the $(n-4)/8$ centered codewords (3.5) just as they are, and C_d be the set of (3.6) for $1 \leq i \leq (n-20)/32 - 1$. Further let N_{od} be the set of $\{0, 8, n/4+11\}$, (3.7) for $1 \leq i \leq (n-20)/32$, and (3.8) for $1 \leq i \leq (n+12)/32+1$ and $i \neq 2$, where $\{(a_i, b_i) : 1 \leq i \leq (n+12)/32 + 1, \ i \neq 2\}$ is a 2-ext $\mathcal{O}_{(n+12)/32+1}$ of defect $\{(n+4)/8+2, (n+4)/8+4\}$ whose existence is guaranteed by Lemma 2.7(3) since $(n+12)/32 + 1 \equiv 2, 3 \pmod{4}$.

Counting the number of codewords in the resulting code $\mathcal{C}$, we have

$$|\mathcal{C}| = \beta + |C_o| + |C_d| + |N_{od}| = 1 + \frac{n-4}{8} + \left(\frac{n-20}{32} - 1\right) + \frac{n+12}{16} = \frac{7n-12}{32}.$$

Construction 3.7. The case $m \equiv 14, 26, 30, 42 \pmod{48}$, i.e., $n \equiv 116, 212, 244, 340 \pmod{384}$. Let C_o be the set of $\{0, n/4-2, n/2-4\}$ and (3.5) for $1 \leq i \leq (n-4)/8 - 1$, and C_d be the set of (3.6) for $1 \leq i \leq (n-20)/32 - 1$. Further let N_{od} be the set of $\{0, 8, n/4+11\}$, $\{0, n/4+2, n/2-6\}$, (3.9) for $1 \leq i \leq \lfloor (n-20)/64 \rfloor$, (3.10) for $1 \leq i \leq \lfloor (n-20)/64 \rfloor - 1$, and (3.8) for $1 \leq i \leq (n+12)/32+1$ and $i \neq 2$, where $\{(a_i, b_i) : 1 \leq i \leq (n+12)/32+1,\ i \neq 2\}$ is a 2-ext $\mathcal{O}_{(n+12)/32+1}$ of defect

$$F = \begin{cases} \{(n+4)/8, (n+4)/8+2\} & \text{if } m \equiv 26, 42 \pmod{48}, \\ \{(n+4)/8-2, (n+4)/8+4\} & \text{if } m \equiv 14, 30 \pmod{48}. \end{cases}$$

Note that since $(n+12)/32+1 \equiv 0, 1 \pmod 4$, Lemma 2.7(1) and (2) guarantee the existence of the required odd sequences. Then we have $|\mathcal{C}| = (7n-12)/32$.

Construction 3.8. The case $m \equiv 22, 34 \pmod{48}$, i.e., $n \equiv 180, 276 \pmod{384}$. Let C_o be the set of $\{0, n/6+1, n/3+2\}$ and (3.5) except $i = n/12+1$, and C_d be the set of (3.11) for $1 \leq i \leq (n-20)/32$. Further let N_{od} be the set of $\{0, n/3-1, n/2-2\}$, (3.7) for $1 \leq i \leq (n+12)/32$ except $i = (n+12)/48$, and (3.8) for $1 \leq i \leq (n-20)/32$, where $\{(a_i, b_i) : 1 \leq i \leq (n-20)/32\}$ is an $\mathcal{O}_{(n-20)/32}$ whose existence is guaranteed by Lemma 2.3 since $(n-20)/32 \equiv 1, 0 \pmod 4$.

Counting the number of codewords in the resulting code $\mathcal{C}$, we have

$$|\mathcal{C}| = \alpha + \beta + |C_o| + |C_d| + |N_{od}| = 1 + 1 + \frac{n-4}{8} + \frac{n-20}{32} + \frac{n-4}{16} = \frac{7n+20}{32}.$$

Construction 3.9. The case $m \equiv 10, 46 \pmod{48}$ and $m \geq 46$, i.e., $n \equiv 84, 372 \pmod{384}$ and $n \geq 372$. Let C_o be the set of

$$\{0, n/6+1, n/3+2\}, \begin{cases} \{0, (n-4)/16+6, (n-4)/8+12\} & \text{if } m \equiv 10 \pmod{48}, \\ \{0, (n-4)/8-5, n/4-11\} & \text{if } m \equiv 46 \pmod{48}, \end{cases}$$

and (3.5) except

$$i = \begin{cases} (n+12)/32+3 \text{ and } n/12+1 & \text{if } m \equiv 10 \pmod{48}, \\ (n-4)/16-2 \text{ and } n/12+1 & \text{if } m \equiv 46 \pmod{48}, \end{cases}$$

and C_d be the set of

$$\{0, n/4-5-4i, n/2-10-8i\},\ 1 \leq i \leq (n-20)/32.$$

Further let N_{od} be the set of

$$\{0, n/3-1, n/2-2\}, \begin{cases} \{0, (n-4)/16-4, n/2-10\} & \text{if } m \equiv 10 \pmod{48}, \\ \{0, (n-4)/8-15, n/2-10\} & \text{if } m \equiv 46 \pmod{48}, \end{cases}$$

(3.7) for $1 \le i \le (n+12)/32$ except $i = (n+12)/48$, and (3.8) for $1 \le i \le (n-20)/32-1$, where $\{(a_i, b_i) : 1 \le i \le (n-20)/32-1\}$ is an $((n-20)/32)$-ext $\mathcal{O}_{(n-20)/32}$ of defect

$$F = \begin{cases} \{(n-4)/16-4, (n-4)/16+6\} & \text{if } m \equiv 10 \pmod{48}, \\ \{(n-4)/8-5, (n-4)/8-5\} & \text{if } m \equiv 46 \pmod{48}. \end{cases}$$

As shown in Lemma 2.5(2) and (3), such odd sequences do exist since $(n-20)/32 \equiv 2, 3 \pmod 4$. Then we have $|\mathcal{C}| = (7n+20)/32$.

Construction 3.10. The case $m \equiv 3 \pmod 4$ and $m \ge 11$, i.e., $n \equiv 28 \pmod{32}$ and $n \ge 92$. Let C_o be the set of $\{0, 6, 12\}$ and (3.5) for $1 \le i \le (n-4)/8$ except $i = 2$, and C_d be the set of (3.11) for $1 \le i \le (n-28)/32$. Further let N_{od} be the set of $\{0, c, n/2-2\}$, $\{0, 3, n/4+1\}$, (3.12) for $1 \le i \le (n-28)/32$, and (3.8) for $1 \le i \le (n+4)/32$ except $i = 3$, where $c = 1$ or 5 depending on $m \equiv 3, 15 \pmod{16}$ or $m \equiv 7, 11 \pmod{16}$ respectively, and $\{(a_i, b_i) : 1 \le i \le (n+4)/32,\ i \ne 3\}$ is a 3-ext $\mathcal{O}_{(n+4)/32}$ of defect $\{c, 3\}$ whose existence is guaranteed by Lemma 2.9.

Counting the number of codewords in the resulting code $\mathcal{C}$, we have

$$|\mathcal{C}| = \beta + |C_o| + |C_d| + |N_{od}| = 1 + \frac{n-4}{8} + \frac{n-28}{32} + \frac{n+4}{16} = \frac{7n-4}{32}.$$

Note that there are nine cases $(n = 12, 20, 28, 44, 60, 76, 84, 108, 140)$ to which Constructions 3.1–3.10 cannot be applied. This means that we still need to prove that those cases also satisfy Theorem 1.6 by presenting codewords specifically.

Since it is common to all the nine cases that the resulting code $\mathcal{C}$ contains $\{0, n/4, n/2\}$ and C_o is of form

$$C_o = \{\{0, n/2+1-2i, n+2-4i\} : 1 \le i \le (n-4)/8\}.$$

We will show that those remaining cases also meet the upper bound on $M(n)$ in Theorem 1.6. Specifically, $n = 12, 28, 44, 60, 76, 84, 108, 140$ are left behind. We construct them respectively.

(1) When $m = 1$, i.e., $n = 12$, $\alpha = 1$, $\beta = 1$,
$C_o = \{\{0, 5, 10\}$.

(2) $m = 2$, i.e., $n = 20$, $\alpha = 0$, $\beta = 1$,
$C_o = \{\{0, 13, 26\}, \{0, 11, 22\}, \{0, 9, 18\}\}$,
$C_d = \{\{0, 8, 16\}\}$,
$N_{od} = \{\{0, 1, 4\}\}$.

(3) $m = 5$, i.e., $n = 44$, $\alpha = 0$, $\beta = 1$,
$C_o = \{\{0, 21, 42\}, \{0, 19, 38\}, \{0, 17, 34\}\{0, 15, 30\}\}$,
$C_d = \{\{0, 8, 16\}\}$,
$N_{od} = \{\{0, 1, 4\}, \{0, 5, 12\}\}$.

(4) $m = 7$, i.e., $n = 60$, $\alpha = 1$, $\beta = 1$,
$C_o = \{\{0, 29, 58\}, \{0, 27, 54\}, \{0, 25, 50\}, \{0, 23, 46\}, \{0, 21, 42\}, \{0, 19, 38\}, \{0, 17, 34\}\}$,
$C_d = \{\{0, 8, 16\}\}$,
$N_{od} = \{\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}\}$.

(5) $m = 9$, i.e., $n = 76$, $\alpha = 0$, $\beta = 1$,
$C_o = \{\{0, 37, 74\}, \{0, 35, 70\}, \{0, 33, 66\}, \{0, 31, 62\}, \{0, 29, 58\}, \{0, 27, 54\}$,
$\{0, 25, 50\}, \{0, 23, 46\}, \{0, 21, 42\}\}$,
$C_d = \{\{0, 8, 16\}, \{0, 28, 56\}\}$,
$N_{od} = \{\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}, \{0, 15, 32\}\}$.

(6) $m = 10$, i.e., $n = 84$, $\alpha = 1$, $\beta = 1$,
$C_o = \{\{0, 41, 82\}, \{0, 39, 78\}, \{0, 37, 74\}, \{0, 35, 70\}, \{0, 33, 66\}, \{0, 31, 62\}$,
$\{0, 29, 58\}, \{0, 27, 54\}, \{0, 25, 50\}, \{0, 23, 46\}\}$,
$C_d = \{\{0, 40, 80\}, \{0, 36, 72\}\}$,
$N_{od} = \{\{0, 3, 8\}, \{0, 7, 16\}, \{0, 11, 24\}, \{0, 15, 32\}, \{0, 1, 20\}\}$.

(7) $m = 13$, i.e., $n = 108$, $\alpha = 1$, $\beta = 1$,
$C_o = \{\{0, 53, 106\}, \{0, 51, 102\}, \{0, 49, 98\}, \{0, 47, 94\}, \{0, 45, 90\}, \{0, 43, 86\}$,
$\{0, 41, 82\}, \{0, 39, 78\}, \{0, 37, 74\}, \{0, 35, 70\}, \{0, 33, 66\}, \{0, 31, 62\}, \{0, 29, 58\}\}$,
$C_d = \{\{0, 8, 16\}, \{0, 28, 56\}, \{0, 44, 88\}\}$,
$N_{od} = \{\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}, \{0, 15, 32\}, \{0, 19, 40\}, \{0, 23, 48\}\}$.

(8) $m = 17$, i.e., $n = 140$, $\alpha = 0$, $\beta = 1$,
$C_o = \{\{0, 69, 138\}, \{0, 67, 134\}, \{0, 65, 130\}, \{0, 63, 126\}, \{0, 61, 122\}, \{0, 59, 118\}$,
$\{0, 57, 114\}, \{0, 55, 110\}, \{0, 53, 106\}, \{0, 51, 102\}, \{0, 49, 98\}, \{0, 47, 94\}, \{0, 45, 90\}$,
$\{0, 43, 86\}, \{0, 41, 82\}, \{0, 39, 78\}, \{0, 37, 74\}\}$,
$C_d = \{\{0, 8, 16\}, \{0, 36, 72\}, \{0, 44, 88\}, \{0, 60, 120\}\}$,
$N_{od} = \{\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}, \{0, 15, 32\}, \{0, 19, 40\}\}, \{0, 23, 48\}, \{0, 27, 56\}, \{0, 31, 64\}\}$.

4 Conclusion

By using a class of newly constructed special sequences, extended odd sequence with doubly even integers latently, we are able to obtain an optimal CAC(n) with weight three for each $n \equiv 4, 12 \pmod{16}$. Now, combining this result with known results on constructing optimal CAC's with weight three, the spectrum of the size of optimal CAC's of even length with weight three is completely settled. Unfortunately, the case when n is odd and weight three is still very far from being solved. We believe Algebra and Number theory are going to play important roles in tackling this part. Hopefully, this can be done in near future.

References

[1] L. A. Bassalygo and M. S. Pinsker, "Limited multiple-access of a nonsynchronous channel," (in Russian) *Probl. Inf. Transm.*, vol. 19, no. 4, pp. 92–96, 1983.

[2] C. J. Colbourn, J. H. Dinitz and D. R. Stinson, "Applications to communications, cryptography, and networking," in *London Math. Soc. Lecture Note*, ser. 267, J. D. Lamb and D. A. Preece, Eds. Cambridge Univ. Press, 1999, pp. 37–100.

[3] L. Györfi and I. Vajda, "Constructions of protocol sequences for multiple access collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. 39, no. 5,(1993), pp. 1762–1765, Sep. 1993.

[4] M. Jimbo, M. Mishima, S. Janiszewski, A. Y. Teymorian and V. D. Tonchev, "On conflict-avoiding codes of length $n = 4m$ for three active users, " *IEEE Trans. Inform. Theory*, vol. 53, no. 8, pp. 2732–2742, 2007.

[5] V. I. Levenshtein, "Conflict-avoiding codes for three active users and cyclic triple systems," *Probl. Inf. Transm.*, vol. 43, no. 3, pp. 199–212, 2007.

[6] V. I. Levenshtein and V. D. Tonchev, "Optimal conflict-avoiding codes for three active users," *Proc. IEEE Int. Symp. Inform. Theory*, Adelaide, Australia, pp. 535–537, Sep. 2005.

[7] J. L. Massey and P. Mathys, "The collision channel wihout feedback," *IEEE Trans. Ifrom. Theory*, vol. IT-31, no. 2 (1985), pp. 192–204, Mar. 1985.

[8] P. Mathys, "A class of codes for a T active users out of N multiple-access communication system," *IEEE Trans. Infrom. Theory*, vol. 36, no. 6, pp. 1206–1219, Nov. 1990.

[9] M. Mishima, H.-L. Fu and S. Uruno, "Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3," *Des. Codes Cryptogr.*, vol. 52, no. 3, pp. 275–291, Sep. 2009.

[10] K. Momihara, "Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three," *Des. Codes Cryptogr.*, vol. 45, no. 3, pp. 379–390, Dec. 2007.

[11] K. Momihara, M. Müller, J. Satoh and M. Jimbo, "Constant weight conflict-avoiding codes," *SIAM J. Discrete Math.*, vol. 21, no. 4, pp. 959–979, 2007.

[12] Q. A. Nguyen, L. Györfi and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 940–949, May 1992.

[13] B. S. Tsybakov and A. R. Rubinov, "Some constructions of conflict-avoiding codes," *Probl. Inf. Transm.*, vol. 38, no. 4, pp. 268–279, 2002.