Optimal Conflict-Avoiding Codes of Even Length and Weight 3

Hung-Lin Fu, Yi-Hean Lin, and Miwako Mishima

***Abstract*—Direct constructions for optimal conflict-avoiding codes of length $n \equiv 4 \pmod 8$ and weight 3 are provided by bringing in a new concept called an extended odd sequence. Constructions for those odd sequences are also given in this paper. As a consequence, with previously known results, the spectrum of the size of optimal conflict-avoiding codes of even length and weight 3 is completely settled.**

***Index Terms*—Conflict-avoiding codes, extended odd sequences.**

I. Introduction

FOR a subset A of $\mathbb{Z}_n$, define the difference set of A to be the multiset

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

A *conflict-avoiding code* (CAC) of length n and weight k is a collection $\mathcal{C}$ of k-subsets, called *codewords*, of $\mathbb{Z}_n$ such that

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

Two codewords are said to be *equivalent* if $\Delta(A) = \Delta(B)$. Therefore, without loss of generality, we usually consider $0 \in A$ for every codeword A in a 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 as

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

instead of $\Delta(A)$. Note that $\Delta(A)$ is a multiset, but $\Delta_2(A)$ is not. We also use the notation $\Delta_2(\mathcal{C})$ to denote $\cup_{A \in \mathcal{C}} \Delta_2(A)$.

Example 1.1: Suppose that $A = \{0, 3, 6\}$ and $B = \{0, 1, 21\}$ are codewords of a conflict-avoiding code of length 48. In this case

$$\begin{aligned} \Delta(A) &= \{3, 3, 6, 42, 45, 45\}, \\ \Delta_2(A) &= \{3, 6\}, \\ \Delta(B) &= \{1, 20, 21, 27, 28, 47\}, \\ \Delta_2(B) &= \{1, 20, 21\}. \end{aligned}$$

Manuscript received March 01, 2010. Date of current version October 20, 2010. The work of H.-L. Fu was supported in part by the NSC under Grant 97-2115-M-009-011-MY3, and the work of M. Mishima was supported in part by JSPS Scientific Research under Grant-in-Aid for Scientific Research (B)22340016.

H.-L. Fu and Y.-H. Lin are with the Department of Applied Mathematics, National Chiao Tung University, Hsin Chu, Taiwan 30050 (e-mail: hlfu@math.nctu.edu.tw; leona.am96g@math.nctu.edu.tw).

M. Mishima is with the Department of Information Science, Gifu University, Gifu 501-1193, Japan (e-mail: miwako@gifu-u.ac.jp).

Communicated by N. Kashyap, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2010.2069270

Let x_A be the binary vector representation of a codeword A and $x_A(i)$ be the ith component of x_A for $i = 0, 1, \ldots, n-1$, i.e., $x_A(i) = 1$ if $i \in A$, otherwise $x_A(i) = 0$. Then the definition of a CAC can be restated in terms of Hamming crosscorrelation H_{x_A, x_B} as follows: for any pair of distinct codewords A and B in a CAC of length n

$$H_{x_A, x_B}(\tau) = \sum_{i=0}^{n-1} x_A(i) x_B(i + \tau) \leq 1$$

independently of a relative delay offset τ. In fact, $H_{x_A, x_B}(\tau) \geq 2$ for some τ means that there exists at least one pair of distinct coordinates i and j such that

$$x_A(i) = x_B(i + \tau) = x_A(j) = x_B(j + \tau) = 1$$

which implies that $0 \neq j - i \in \Delta(A) \cap \Delta(B)$. A conflict-avoiding code of length n and weight k can be viewed as an $(n, k, 1)$ optical orthogonal code leaving the Hamming autocorrelation H_{x_A, x_A} out of consideration for all $A \in \mathcal{C}$. For the definition and some results of optical orthogonal codes, see, for example, [3] and its references.

Conflict-avoiding codes have been studied as protocol sequences for a multiple-access channel (collision channel) without feedback ([4], [6], [7], [9], [13], [14]). In such a multiple-access channel model ([2], [8]), the time axis is partitioned into slots whose duration corresponds to the transmission time for one packet, and being time-synchronized, multiple users share a common channel. In a particular time slot, if none of the users (senders) sends 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 sends a packet in a time slot, then the packet is transmitted successfully and the channel output in that slot is this packet value. If more than one users transmit packets in the same time slot simultaneously, then there occurs a conflict and the channel output in that slot is the collision symbol (see Fig. 1). There is no feedback available to inform the senders of the channel outputs in previous slots.

Each user is statically assigned a protocol sequence, which is a binary sequence of length n. Suppose that a user becomes active at time T after a certain duration (at least $n - 1$ time slots) of being inactive. Note that since the users can become active at different times, at least $n - 1$ silent slots are necessary for the receiver to synchronize the session of the sender without any assumption other than slot-synchronization, which is a major difference from the synchronizing technique of optical orthogonal codes. Using his/her assigned protocol sequence periodically until there are no more packets to send, the user transmits a packet in a time slot $T + i$ if the ith component of the protocol sequence is 1, or the silence symbol if it is 0. This means that

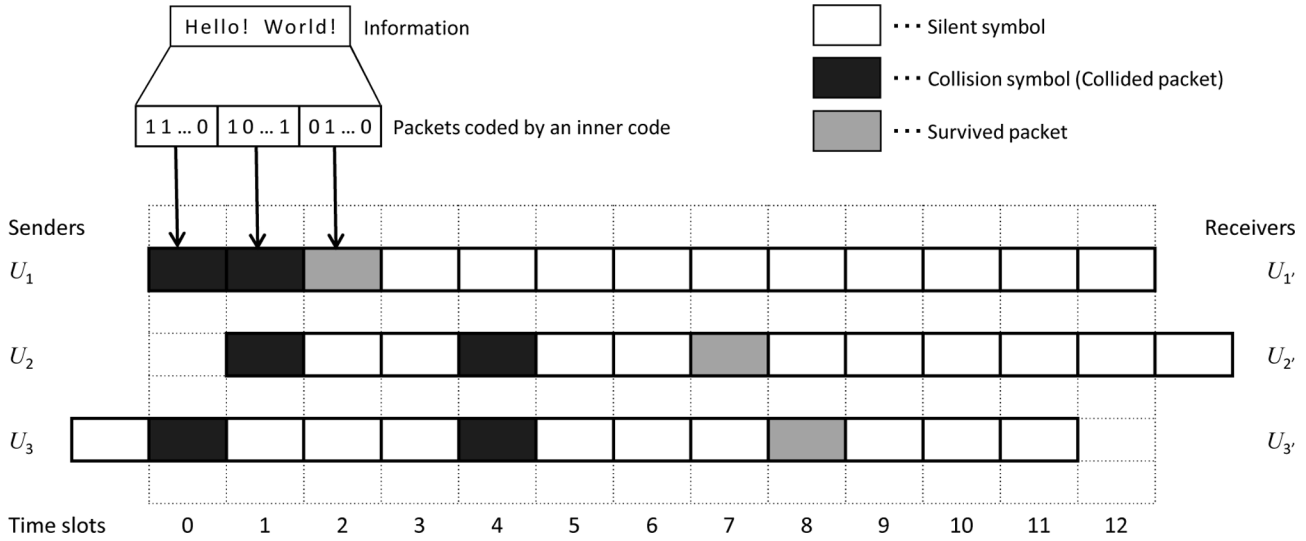

Fig. 1. A multiple-access channel model.

a user assigned a protocol sequence of Hamming weight w can send w packets in each frame of n slots.

The set $\mathcal{X}$ of N binary sequences is said to be an (N,k,n,σ) protocol sequence set if any $x \in \mathcal{X}$ 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. For a binary sequence $x \in \mathcal{X}$ of weight w, a $(w,\sigma,w-\sigma+1)$ shortened Reed–Solomon (RS) code is proposed as an inner code to code σ information packets into w transmitted packets (see [4] and [13]), by which at most $w-\sigma$ packet erasures due to collision can be recovered from σ survived packets. Since it is not the objective of this paper, we do not go any further into inner codes.

In order to support k active users, i.e., in order to guarantee that each of arbitrary k active users can successfully send at least one packet without suffering from collision, the weight w of an $(N,k,n,1)$ protocol sequence set cannot be less than the number of active users k. In this sense, a conflict-avoiding code of length n and weight k is considered as an $(N,k,n,1)$ protocol sequence set of constant (and minimum possible) weight k.

Throughout this paper, we use the subset representation of $\mathbb{Z}_n$ to denote codewords in a CAC, instead of binary sequences of length n. Let $\mathrm{CAC}(n,k)$ be the class of all the CACs of length n and weight 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 is of form

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

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

The maximum size of 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 $|\mathcal{C}| = M(n,k)$. Since this article treats only the case $k=3$, we write, for simplicity, $\mathrm{CAC}(n,3)$ and $M(n,3)$ just as $\mathrm{CAC}(n)$ and $M(n)$, respectively.

Levenshtein and Tonchev [7] derived the following upper bound on $M(n)$:

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

and further proved that

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

Jimbo *et al.* [5] 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. [5]): 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.* [5]. Partition integers not exceeding $n/2$ into the following three subsets:

$$\begin{aligned} O &= \{i : i \equiv 1 \pmod 2,\ 1 \le i \le n/2\}, \\ E &= \{i : i \equiv 2 \pmod 4,\ 1 \le i \le n/2\}, \\ D &= \{i : i \equiv 0 \pmod 4,\ 1 \le i \le n/2\}. \end{aligned}$$

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 [5]: 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 $i \neq n/3$, 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 [5]: Any noncentered 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 [5], 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 noncentered 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:

$$\alpha = \begin{cases} 1, & \text{if } \{0, n/3, 2n/3\} \in \mathcal{C}, \\ 0, & \text{otherwise,} \end{cases}$$
$$\beta = \begin{cases} 1, & \text{if } \{0, n/4, n/2\} \in \mathcal{C}, \\ 0, & \text{otherwise.} \end{cases}$$

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

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

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

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

where

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

For the conditions (1.3) and (1.4), see [5, Sec. II]. The technique for solving the LP problem is also demonstrated in [5] (and [10]).

In [5] Jimbo *et al.* further proved that the upper bounds in Theorem 1.2 are strict if $t \equiv 2 \pmod 4$, i.e., $n \equiv 8 \pmod{16}$ [5, Th. 3.1]. Recently, Mishima *et al.* [10] 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. [10]): 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 article, the necessary and sufficient condition to satisfy $M(n) = (n-1)/4$ or $(n+1)/4$ can be found in [11], but known results on $M(n)$ for odd n are very few so far.

In this paper, in order to prove Theorem 1.6, we bring in a new concept called an "extended odd sequence." Those series of extended odd sequences that are required in our constructions for optimal CACs are also given.

II. Extended Odd Sequences

Mishima *et al.* [10] used Skolem type sequences effectively in the proof of Theorem 1.5 and with those sequences, they also gave a simpler proof of [5, Th. 3.1] than the original one. Unfortunately, the Skolem type sequences used in [10] to prove the strictness 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 $\mathrm{CAC}(n)$.

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

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

with

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

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

We should remark that Baker [1, Lemma 2] used almost the same notation such as 3-ext $\mathcal{O}_{4s+1}$ (or equivalently 5-ext $\mathcal{O}_{4s+1}$) to denote a sequence of $4s+3$ integers with a different property from Definition 2.1.

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 $\mathcal{O}_s$ if $s\equiv 0,1 \pmod 4$.

Proof: The proof is divided into two cases.

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

$$\begin{aligned}
&4 \text{ in } (3s-3,3s+1);\\
&8+8i \text{ in } (2s-7-4i,2s+1+4i),\ 0\le i\le s/4-2;\\
&12+8i \text{ in } (2s-5-4i,2s+7+4i),\ 0\le i\le s/4-2;\\
&2s \text{ in } (3,2s+3);\\
&4s-8-4i \text{ in } (5+2i,4s-3-2i),\ 0\le i\le s/2-3;\\
&4s-4 \text{ in } (2s-3,2s-1);\\
&4s \text{ in } (1,4s-1).
\end{aligned}$$

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

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

$$\begin{aligned}
&2s-2 \text{ in } (2s+1,4s-1);\\
&4s \text{ in } (3,4s-3).
\end{aligned}$$

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

Lemma 2.4: There exists an s-ext $\mathcal{O}_s$ of defect F if

1) $s\equiv 0 \pmod 4$ and $F\in\{\{2s-1,2s+1\},\{4s-7,4s-1\}$.
2) $s\equiv 2 \pmod 4$, $s\ge 6$ and $F=\{2s-3,2s+7\}$, and
3) $s\equiv 3 \pmod 4$ and $F\in\{\{4s-13,4s-3\},\{4s-5,4s-3\}\}$.

Proof:

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

$$\begin{aligned}
&4 \text{ in } (3s-5,3s-1);\\
&8+8i \text{ in } (2s-3-4i,2s+5+4i),\ 0\le i\le s/2-2;\\
&12+8i \text{ in } (2s-9-4i,2s+3+4i),\ 0\le i\le s/4-3;\\
&2s-4 \text{ in } (1,2s-5);\\
&4s-4-8i \text{ in } (3+4i,4s-1-4i),\ 0\le i\le s/4-1.
\end{aligned}$$

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

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

$$\begin{aligned}
&4 \text{ in } (s-1,s+3);\\
&8+8i \text{ in } (2s-1-4i,2s+7+4i),\\
&\qquad 0\le i\le s/4-2;\\
&12+8i \text{ in } (2s-11-4i,2s+1+4i),\\
&\qquad 0\le i\le s/2-3;\\
&4s-8-8i \text{ in } (3+4i,4s-5-4i),\\
&\qquad 0\le i\le s/4-2;\\
&2s \text{ in } (2s-3,4s-3);\\
&4s-4 \text{ in } (2s-7,2s+3).
\end{aligned}$$

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

$$\begin{aligned}
&4 \text{ in } (s+1,s+5);\\
&8+8i \text{ in } (2s+3-4i,2s+11+4i),\\
&\qquad 0\le i\le (s-2)/4-1;\\
&12+8i \text{ in } (2s-7-4i,2s+5+4i),\\
&\qquad 0\le i\le s/2-2;\\
&4s-8-8i \text{ in } (7+4i,4s-1-4i),\\
&\qquad 0\le i\le (s-2)/4-2;\\
&2s+4 \text{ in } (3,2s+1).
\end{aligned}$$

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

$$\begin{aligned}
&4 \text{ in } (s-4,s);\\
&8 \text{ in } (4s-9,4s-1);\\
&12+8i \text{ in } (2s-9-4i,2s+3+4i),\\
&\qquad 0\le i\le (s-1)/2-2;\\
&16+8i \text{ in } (2s-11-4i,2s+5+4i),\\
&\qquad 0\le i\le (s-3)/4-3;\\
&4s-20-8i \text{ in } (3+4i,4s-17-4i),\\
&\qquad 0\le i\le (s-3)/4-2;\\
&2s-6 \text{ in } (2s+1,4s-5);\\
&4s-12 \text{ in } (2s-7,2s-5);\\
&4s-4 \text{ in } (2s-3,2s-1).
\end{aligned}$$

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

$$\begin{aligned} 4 \text{ in } (3s-4, 3s);\\ 8+8i \text{ in } (2s-9-4i, 2s-1+4i),\\ 0 \leq i \leq (s-3)/4-1;\\ 12+8i \text{ in } (2s-7-4i, 2s+5+4i),\\ 0 \leq i \leq (s-1)/2-3;\\ 4s-12-8i \text{ in } (5+4i, 4s-7-4i),\\ 0 \leq i \leq (s-3)/4-2;\\ 2s+2 \text{ in } (1, 2s+1);\\ 4s-8 \text{ in } (2s-5, 2s-3);\\ 4s-4 \text{ in } (3, 4n-1). \end{aligned}$$

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

■

Lemma 2.5: There exists a 2-ext $\mathcal{O}_s$ of defect F if
1) $s \equiv 0 \pmod 4$ and $F = \{4s-5, 4s-3\}$,
2) $s \equiv 1 \pmod 4$, $s \geq 5$ and $F = \{4s-7, 4s-1\}$, and
3) $s \equiv 2,3 \pmod 4$ and $F = \{4s-3, 4s-1\}$.

Proof:

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

$$\begin{aligned} 4 \text{ in } (3s-11, 3s-7);\\ 12+8i \text{ in } (2s-11-4i, 2s+1+4i),\\ 0 \leq i \leq s/4-3;\\ 16+8i \text{ in } (2s-9-4i, 2s+7+4i),\\ 0 \leq i \leq s/2-4;\\ 4s-12-8i \text{ in } (5+4i, 4s-7-4i),\\ 0 \leq i \leq s/4-2;\\ 2s-4 \text{ in } (3, 2s-1);\\ 4s-8 \text{ in } (2s-5, 2s-3);\\ 4s-4 \text{ in } (2s-7, 2s+3);\\ 4s \text{ in } (1, 4s-1). \end{aligned}$$

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

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

$$\begin{aligned} 2s-6 \text{ in } (2s-3, 4s-9);\\ 4s \text{ in } (3, 4s-3). \end{aligned}$$

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

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

$$\begin{aligned} 4 \text{ in } (3s-3, 3s+1);\\ 12+8i \text{ in } (2s-11-4i, 2s+1+4i),\\ 0 \leq i \leq s/2-3;\\ 16+8i \text{ in } (2s-9-4i, 2s+7+4i),\\ 0 \leq i \leq (s-2)/4-3;\\ 4s-16-8i \text{ in } (11+4i, 4s-5-4i),\\ 0 \leq i \leq (s-2)/4-2;\\ 2s-4 \text{ in } (3, 2s-1);\\ 4s-8 \text{ in } (2s-5, 2s-3);\\ 4s-4 \text{ in } (2s-7, 2s+3);\\ 4s \text{ in } (7, 4s-7). \end{aligned}$$

If $s = 6$, $\{(7,11),(5,17),(3,13),(1,19),(9,15)\}$ is a 2-ext $\mathcal{O}_6$ of defect $\{21,23\}$. If $s = 2$, $\{(1,3)\}$ is a 2-ext $\mathcal{O}_2$ of defect $\{5,7\}$.
The case $s \equiv 3 \pmod 4$. If $s \geq 7$, put doubly even integers as follows:

$$\begin{aligned} 4 \text{ in } (s-2, s+2);\\ 12+8i \text{ in } (2s-5-4i, 2s+7+4i),\\ 0 \leq i \leq (s-3)/4-2;\\ 16+8i \text{ in } (2s-11-4i, 2s+5+4i),\\ 0 \leq i \leq (s-1)/2-3;\\ 4s-8-8i \text{ in } (1+4i, 4s-7-4i),\\ 0 \leq i \leq (s-3)/4-1;\\ 2s-2 \text{ in } (2s-3, 4s-5);\\ 4s-4 \text{ in } (2s-7, 2s+3);\\ 4s \text{ in } (2s-1, 2s+1). \end{aligned}$$

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

■

Lemma 2.6: There exists a 3-ext $\mathcal{O}_s$ of defect F if
1) $s \equiv 0,1 \pmod 4$, $s \geq 4$ and $F = \{1,3\}$, and
2) $s \equiv 2,3 \pmod 4$, $s \geq 3$ and $F = \{3,5\}$.

Proof:

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

$$\begin{aligned} 4 \text{ in } (3s+1, 3s+5);\\ 8 \text{ in } (2s+3, 2s+11);\\ 16+8i \text{ in } (2s-11-4i, 2s+5+4i),\\ 0 \leq i \leq s/4-2;\\ 20+8i \text{ in } (2s-5-4i, 2s+15+4i),\\ 0 \leq i \leq s/2-4;\\ 4s-8-8i \text{ in } (5+4i, 4s-3-4i),\\ 0 \leq i \leq s/4-3;\\ 2s+8 \text{ in } (7, 2s+1);\\ 4s-4 \text{ in } (2s-3, 2s-1);\\ 4s \text{ in } (2s-7, 2s+7). \end{aligned}$$

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

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

$$\begin{aligned}
4 &\text{ in } (3s, 3s+4);\\
8 &\text{ in } (2s-3, 2s+5);\\
16+8i &\text{ in } (2s-5-4i, 2s+11+4i),\\
&\quad 0 \leq i \leq (s-1)/2-3;\\
20+8i &\text{ in } (2s-11-4i, 2s+9+4i),\\
&\quad 0 \leq i \leq (s-1)/4-3;\\
4s-8-8i &\text{ in } (7+4i, 4s-1-4i),\\
&\quad 0 \leq i \leq (s-1)/4-2;\\
2s+2 &\text{ in } (5, 2s+7);\\
4s-4 &\text{in } (2s-7, 2s+3);\\
4s &\text{ in } (2s-1, 2s+1).
\end{aligned}$$

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

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

$$\begin{aligned}
4 &\text{ in } (3s+1, 3s+5);\\
8 &\text{ in } (2s+1, 2s+9);\\
16+8i &\text{ in } (2s-9-4i, 2s+7+4i),\\
&\quad 0 \leq i \leq (s-2)/4-2;\\
20+8i &\text{ in } (2s-7-4i, 2s+13+4i),\\
&\quad 0 \leq i \leq s/2-4;\\
4s-8-8i &\text{ in } (7+4i, 4s-1-4i),\\
&\quad 0 \leq i \leq (s-2)/4-2;\\
2s+4 &\text{ in } (1, 2s+3);\\
4s-4 &\text{ in } (2s-3, 2s-1);\\
4s &\text{ in } (2s-5, 2s+5).
\end{aligned}$$

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

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

$$\begin{aligned}
4 &\text{ in } (3s+2, 3s+6);\\
8 &\text{ in } (2s-3, 2s+5);\\
16+8i &\text{ in } (2s-5-4i, 2s+11+4i),\\
&\quad 0 \leq i \leq (s-1)/2-3;\\
20+8i &\text{ in } (2s-11-4i, 2s+9+4i),\\
&\quad 0 \leq i \leq (s-3)/4-2;\\
4s-8-8i &\text{ in } (7+4i, 4s-1-4i),\\
&\quad 0 \leq i \leq (s-3)/4-2;\\
2s+6 &\text{ in } (1, 2s+7);\\
4s-4 &\text{ in } (2s-7, 2s+3);\\
4s &\text{ in } (2s-1, 2s+1).
\end{aligned}$$

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

Lemma 2.7: There exists a $\{2,3\}$-ext $\mathcal{O}_s$ of defect F if

1) $s \equiv 0,1 \pmod 4$, $s\geq 8$ and $F=\{3,5,4s-3,4s-1\}$, and
2) $s \equiv 2,3 \pmod 4$, $s\geq 7$ and $F=\{1,3,4s-3,4s-1\}$.

Proof:

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

$$\begin{aligned}
4 &\text{ in } (3s-1, 3s+3);\\
16+8i &\text{ in } (2s-7-4i, 2s+9+4i),\\
&\quad 0 \leq i \leq s/2-4;\\
20+8i &\text{ in } (2s-13-4i, 2s+7+4i),\\
&\quad 0 \leq i \leq s/4-3;\\
4s-12-8i &\text{ in } (7+4i, 4s-5-4i),\\
&\quad 0 \leq i \leq s/4-3;\\
2s+4 &\text{ in } (1, 2s+3);\\
4s-8 &\text{ in } (2s-5, 2s-3);\\
4s-4 &\text{ in } (2s-9, 2s+5);\\
4s &\text{ in } (2s-1, 2s+1).
\end{aligned}$$

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

$$\begin{aligned}
4 &\text{ in } (3s, 3s+4);\\
16+8i &\text{ in } (2s-11-4i, 2s+5+4i),\\
&\quad 0 \leq i \leq (s-1)/4-2;\\
20+8i &\text{ in } (2s-9-4i, 2s+11+4i),\\
&\quad 0 \leq i \leq (s-1)/2-4;\\
4s-12-8i &\text{ in } (7+4i, 4s-5-4i),\\
&\quad 0 \leq i \leq (s-1)/4-3;\\
2s+6 &\text{ in } (1, 2s+7);\\
4s-8 &\text{ in } (2s-5, 2s-3);\\
4s-4 &\text{ in } (2s-7, 2s+3);\\
4s &\text{ in } (2s-1, 2s+1).
\end{aligned}$$

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

$$\begin{aligned}
4 &\text{ in } (3s+1, 3s+5);\\
16+8i &\text{ in } (2s-7-4i, 2s+9+4i),\\
&\quad 0 \leq i \leq s/2-4;\\
20+8i &\text{ in } (2s-13-4i, 2s+7+4i),\\
&\quad 0 \leq i \leq (s-2)/4-2;\\
4s-12-8i &\text{ in } (7+4i, 4s-5-4i),\\
&\quad 0 \leq i \leq (s-2)/4-3;\\
2s+8 &\text{ in } (5, 2s+3);\\
4s-8 &\text{ in } (2s-5, 2s-3);\\
4s-4 &\text{ in } (2s-9, 2s+5);\\
4s &\text{ in } (2s-1, 2s+1).
\end{aligned}$$

TABLE I
SIZES OF SUBSETS OF CODEWORDS FOR AN OPTIMAL CODE IN $\mathrm{CAC}(n = 8m + 4)$

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	$(n-4)/8$	$(n-20)/32$	$(n-4)/16$	$(7n+20)/32$

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

$$\begin{aligned}
4 &\text{ in } (3s-2, 3s+2);\\
16+8i &\text{ in } (2s-11-4i, 2s+5+4i),\\
&\quad 0 \leq i \leq (s-3)/4-2;\\
20+8i &\text{ in } (2s-9-4i, 2s+11+4i),\\
&\quad 0 \leq i \leq (s-1)/2-4;\\
4s-12-8i &\text{ in } (7+4i, 4s-5-4i),\\
&\quad 0 \leq i \leq (s-3)/4-2;\\
2s+2 &\text{ in } (5, 2s+7);\\
4s-8 &\text{ in } (2s-5, 2s-3);\\
4s-4 &\text{ in } (2s-7, 2s+3);\\
4s &\text{ in } (2s-1, 2s+1).
\end{aligned}$$

■

III. CONSTRUCTIONS FOR OPTIMAL CACS

We will now present direct constructions for optimal codes in $\mathrm{CAC}(n = 8m + 4)$, which will eventually prove Theorem 1.6. The constructions are given for the following 10 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) $m \equiv 10 \pmod{48}$,
9) $m \equiv 46 \pmod{48}$, and
10) $m \equiv 3 \pmod 4$.

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

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:

$$\{0, n/2+1-2i, n+2-4i\}, 1 \leq i \leq (n-4)/8 \tag{3.1}$$

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

$$\{0, n/4+3-4i, n/2+6-8i\}, 1 \leq i \leq (n-4)/32. \tag{3.2}$$

Then it is easy to verify that

$$\begin{aligned}
\Delta_2(C_o) &= \{2i-1 : (n+4)/8+1 \leq i \leq n/4\}\\
&\quad \cup \{4i-2 : (n+4)/8+1 \leq i \leq n/4\}\\
\Delta_2(C_d) &= \{4i : (n+28)/32+1 \leq i \leq (n-4)/16\}\\
&\quad \cup \{8i : (n+28)/32+1 \leq i \leq (n-4)/16\}.
\end{aligned}$$

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

$$\{0, n/4+2-4i, n/2+2-8i\}, 1 \leq i \leq (n-4)/32; \tag{3.3}$$

$$\{0, a_i, b_i\} \text{ or } \{0, a_i, a_i+b_i\}, 1 \leq i \leq (n-4)/32 \tag{3.4}$$

where $\{(a_i, b_i) : 1 \leq i \leq (n-4)/32\}$ 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

$$\begin{aligned}
&\Delta_2(N_{od})\\
&\quad = \{2i-1 : 1 \leq i \leq (n-4)/8-1,\ i \neq (n+12)/16\}\\
&\qquad \cup \{4i : 1 \leq i \leq (n-4)/32\}\\
&\qquad \cup \{8i-4 : (n+28)/32 \leq i \leq (n-4)/16\}.
\end{aligned}$$

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

$$\begin{aligned}
\lvert\mathcal{C}\rvert &= \beta + \lvert C_o\rvert + \lvert C_d\rvert + \lvert N_{od}\rvert\\
&= 1 + \frac{n-4}{8} + \frac{n-4}{32} + \frac{n-4}{16} = \frac{7n+4}{32}.
\end{aligned}$$

Construction 3.2: 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 (3.1) for $1 \leq i \leq (n-4)/8-1$, C_d be the set of (3.2) just as it is, and N_{od} be the set of $\{0, n/4+2, n/2-6\}$,

$$\{0, n/4+4-8i, n/2+2-16i\}, 1 \leq i \leq \lfloor (n-4)/64 \rfloor; \tag{3.5}$$

$$\{0, n/4+2-8i, n/2-6-16i\}, 1 \leq i \leq \lceil (n-4)/64 \rceil - 1; \tag{3.6}$$

and (3.4), where $\{(a_i, b_i) : 1 \le i \le (n-4)/32\}$ is an $((n+28)/32)$-ext $\mathcal{O}_{(n+28)/32}$ of defect

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

Note that since $(n+28)/32 \equiv 3, 0 \pmod 4$, Lemma 2.4(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 straightforward, we leave it to the reader.

Construction 3.3: 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 (3.1) 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:

$$\{0, n/4+1-4i, n/2+2-8i\},\ 1 \le i \le (n-12)/32. \quad (3.7)$$

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

$$\{0, n/4-4i, n/2-2-8i\}, 1 \le i \le (n-12)/32-1, \\ i \ne (n-12)/48 \quad (3.8)$$

and (3.4) 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

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

It is easy to see that Lemmas 2.3, 2.4(1), and 2.4(3) guarantee the existence of the respective required sequences.

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

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

Construction 3.4: The case $m \equiv 5, 9 \pmod{12}$ and $m \ge 21$, i.e., $n \equiv 44, 76 \pmod{96}$ and $n \ge 172$. Let C_o be the set of $\{0, 6, 12\}$ and (3.1) for $1 \le i \le (n-4)/8$ except $i = 2$, and C_d be the set of (3.7) for $1 \le i \le (n-12)/32-2$. Further let N_{od} be the set of

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

(3.8) for $1 \le i \le (n-12)/32-1$, and (3.4) for $1 \le i \le (n+20)/32+1$ with $i \ne 2, 3$, 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 $\{(a_i, b_i) : 1 \le i \le (n+20)/32+1,\ i \ne 2, 3\}$ 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 2.7.

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

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

Construction 3.5: The case $m \equiv 2, 6, 18, 38 \pmod{48}$ and $m \ge 6$, i.e., $n \equiv 20, 52, 148, 308 \pmod{384}$ and $n \ge 52$. Let C_o be the set of the $(n-4)/8$ centered codewords (3.1) just as they are, and C_d be the set of (3.2) for $1 \le i \le (n-20)/32-1$. Further let N_{od} be the set of $\{0, 8, n/4+11\}$, (3.3) for $1 \le i \le (n-20)/32$, and (3.4) for $1 \le i \le (n+12)/32+1$ except $i = 2$, where $\{(a_i, b_i) : 1 \le i \le (n+12)/32+1,\ i \ne 2\}$ 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 2.5(3) since $(n+12)/32+1 \equiv 2, 3 \pmod 4$.

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

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

Construction 3.6: 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 (3.1) for $1 \le i \le (n-4)/8-1$, and C_d be the set of (3.2) for $1 \le i \le (n-20)/32-1$. Further let N_{od} be the set of $\{0, 8, n/4+11\}$, $\{0, n/4+2, n/2-6\}$, (3.5) for $1 \le i \le \lfloor (n-20)/64 \rfloor$, (3.6) for $1 \le i \le \lfloor (n-20)/64 \rfloor - 1$, and (3.4) for $1 \le i \le (n+12)/32+1$ except $i = 2$, where $\{(a_i, b_i) : 1 \le i \le (n+12)/32+1,\ i \ne 2\}$ is a 2-ext $\mathcal{O}_{(n+12)/32+1}$ of defect

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

Note that since $(n+12)/32+1 \equiv 0, 1 \pmod 4$, Lemma 2.5(1) and (2) guarantee the existence of the required odd sequences. Then we have $|\mathcal{C}| = (7n-12)/32$.

Construction 3.7: 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 (3.1) except $i = n/12+1$, and C_d be the set of (3.7) for $1 \le i \le (n-20)/32$. Further let N_{od} be the set of $\{0, n/3-1, n/2-2\}$, (3.3) for $1 \le i \le (n+12)/32$ except $i = (n+12)/48$, and (3.4) for $1 \le i \le (n-20)/32$, where $\{(a_i, b_i) : 1 \le i \le (n-20)/32\}$ is an $\mathcal{O}_{(n-20)/32}$ whose

TABLE II
ALL CODEWORDS OTHER THAN $\{0, n/3, 2n/3\}$ AND C_o IN OPTIMAL CACS OF SMALL CODE LENGTHS $n = 8m + 4$

m	n	$\{0, n/3, 2n/3\}$	C_d	N_{od}
1	12	$\{0, 4, 8\}$	-	-
2	20	-	-	$\{0, 1, 4\}$
3	28	-	$\{0, 8, 16\}$	$\{0, 1, 4\}$
5	44	-	$\{0, 8, 16\}$	$\{0, 1, 4\}, \{0, 5, 12\}$
7	60	$\{0, 20, 40\}$	$\{0, 8, 16\}$	$\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}$
9	76	-	$\{0, 8, 16\}, \{0, 28, 56\}$	$\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}, \{0, 15, 32\}$
10	84	$\{0, 28, 56\}$	$\{0, 36, 72\}, \{0, 40, 80\}$	$\{0, 3, 8\}, \{0, 7, 16\}, \{0, 11, 24\}, \{0, 15, 32\}, \{0, 1, 20\}$
13	108	$\{0, 36, 72\}$	$\{0, 8, 16\}, \{0, 28, 56\}, \{0, 44, 88\}$	$\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}, \{0, 15, 32\}, \{0, 19, 40\}, \{0, 23, 48\}$
17	140	-	$\{0, 8, 16\}, \{0, 36, 72\}, \{0, 44, 88\}, \{0, 60, 120\}$	$\{0, 1, 4\}, \{0, 5, 12\}, \{0, 11, 24\}, \{0, 15, 32\}, \{0, 19, 40\}, \{0, 23, 48\}, \{0, 27, 56\}, \{0, 31, 64\}$

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

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

Construction 3.8: The case $m \equiv 10 \pmod{48}$ and $m \geq 58$, i.e., $n \equiv 84 \pmod{384}$ and $n \geq 468$. Let C_o be the set of

$$\{0, (n-4)/16+6, (n-4)/8+12\}\{0, n/6+1, n/3+2\} \tag{3.9}$$

and (3.1) with $i \neq (n+12)/32+3$ and $n/12+1$, and C_d be the set of

$$\{0, n/4-5-4i, n/2-10-8i\},\ 1 \leq i \leq (n-20)/32. \tag{3.10}$$

Further let N_{od} be the set of

$$\{0, (n-4)/16-4, n/2-10\}, \{0, n/3-1, n/2-2\} \tag{3.11}$$

(3.3) for $1 \leq i \leq (n+12)/32$ except $i = (n+12)/48$, and (3.4) for $1 \leq i \leq (n-20)/32-1$, where $\{(a_i, b_i) : 1 \leq i \leq (n-20)/32-1\}$ is an $((n-20)/32)$-ext $\mathcal{O}_{(n-20)/32}$ of defect $\{(n-4)/16-4, (n-4)/16+6\}$. As shown in Lemma 2.4(2), such odd sequences do exist since $(n-20)/32 \equiv 2 \pmod 4$. Then we have $|\mathcal{C}| = (7n+20)/32$.

Construction 3.9: The case $m \equiv 46 \pmod{48}$ and $m \geq 46$, i.e., $n \equiv 372 \pmod{384}$ and $n \geq 372$. The construction is quite similar to Construction 3.8.

Let C_o be the set of

$$\{0, (n-4)/8-5, n/4-11\}$$

(3.9) and (3.1) with $i \neq (n-4)/16-2$ and $n/12+1$, and C_d be the set of (3.10). Further let N_{od} be the set of

$$\{0, (n-4)/8-15, n/2-10\}$$

(3.11), (3.3) for $1 \leq i \leq (n+12)/32$ except $i = (n+12)/48$, and (3.4) for $1 \leq i \leq (n-20)/32-1$, where $\{(a_i, b_i) : 1 \leq i \leq (n-20)/32-1\}$ is an $((n-20)/32)$-ext $\mathcal{O}_{(n-20)/32}$ of defect $\{(n-4)/8-15, (n-4)/8-5\}$ whose existence is assured by Lemma 2.4(3) since $(n-20)/32 \equiv 3 \pmod 4$. Then we have $|\mathcal{C}| = (7n+20)/32$.

Construction 3.10: The case $m \equiv 3 \pmod 4$ and $m \geq 11$, i.e., $n \equiv 28 \pmod{32}$ and $n \geq 92$. Let C_o be the set of $\{0, 6, 12\}$ and (3.1) for $1 \leq i \leq (n-4)/8$ except $i = 2$, and C_d be the set of (3.7) for $1 \leq i \leq (n-28)/32$. Further let N_{od} be the set of $\{0, c, n/2-2\}$, $\{0, 3, n/4+1\}$, (3.8) for $1 \leq i \leq (n-28)/32$, and (3.4) for $1 \leq i \leq (n+4)/32$ 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 $\{(a_i, b_i) : 1 \leq i \leq (n+4)/32,\ i \neq 3\}$ is a 3-ext $\mathcal{O}_{(n+4)/32}$ of defect $\{c, 3\}$ whose existence is guaranteed by Lemma 2.6.

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

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

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

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

we provide just the rest of the codewords for each case in Table II.

IV. CONCLUSION

By using a class of newly constructed special sequences, called extended odd sequences, an optimal CAC of length n and weight three has been obtained for any $n \equiv 4 \pmod 8$. Now, combining with previously known results on optimal CACs with weight three ([5], [7], [10]), the spectrum of the size of optimal CACs of even length and weight three is completely settled. Unfortunately, the case of odd code lengths n 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.

ACKNOWLEDGMENT

The authors would like to thank Prof. Navin Kashyap, the Associate Editor for Coding Theory, IEEE TRANSACTIONS ON INFORMATION THEORY, and anonymous reviewers for their careful reading. In particular, they are grateful to one of the reviewers for checking that the resulting codes are invariably conflict-avoiding by implementing a program of the constructions in Section III.

REFERENCES

[1] C. A. Baker, "Extended Skolem sequences," *J. Combin. Des.*, vol. 3, no. 5, pp. 363–379, 1995.

[2] L. A. Bassalygo and M. S. Pinsker, "Limited multiple-access of a non-synchronous channel," *Probl. Inf. Transm.*, vol. 19, no. 4, pp. 92–96, 1983.

[3] 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, U.K.: Cambridge Univ. Press, 1999, pp. 37–100.

[4] L. Györfi and I. Vajda, "Constructions of protocol sequences for multiple access collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1762–1765, Sep. 1993.

[5] 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. Inf. Theory*, vol. 53, pp. 2732–2742, Aug. 2007.

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

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

[8] J. L. Massey and P. Mathys, "The collision channel wihout feedback," *IEEE Trans. Inf. Theory*, vol. IT-31, pp. 192–204, Mar. 1985.

[9] P. Mathys, "A class of codes for a T active users out of N multiple-access communication system," *IEEE Trans. Inf. Theory*, vol. 36, pp. 1206–1219, Nov. 1990.

[10] 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.

[11] 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.

[12] 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, Jan. 2007.

[13] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inf. Theory*, vol. 38, pp. 940–949, May 1992.

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

Hung-Lin Fu was born in 1950 in Taipei, Taiwan. He received the B.S. degree in Mathematics from National Taiwan Normal University in 1973 and the Ph.D. degree in mathematics (major in combinatorics) from Auburn University, Auburn, AL, in 1980.

Currently, he is a Fellow of Institute of Combinatorics and Its Applications, and a Professor of Department of Applied Mathematics, National Chiao Tung University, Hsinchu, Taiwan (since 1988). His research interests are graph theory, combinatorial designs, and their applications.

Yi-Hean Lin was born in 1985 in Hua-Lan, Taiwan. He received the B.S. degree in applied mathematics from National Tong Hua University in 2007. He is currently working toward the M.S. degree in the Department of Applied Mathematics, National Chiao Tung University, Hsinchu, Taiwan.

Miwako Mishima received the Ph.D. degree from Keio University, Yokohama, Japan, in 1999.

From 1993 to 1996, she worked for Nippon Telegraph and Telephone Corporation (NTT). In 1996, she moved to the Department of Information Science, Gifu University, Gifu, Japan, as a Research Associate, and is currently an Associate Professor. Her research interests include design theory, graph theory, and their applications.