Des. Codes Cryptogr. (2009) 52:275–291
DOI 10.1007/s10623-009-9282-2

Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3

Miwako Mishima · Hung-Lin Fu · Shoichi Uruno

Received: 9 July 2008 / Revised: 3 February 2009 / Accepted: 21 February 2009 /
Published online: 13 March 2009
© Springer Science+Business Media, LLC 2009

Abstract A conflict-avoiding code of length n and weight k is defined as a set $C \subseteq \{0, 1\}^n$ 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 paper, we obtain direct constructions for optimal conflict-avoiding codes of length $n = 16m$ and weight 3 for any m by utilizing Skolem type sequences. We also show that for the case $n = 16m + 8$ Skolem type sequences can give more concise constructions than the ones obtained earlier by Jimbo et al.

Keywords Conflict-avoiding codes · Extended Langford sequences · Extended Skolem sequences · Near-Skolem sequences

Mathematics Subject Classification (2000) 94B65 · 94B25

1 Introduction

Conflict-avoiding codes have been studied as protocol sequences for a multiple-access channel (collision channel) without feedback [3,5,6,9,12,14]. The technical description of such a multiple-access channel model can be found in [2] and [8].

Communicated by V.D. Tonchev.

M. Mishima (✉)
Department of Information Science, Gifu University, 1-1 Yanagido, Gifu 501-1193, Japan
e-mail: miwako@gifu-u.ac.jp

H.-L. Fu
Department of Applied Mathematics, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu 30050, Taiwan
e-mail: hlfu@math.nctu.edu.tw

S. Uruno
Makita Corporation, 3-11-8 Sumiyoshi, Anjyo, Aichi 446-8502, Japan
e-mail: s_uruno@mj.makita.co.jp

In mathematical terms, a conflict-avoiding code (CAC) of length n and weight k is defined as a set $C \subseteq \{0, 1\}^n$ of binary vectors, called *codewords*, all of Hamming weight k such that arbitrary cyclic shifts x', y' of distinct codewords $x, y \in C$ intersect at most at one coordinate, i.e., $\mathrm{dist}(x', y') \geq 2k - 2$ holds, where $\mathrm{dist}(x', y')$ is the Hamming distance between x' and y'. We denote the class of all the CACs of length n and weight k by $\mathrm{CAC}(n, k)$. Note that a code $C \in \mathrm{CAC}(n, k)$ can be viewed as an $(n, k, 1)$ optical orthogonal code without the autocorrelation property.

The *support* of a codeword $x = (x_0, x_1, \ldots, x_{n-1})$, denoted by $\mathrm{supp}(x)$, is the set of indices of its nonzero coordinates. For ease of manageability, we identify $\mathrm{supp}(x)$ with x throughout this article. Then any code $C \in \mathrm{CAC}(n, k)$ can be regarded as a collection of k-subsets of $\mathbb{Z}_n$ such that

$$\Delta(x) \cap \Delta(y) = \emptyset \quad \text{for any } x, y \in C,$$

where $\Delta(x) = \{j - i \pmod{n} : i, j \in x, i \neq j\}$ is the multiset of differences arising from x. If x is of form $\{0, i, \ldots, (k-1)i\}$ or its cyclic shift, then it is said to be *equi-difference* (or *centered* when $k = 3$) (see [10,11]), and if every codeword in a code $C \in \mathrm{CAC}(n, k)$ is equi-difference, then 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.,

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

A code $C \in \mathrm{CAC}(n, k)$ is said to be *optimal* if $|C| = M(n, k)$ and we are interested in optimal codes. The maximum size of equi-difference codes is defined in a similar manner to $M(n, k)$ as follows:

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

where $\mathrm{CAC}^e(n, k)$ is the class of all the equi-difference codes in $\mathrm{CAC}(n, k)$. Some constructions for optimal equi-difference CACs of weight $k \geq 4$ can be found in [11].

In this article, only the case $k = 3$ is treated. In what follows, $\mathrm{CAC}(n, 3)$, $M(n, 3)$ and $M^e(n, 3)$ are simply written as $\mathrm{CAC}(n)$, $M(n)$ and $M^e(n)$, respectively. The function $M(n)$ and $M^e(n)$ were studied in [4–6,10]. Levenshtein and Tonchev obtained the following upper bound on $M(n)$ in [6]:

$$M(n) \leq \frac{n+1}{4}.$$

Furthermore, they proved that

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

and

$$M(n) \simeq M^e(n) \simeq \frac{n}{4} \quad \text{for odd prime } n. \tag{1.1}$$

In [5] Levenshtein extended the asymptotic result (1.1) to all sufficiently large odd n, and gave the following upper bounds on $M(n)$ and $M^e(n)$ in the case where n is divisible by 4:

$$M(n) \leq \frac{23}{96}n + \frac{5}{8}, \quad M^e(n) \leq \frac{7}{32}n + \frac{3}{8}. \tag{1.2}$$

Jimbo et al. [4] improved Levenshtein's bound on $M(n)$ of (1.2) as follows:

$$M(n) \leq \frac{7}{32}n + \delta, \tag{1.3}$$

where $n = 4t$ and δ is a constant depending on the congruence of t modulo 24. They further showed that the upper bound (1.3) is strict when $t \equiv 2 \pmod 4$ by providing direct constructions.

Theorem 1.1 (Jimbo et al. [4]) *Let $n = 16m + 8$. The maximum size $M(n)$ of a code $C \in \mathrm{CAC}(n)$ is*

$$M(n) = \begin{cases} (7n-8)/32, & \text{if } m \equiv 1 \pmod 2, \\ (7n-24)/32, & \text{if } m \equiv 0, 2 \pmod 6, \\ (7n+8)/32, & \text{if } m \equiv 4 \pmod 6. \end{cases}$$

Meanwhile, Momihara [10] recently gave the necessary and sufficient condition for odd n to satisfy

$$M(n) = M^e(n) = \frac{n-1}{4} \quad \text{or} \quad \frac{n+1}{4}.$$

What it comes down to is that the exact values of $M(n)$ and $M^e(n)$ have not been determined yet for odd n, and $n = 4t$ with $t \not\equiv 2 \pmod 4$. In this article, by giving direct constructions, we will prove the equality of (1.3) holds for any $n \equiv 0 \pmod{16}$, which is a subcase of $n = 4t$, i.e., the case $t \equiv 0 \pmod 4$.

2 Upper bound on $M(n)$

Before presenting our direct constructions for optimal CACs, let us review the linear programming problem formulated by Jimbo et al. [4] and restate an upper bound on $M(n)$ derived from it just for the case $n \equiv 0 \pmod{16}$.

Since for any codeword x in a code $C \in \mathrm{CAC}(n)$, the elements of $\Delta(x)$ are symmetric with respect to $n/2$, we henceforth consider the halved difference set

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

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

Given an integer $i \in [1, n/2)$, we denote by $x(i)$ a centered codeword $x = \{0, i, 2i\}$ in a code $C \in \mathrm{CAC}(n)$. Then,

$$\Delta_2(x(i)) = \begin{cases} \{i, 2i\} & \text{if } i \in [1, n/4], \\ \{i, n-2i\} & \text{if } i \in (n/4, n/2) \text{ and } i \neq n/3, \\ \{n/3\} & \text{if } 3 \mid n \text{ and } i = n/3. \end{cases}$$

Example 2.1 Suppose that $x = \{0, 3, 6\}$ (or $x(3)$ alternatively) and $y = \{0, 1, 21\}$ are codewords of a conflict-avoiding code of length 48. In this case,

$$\Delta(x) = \{3, 3, 6, 42, 45, 45\}, \quad \Delta_2(x) = \{3, 6\},$$
$$\Delta(y) = \{1, 20, 21, 27, 28, 47\}, \quad \Delta_2(y) = \{1, 20, 21\}.$$

Note that for a code $C \in \mathrm{CAC}(n)$, any pair of codewords $x, y \in C$ $(x \neq y)$ must satisfy $\Delta_2(x) \cap \Delta_2(y) = \emptyset$. Then we have the next lemma.

Lemma 2.1 (**[4]**) *Any code $C \in \mathrm{CAC}(n)$ can contain at most one codeword among $x(i)$, $x(2i)$ and $x(n/2 - i)$ for each integer $i \in [1, n/4]$.*

For further argument, we partition the set of 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 2.2 and 2.3 according to the composition of its halved difference set.

Lemma 2.2 **([4])** *Any centered codeword $x \in C$ such that $\Delta_2(x) = \{i, j\}$, 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 2.3 **([4])** *Any non-centered codeword $x \in C$ such that $\Delta_2(x) = \{i, j, k\}$ 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 2.2, 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 2.3, respectively. For convenience, we treat the centered codewords $x(n/3)$ and $x(n/4)$ separately from C_o, C_e and C_d, and define the following parameters.

$$\alpha = \begin{cases} 0 \text{ if } x(n/3) \notin C, \\ 1 \text{ if } x(n/3) \in C, \end{cases} \quad \beta = \begin{cases} 0 \text{ if } x(n/4) \notin C, \\ 1 \text{ if } x(n/4) \in C. \end{cases}$$

Then it follows that

$$C_o \cup C_e \cup C_d \cup N_{oe} \cup N_{od} \cup N_e \cup N_d = C \setminus \{x(n/3), x(n/4)\}$$

and

$$|C| = s\alpha + \beta + |C_o| + |C_e| + |C_d| + |N_{oe}| + |N_{od}| + |N_e| + |N_d|, \tag{2.1}$$

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

An upper bound (1.3) on $M(n = 16m)$ can be obtained by maximizing (2.1) subject to

$$\begin{aligned} & k_1\beta + |C_o| + 2|N_{oe}| + 2|N_{od}| \le \frac{n}{4}, \\ & k_2\beta + |C_o| + |C_e| + |N_{oe}| + 2|N_e| \le \frac{n}{8}, \\ & s\alpha + k_3\beta + |C_e| + 2|C_d| + |N_{od}| + |N_e| + 3|N_d| \le \frac{n}{8}, \\ & |C_o| \le \frac{n}{8},\ \alpha \le 1,\ \beta \le 1, \end{aligned} \tag{2.2}$$

where

$$(s, k_1, k_2, k_3) = \begin{cases} (1, 0, 0, 2) \text{ if } m \equiv 0 \pmod{3}, \\ (0, 0, 0, 2) \text{ if } m \equiv 1, 2 \pmod{3}. \end{cases} \tag{2.3}$$

For more details of the conditions (2.2) and (2.3), see [4, Sect. 2].

Although Jimbo et al. stated the following lemma for any $n \equiv 0 \pmod{4}$ [4, Lemma 2.9] as a result of linear programming, in this paper we focus on the case $n \equiv 0 \pmod{16}$.

Lemma 2.4 *Let $n = 16m$. For any code $C \in \mathrm{CAC}(n)$,*

$$|C| \leq \begin{cases} \lfloor (7n + 16)/32 \rfloor & \text{if } m \equiv 0 \pmod{3}, \\ \lfloor 7n/32 \rfloor & \text{if } m \equiv 1, 2 \pmod{3}. \end{cases}$$

The proof of Lemma 2.4 is given in Appendix. Removing the floor function from Lemma 2.4, we have the following which is a partial result of Lemma 2.10 in [4].

Theorem 2.2 *Let $n = 16m$. Then*

$$M(n) \leq \begin{cases} 7n/32, & \text{if } m \equiv 0 \pmod{2}, \\ (7n - 16)/32, & \text{if } m \equiv 1, 5 \pmod{6}, \\ (7n + 16)/32, & \text{if } m \equiv 3 \pmod{6}. \end{cases} \tag{2.4}$$

Our objective is to prove the equality of (2.4) holds for all positive integer m except when $m = 3$ and 4.

3 Direct constructions

In this section, taking advantage of Skolem type sequences, we will give direct constructions for optimal conflict-avoiding codes of length $n = 16m$ and weight 3.

Definition 3.1 Let k and n be integers with $1 \leq k \leq 2n+1$. A k-extended Skolem sequence of order n is a sequence $(a_1, a_2, \ldots, a_n)$ of n integers such that

$$\bigcup_{i=1}^{n} \{a_i, a_i - i\} = \{1, 2, \ldots, 2n + 1\} \setminus \{k\}.$$

When $k = 2n + 1$, it is simply called a Skolem sequence of order n.

Definition 3.2 Let d, k and n be integers with $n > d$ and $1 \leq k \leq 2n + 1$. A k-extended Langford sequence of order n and defect d is a sequence $(a_1, a_2, \ldots, a_n)$ of n integers such that

$$\bigcup_{i=1}^{n} \{a_i, a_i - (d + i - 1)\} = \{d, d + 1, \ldots, d + 2n\} \setminus \{d + k - 1\}.$$

When $k = 2n + 1$, it is simply called a Langford sequence of order n and defect d.

Definition 3.3 Let m and n be integers with $n \geq m$. A near-Skolem sequence of order n and defect m is a sequence $(a_1, \ldots, a_{m-1}, \text{-}, a_{m+1}, \ldots, a_n)$ of $n - 1$ integers such that

$$\bigcup_{\substack{i=1 \\ i \neq m}}^{n} \{a_i, a_i - i\} = \{1, 2, \ldots, 2n - 2\}.$$

Example 3.2 (1) A 4-extended Skolem sequence of order 2: (2, 5).
(2) A Skolem sequence of order 4: (2, 7, 6, 8).
(3) A 2-extended Langford sequence of order 2 and defect 2: (6, 5).
(4) A near-Skolem sequence of order 4 and defect 3: (3, 6, -, 5).

Theorem 3.1 (Baker [1]) *A k-extended Skolem sequence of order n exists if and only if*

(i) *k is odd and $n \equiv 0, 1 \pmod 4$, or*
(ii) *k is even and $n \equiv 2, 3 \pmod 4$.*

Theorem 3.2 (Linek and Jiang [7]) *A k-extended Langford sequence of order n and defect 2 exists if and only if*

(i) *k is odd and $n \equiv 0, 3 \pmod 4$, or*
(ii) *k is even and $n \equiv 1, 2 \pmod 4$.*

Theorem 3.3 (Shalaby [13]) *A near-Skolem sequence of order n and defect m exists if and only if*

(i) *$n \equiv 0, 1 \pmod 4$ and m is odd, or*
(ii) *$n \equiv 2, 3 \pmod 4$ and m is even.*

We will now present direct constructions for optimal codes in CAC$(n = 16m)$ with respect to the following seven cases in order.

(1) $m \equiv 2, 8, 10, 16 \pmod{24}$,
(2) $m \equiv 4, 14, 20, 22 \pmod{24}$,
(3) $m \equiv 0, 18 \pmod{24}$,
(4) $m \equiv 6, 12 \pmod{24}$,
(5) $m \equiv 1, 5 \pmod 6$,
(6) $m \equiv 15, 21 \pmod{24}$, and
(7) $m \equiv 3, 9 \pmod{24}$.

For the reader's 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 2.2. The variables not listed in the table are all zero, i.e., $|C_e| = |N_{oe}| = |N_e| = |N_d| = 0$.

Construction 3.1 The case $m \equiv 2, 8, 10, 16 \pmod{24}$, i.e., $n \equiv 32, 128, 160, 256 \pmod{384}$. Let C_o be the set of the following $n/8$ centered codewords:

$$\{0, 4i - 1, 8i - 2\}, \quad 1 \le i \le n/16; \tag{3.1}$$
$$\{0, n/2 - 4i + 3, n - 8i + 6\}, \quad 1 \le i \le n/16. \tag{3.2}$$

Table 1 Sizes of subsets of codewords for an optimal code in CAC$(n = 16m)$

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

Then it is easy to check that

$$\Delta_2(C_o) = \{4i - 1 : 1 \le i \le n/8\} \cup \{4i - 2 : 1 \le i \le n/8\}. \tag{3.3}$$

Next, consider the set C_d consisting of the following $n/32 - 1$ centered codewords:

$$\{0, n/8 + 4i, n/4 + 8i\}, \qquad 1 \le i \le n/32 - 1. \tag{3.4}$$

Then

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

Lastly let N_{od} be the set of the following $n/16$ non-centered codewords:

$$\{0, 4i - 3, n/2 - 4i + 1\}, \;\; 1 \le i \le n/32; \tag{3.5}$$

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

where $(a_1, a_2, \ldots, a_{n/32})$ is a Skolem sequence of order $n/32$. Then

$$\begin{aligned}\Delta_2(N_{od}) = \;& \{4i - 3 : 1 \le i \le n/8\} \cup \{8i - 4 : n/32 + 1 \le i \le n/16\} \\ & \cup \{4i : 1 \le i \le n/32\}.\end{aligned}$$

Note that since $n/32 \equiv 0, 1 \pmod{4}$ holds, provided that $m \equiv 2, 8, 10, 16 \pmod{24}$, Theorem 3.1(i) with $k = n/16 + 1$ guarantees the existence of a Skolem sequence of order $n/32$.

Counting the number of codewords in the resulting code C including $x(n/4)$, we have

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

which meets the upper bound on $M(n)$ of Theorem 2.2.

Example 3.3 The case $n = 128$ (thus $m = 8$). Take C_o, C_d and N_{od} according to Construction 3.1 with the Skolem sequence of order 4 in Example 3.2(2). That is,

$$\begin{aligned}C_o = \;& \{\{0, 3, 6\}, \{0, 7, 14\}, \{0, 11, 22\}, \{0, 15, 30\}, \{0, 19, 38\}, \{0, 23, 46\}, \\ & \{0, 27, 54\}, \{0, 31, 62\}, \{0, 63, 126\}, \{0, 59, 118\}, \{0, 55, 110\}, \\ & \{0, 51, 102\}, \{0, 47, 94\}, \{0, 43, 86\}, \{0, 39, 78\}, \{0, 35, 70\}\}, \\ C_d = \;& \{\{0, 20, 40\}, \{0, 24, 48\}, \{0, 28, 56\}\}, \\ N_{od} = \;& \{\{0, 1, 61\}, \{0, 5, 57\}, \{0, 9, 53\}, \{0, 13, 49\}, \{0, 17, 21\}, \{0, 33, 41\}, \\ & \{0, 25, 37\}, \{0, 29, 45\}\}.\end{aligned}$$

Together with $x(n/4) = \{0, 32, 64\}$, $C = \{x(n/4)\} \cup C_o \cup C_d \cup N_{od}$ becomes an optimal code in CAC(128), and then $|C| = 28$.

Construction 3.2 The case $m \equiv 4, 14, 20, 22 \pmod{24}$ and $m \ne 4$, i.e., $n \equiv 64, 224, 320, 352 \pmod{384}$ and $n \ne 64$. Let C_o be the set of (3.1) and (3.2) just as they are, C_d be the set of $\{0, n/2 - 8, n - 16\}$ and (3.4) for $1 \le i \le n/32 - 2$, and N_{od} be the set of (3.5) for $1 \le i \le n/32 + 1$ and

$$\{0, n/8 + 4(a_i - i) + 1, n/8 + 4a_i + 1\}, \;\; 1 \le i \le n/32 + 1, \;\; i \ne 4,$$

where $(a_1, a_2, a_3, \text{-}, a_5, \ldots, a_{n/32})$ is a near-Skolem sequence of order $n/32$ and defect 4. Since $n/32 \equiv 2, 3 \pmod{4}$, the existence of a required near-Skolem sequence is assured by Theorem 3.3(ii). Then it can be verified that

$$\Delta_2(C_d) = \{4i : n/32 + 1 \le i \le n/16 - 2\} \cup \{8i : n/32 + 1 \le i \le n/16 - 1\} \cup \{16\}$$

and

$$\Delta(N_{od}) = \{4i-3 : 1 \le i \le n/8\} \cup \{8i-4 : n/32 \le i \le n/16\}$$
$$\cup\{4i : 1 \le i \le n/32\} \setminus \{16\}.$$

Together with $\Delta_2(C_o)$ calculated as (3.3) and $\Delta_2(x(n/4))$, it turns out that $\Delta_2(C) = [1, n/2]$ and $|C| = 7n/32$.

Construction 3.3 The case $m \equiv 0, 18 \pmod{24}$, i.e., $n \equiv 0, 288 \pmod{384}$. The construction is almost the same as Construction 3.1 except that in (3.4) $i = n/96$ is skipped (thus $\Delta_2(C_d) = (\{4i : n/32+1 \le i \le n/16-1\}\setminus\{n/6\})\cup(\{8i : n/32+1 \le i \le n/16-1\}\setminus\{n/3\}))$ and the centered codeword $x(n/3) = \{0, n/3, 2n/3\}$ exists. Then, we have

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

In fact, $m \equiv 0, 18 \pmod{24}$ implies $n/32 \equiv 0, 1 \pmod 4$, which guarantees the existence of a Skolem sequence of order $n/32$ (see Theorem 3.1(i)). Note that in this case, $\Delta_2(C) = [1, n/2] \setminus \{n/6\}$.

Construction 3.4 The case $m \equiv 6, 12 \pmod{24}$, i.e., $n \equiv 96, 192 \pmod{384}$. In this case, both of the centered codewords $x(n/3)$ and $x(n/4)$ exist. Let C_o be the set of (3.1) and (3.2) just as they are, and C_d is defined as in Construction 3.3, i.e., as the set of (3.4) with $i \ne n/96$. As N_{od}, besides (3.5), take $\{0, 5n/24 - 3, 3n/8 - 3\}$ and

$$\{0, n/8 + 4(a_i - i) - 11, n/8 + 4a_i - 7\},\ 1 \le i \le n/32 - 1,$$

where $(a_1, a_2, \dots, a_{n/32-1})$ is an $(n/48)$-extended Langford sequence of order $n/32 - 1$ and defect 2. Since $n/48$ is even and $n/32 - 1 \equiv 1, 2 \pmod 4$, the existence of an $(n/48)$-extended Langford sequence of order $n/32-1$ and defect 2 is guaranteed by Theorem 3.2(ii). Then we have $|C| = 7n/32$.

Note that

$$\Delta_2(N_{od}) = \{4i-3 : 1 \le i \le n/8\} \cup \{8i-4 : n/32+1 \le i \le n/16\}$$
$$\cup\{4i : 2 \le i \le n/32\} \cup \{n/6\}$$

and $\Delta_2(C) = [1, n/2] \setminus \{4\}$.

Example 3.4 The case $n = 96$ (thus $m = 6$). Take C_o, C_d and N_{od} according to Construction 3.4 with the 2-extended Langford sequence of order 2 and defect 2 in Example 3.2(3). That is,

$$C_o = \{\{0, 3, 6\}, \{0, 7, 14\}, \{0, 11, 22\}, \{0, 15, 30\}, \{0, 19, 38\}, \{0, 23, 46\},$$
$$\{0, 47, 94\}, \{0, 43, 86\}, \{0, 39, 78\}, \{0, 35, 70\}, \{0, 31, 62\}, \{0, 27, 54\}\},$$
$$C_d = \{\{0, 20, 40\}\},$$
$$N_{od} = \{\{0, 1, 45\}, \{0, 5, 41\}, \{0, 9, 37\}, \{0, 17, 33\}, \{0, 21, 29\}, \{0, 13, 25\}\}.$$

Then $C = \{\{0, 32, 64\}, \{0, 24, 48\}\} \cup C_o \cup C_d \cup N_{od}$ is an optimal code in CAC(96), and $|C| = 21$.

Construction 3.5 The case $m \equiv 1, 5 \pmod 6$, i.e., $n \equiv 16, 80 \pmod{96}$. Let C_o be the set of (3.1) and (3.2) as they are, and let C_d be the set of the following $(n-16)/32$ centered codewords:

$$\{0, n/8 + 4i - 2, n/4 + 8i - 4\},\ 1 \le i \le (n-16)/32. \quad (3.7)$$

Then it is easy to check that

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

As N_{od}, define the set of (3.5) for $1 \le i \le (n-16)/32$ and the following $(n-16)/32$ codewords:

$$\{0, n/8 + 4(a_i - i) - 1, n/8 + 4a_i - 1\},\ 1 \le i \le (n-16)/32, \tag{3.8}$$

where $(a_1, a_2, \ldots, a_{(n-16)/32})$ is a k-extended Skolem sequence of order $(n-16)/32$ and k can be any odd integer in the interval $[2, n/16+1]$ if $m \equiv 1, 11, 17, 19 \pmod{24}$, and any even in the same interval if $m \equiv 5, 7, 13, 23 \pmod{24}$. Since

$$\frac{n-16}{32} \equiv \begin{cases} 0 \pmod 4, & \text{if } m \equiv 1, 17 \pmod{24},\\ 1 \pmod 4, & \text{if } m \equiv 11, 19 \pmod{24},\\ 2 \pmod 4, & \text{if } m \equiv 5, 13 \pmod{24},\\ 3 \pmod 4, & \text{if } m \equiv 7, 23 \pmod{24},\end{cases}$$

there does exist a desired extended Skolem sequence (see Theorem 3.1). Then, taking the centered codeword $x(n/4)$ into account, we have

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

Note that

$$\begin{aligned}\Delta_2(N_{od}) = &(\{4i-3 : 1 \le i \le n/8\} \setminus \{n/8-1\})\\ &\cup\{8i-4 : (n+16)/32 + 1 \le i \le n/16\}\\ &\cup\{4i : 1 \le i \le (n-16)/32\} \setminus \{n/8+4k-1\}\end{aligned}$$

and $\Delta_2(C) = [1, n/2] \setminus \{n/8-1, n/8+4k-1\}$.

Example 3.5 The case $n = 80$ (thus $m = 5$). Take C_o, C_d and N_{od} according to Construction 3.5 with the 4-extended Skolem sequence of order 2 in Example 3.2(1). That is,

$$\begin{aligned}C_o &= \{\{0,3,6\},\{0,7,14\},\{0,11,22\},\{0,15,30\},\{0,19,38\},\\ &\quad\{0,39,78\},\{0,35,70\},\{0,31,62\},\{0,27,54\},\{0,23,46\}\},\\ C_d &= \{\{0,12,24\},\{0,16,32\}\},\\ N_{od} &= \{\{0,1,37\},\{0,5,33\},\{0,13,17\},\{0,21,29\}\}.\end{aligned}$$

Then $C = \{\{0,20,40\}\} \cup C_o \cup C_d \cup N_{od}$ is an optimal code in CAC(80), and $|C| = 17$.

Construction 3.6 The case $m \equiv 15, 21 \pmod{24}$, i.e., $n \equiv 240, 336 \pmod{384}$. The construction is almost the same as Construction 3.5. The difference is that there exists $x(n/3)$, C_d is defined as the set of (3.7) with $i \ne (n+48)/96$, and N_{od} consists of $\{0, n/8-1, 7n/24-1\}$, (3.5) for $1 \le i \le (n-16)/32$, and (3.8), where $(a_1, a_2, \ldots, a_{(n-16)/32})$ is an $(n/24)$-extended Skolem sequence of order $(n-16)/32$. Since $(n-16)/32 \equiv 2, 3 \pmod 4$ and $n/24$ is even, a required extended Skolem sequence always exists (see Theorem 3.1(ii)). Note that

$$\begin{aligned}\Delta_2(C_d) = &(\{4i : (n+16)/32 \le i \le n/16 - 1\} \setminus \{n/6\})\\ &\cup\{8i : (n+16)/32 \le i \le n/16 - 1\} \setminus \{n/3\}\end{aligned}$$

and

$$\begin{aligned}\Delta_2(N_{od}) = &\{4i-3 : 1 \le i \le n/8\} \cup \{8i-4 : (n+16)/32 + 1 \le i \le n/16\}\\ &\cup\{4i : 1 \le i \le (n-16)/32\}.\end{aligned}$$

In this case, we have

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

Construction 3.7 The case $m \equiv 3, 9 \pmod{24}$ and $m \neq 3$, i.e., $n \equiv 48, 144 \pmod{384}$ and $n \neq 48$. In this case, both of $x(n/3)$ and $x(n/4)$ exist. Let C_o be the set of $\{0, 3n/8 - 1, 3n/4 - 2\}$, (3.1) with $i \neq (n+16)/32$ and (3.2) for $1 \leq i \leq n/16$, C_d be the set of $\{0, n/12, n/6\}$ and (3.7) for $1 \leq i \leq (n-16)/32 - 1$ and $i \neq (n+48)/96$, and N_{od} be the set of $\{0, n/8 - 1, 3n/8 - 5\}$, $\{0, n/8 + 1, n/2 - 8\}$, (3.5) for $1 \leq i \leq (n-16)/32$, and (3.8) with $i \neq n/48$, where $(a_1, \ldots, a_{n/48-1}, \text{-}, a_{n/48+1}, \ldots, a_{(n-16)/32})$ is a near-Skolem sequence of order $(n-16)/32$ and defect $n/48$. Since $(n-6)/32 \equiv 0, 1 \pmod 4$ and $n/48$ is odd, such a near-Skolem sequence does exist (see Theorem 3.3(i)). Note that

$$\begin{aligned}
\Delta_2(C_o) &= \{3n/8 - 1\} \cup (\{4i - 1 : 1 \leq i \leq n/8\} \setminus \{n/8 + 1\}) \\
&\quad \cup \{4i - 2 : 1 \leq i \leq n/8\} \setminus \{n/4 + 2\}, \\
\Delta_2(C_d) &= \{n/12\} \cup \{4i : (n+16)/32 \leq i \leq n/16 - 2\} \\
&\quad \cup \{8i : (n+16)/32 \leq i \leq n/16 - 2\} \setminus \{n/3\}, \\
\Delta_2(N_{od}) &= \{n/8 + 1, n/4 - 4, n/2 - 8\} \cup \{4i - 3 : (n+16)/32 \leq i \leq n/8\} \\
&\quad \cup \{8i - 4 : 1 \leq i \leq (n+16)/32 + 1 \leq i \leq n/16\} \\
&\quad \cup \{4i : 1 \leq i \leq (n+16)/32 - 2\} \setminus \{n/12\}.
\end{aligned}$$

Counting the number of codewords in the resulting code C, we have

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

Example 3.6 The case $n = 144$ (thus $m = 9$). Take C_o, C_d and N_{od} according to Construction 3.7 with the near-Skolem sequence of order 4 and defect 3 in Example 3.2(4). That is,

$$\begin{aligned}
C_o &= \{\{0, 53, 106\}, \{0, 3, 6\}, \{0, 7, 14\}, \{0, 11, 22\}, \{0, 15, 30\}, \{0, 23, 46\}, \\
&\quad \{0, 27, 54\}, \{0, 31, 62\}, \{0, 35, 70\}, \{0, 71, 142\}, \{0, 67, 134\}, \\
&\quad \{0, 63, 126\}, \{0, 59, 118\}, \{0, 55, 110\}, \{0, 51, 102\}, \{0, 47, 94\}, \\
&\quad \{0, 43, 86\}, \{0, 39, 78\}\}, \\
C_d &= \{\{0, 12, 24\}, \{0, 20, 40\}, \{0, 28, 56\}\}, \\
N_{od} &= \{\{0, 17, 49\}, \{0, 19, 64\}, \{0, 1, 69\}, \{0, 5, 65\}, \{0, 9, 61\}, \{0, 13, 57\}, \\
&\quad \{0, 25, 29\}, \{0, 33, 41\}, \{0, 21, 37\}\}.
\end{aligned}$$

Then $C = \{\{0, 48, 96\}, \{0, 36, 72\}\} \cup C_o \cup C_d \cup N_{od}$ becomes an optimal code in CAC(144), and $|C| = 32$.

We should remark that the cases $m = 3$ and 4, i.e., $n = 48$ and 64, are excluded from Constructions 3.7 and 3.2 respectively. In fact, for those two cases, the equality of the upper bound in Theorem 2.2 never hold.

4 Exceptional cases

Recall that for the cases $m = 3$ and 4, Theorem 2.2 claims that $M(48) \leq 11$ and $M(64) \leq 14$ as the solution of the LP problem defined by (2.1)–(2.3). Moreover, from the proof of Lemma 2.4 in Appendix, it also turns out that for a code $C \in \text{CAC}(48)$ if $|C| = 11$ holds, then

$$(\alpha, \beta, |C_o|, |C_d|, |N_{od}|) = (1, 1, 6, 0, 3) \text{ or } (1, 0, 6, 1, 3) \tag{4.1}$$

and $|C_e| = |N_{oe}| = |N_e| = |N_d| = 0$, and for a code $C \in \mathrm{CAC}(64)$ if $|C| = 14$, then

$$(\beta, |C_o|, |C_d|, |N_{od}|) = (1, 8, 1, 4) \text{ or } (0, 8, 2, 4) \tag{4.2}$$

and $\alpha = |C_e| = |N_{oe}| = |N_e| = |N_d| = 0$.

In this section, it will be proved that any of the cases above cannot be admissible, and that $M(48) = 10$ and $M(64) = 13$.

To do that, we will provide two lemmas first. Consider the following two disjoint subsets of $O = \{i : i \equiv 1 \pmod 2, 1 \le i \le n/2\}$.

$$\begin{aligned} A &= \{i : i \equiv \pm 1 \pmod 8,\ 1 \le i \le n/2\}, \\ B &= \{i : i \equiv \pm 3 \pmod 8,\ 1 \le i \le n/2\}. \end{aligned} \tag{4.3}$$

It is quite obvious that for any two odd integers $i, j \in [1, n/2]$, if $i + j \equiv 4 \pmod 8$, then $i \in A$ and $j \in B$, and if $i + j \equiv 0 \pmod 8$, then $i, j \in A$ or $i, j \in B$. Then, we can state the following about $\Delta_2(x)$ for any non-centered codeword $x \in N_{od}$ of a code in $\mathrm{CAC}(n = 16m)$.

Lemma 4.1 *For any non-centered codeword $x \in N_{od}$ of a code in* $\mathrm{CAC}(n = 16m)$, $\Delta_2(x) = \{i, j, k\}$ *satisfies*

$$k \equiv \begin{cases} 4 \pmod 8, & \text{if } i \in A \text{ and } j \in B, \text{ or} \\ 0 \pmod 8, & \text{if } i, j \in A \text{ or } i, j \in B. \end{cases}$$

Let i be an odd integer in the interval $[1, n/4)$, where $n \equiv 0 \pmod{16}$. Then $2i$ is singly even and for any centered codeword $x \in C_o$ such that $2i \in \Delta_2(x)$, it follows from Lemma 2.1 that

$$\Delta_2(x) = \begin{cases} \{i, 2i\}, & \text{if } 1 \le i \le n/8, \\ \{n/2 - i, 2i\}, & \text{if } n/8 < i < n/4, \end{cases}$$

which implies that for any odd integer $i \in [1, n/4)$, i and $n/2 - i$ cannot be contained together in $\Delta_2(C_o)$.

Lemma 4.2 *Let* $n \equiv 0 \pmod{16}$. *For any optimal code* $C \in \mathrm{CAC}(n)$, *if* $|N_{od}| = n/16$ *holds, then* $C_e = N_{oe} = N_e = \emptyset$, $n/2 \notin \Delta_2(N_{od})$, *and* $|\{k : k \equiv 0 \pmod 8,\ k \in \Delta_2(N_{od})\}|$ *is even.*

Proof The solution of the LP problem defined by (2.1)–(2.3) (see the proof of Lemma 2.4 in Appendix) tells that for a code $C \in \mathrm{CAC}(n = 16m)$ to be optimal, $|C_o| = n/8$ is necessary. This means that for every odd $i \in [1, n/4)$, either i or $n/2 - i$ is in $\Delta_2(C_o)$, and therefore $E = \{i : i \equiv 2 \pmod 4,\ 1 \le i \le n/2\} \subset \Delta_2(C_o)$. So, any codeword x such that $\Delta_2(x) \cap E \ne \emptyset$ is not allowed to exist in $C \setminus C_o$, which implies that $C_e = N_{oe} = N_e = \emptyset$.

Now, suppose that $n/2 \in \Delta_2(N_{od})$. Then there should be a codeword $x \in N_{od}$ such that $\Delta_2(x) = \{i, n/2 - i, n/2\}$ for some odd integer $i \in [1, n/4)$. However, this could be impossible since for every odd $i \in [1, n/4)$, either i or $n/2 - i$ is in $\Delta_2(C_o)$. Thus $n/2 \notin \Delta_2(N_{od})$.

Let A and B be the two disjoint subsets of O defined by (4.3), and further let A' and B' be the sets of elements left behind in A and B respectively after taking all the odd integers in $\Delta_2(C_o)$ away. Since $n/2 - i \in A$ if $i \in A$, or $n/2 - i \in B$ if $i \in B$, exactly one-half elements in each of A and B need to be in $\Delta_2(C_o)$. Then, we have

$$|A'| = |B'| = \frac{|A|}{2} = \frac{|B|}{2} = \frac{n}{16}.$$

From the assumption $|N_{od}| = n/16$, it turns out that the set of odd integers in $\Delta_2(N_{od})$ must be exactly $A' \cup B'$. If there is a codeword $x \in N_{od}$ such that $\Delta_2(x) = \{i, j, k\}$ with $k \equiv 4 \pmod 8$, then it follows from Lemma 4.1 that i and j separately belong to A' and B'. Since $|A'| = |B'|$, if there exists a codeword $x \in N_{od}$ such that $\Delta_2(x) = \{i, j, k\}$ with $i, j \in A'$ and $k \equiv 0 \pmod 8$, then there should be another codeword $x' \in N_{od}$ such that $\Delta_2(x') = \{i', j', k'\}$ with $i', j' \in B'$ and $k' \equiv 0 \pmod 8$. This means that $|\{k : k \equiv 0 \pmod 8, k \in \Delta_2(N_{od})\}|$ is even.

Theorem 4.1 $M(48) = 10$.

Proof Firstly we will prove that there does not exist a code $C \in \mathrm{CAC}(48)$ satisfying $|C| = 11$. As mentioned at the beginning of this section, if $|C| = 11$ holds, then (4.1) must be satisfied. In either case in (4.1), the centered codeword $x(n/3) = \{0, n/3, 2n/3\}$ is supposed to exist in C since $\alpha = 1$. Let D be the set of doubly even integers in $[1, n/2]$, i.e., $D = \{4, 8, 12, 16, 20, 24\}$ when $n = 48$.

(i) The case $(\alpha, \beta, |C_o|, |C_d|, |N_{od}|) = (1, 1, 6, 0, 3)$. It follows from $\beta = 1$ that the centered codeword $x(n/4) = \{0, n/4, n/2\}$ exists in a code C. Let $D' = D \setminus \Delta_2(x(n/3)) \setminus \Delta_2(x(n/4))$, i.e., $D' = \{4, 8, 20\}$. Since $|N_{od}| = n/16 = 3$, D' should be exactly the set of the doubly even integers in $\Delta_2(N_{od})$. However, $|\{k : k \equiv 0 \pmod 8, k \in D'\}| = 1$ contradicts Lemma 4.2.

(ii) The case $(\alpha, \beta, |C_o|, |C_d|, |N_{od}|) = (1, 0, 6, 1, 3)$. From Lemma 4.2, we know that $n/2 \notin \Delta_2(N_{od})$. Let $D' = D \setminus \Delta_2(x(n/3)) \setminus \{n/2\} = \{4, 8, 12, 20\}$. Since $C_d \neq \emptyset$, the set of the doubly even integers in $\Delta_2(N_{od})$ should be given by $D' \setminus \Delta_2(C_d)$. Note that the cardinality of N_{od} is equal to the number of the doubly even integers in $\Delta_2(N_{od})$. That is, $|N_{od}| = |D' \setminus \Delta_2(C_d)| = 2$, which contradicts $|N_{od}| = 3$, one of the necessary conditions for $|C| = 11$.

From the arguments in the cases (i) and (ii), it has turned out that $M(48) \leq 10$. To complete the proof, we will present 10 codewords for a code in CAC(48). Take the sets C_o and N_{od} as follows:

$$C_o = \{\{0, 3, 6\}, \{0, 7, 14\}, \{0, 11, 22\}, \{0, 15, 30\}, \{0, 19, 38\}, \{0, 23, 46\}\},$$
$$N_{od} = \{\{0, 1, 21\}, \{0, 5, 13\}\}.$$

Then $C = \{\{0, 16, 32\}, \{0, 12, 24\}\} \cup C_o \cup N_{od}$ is a code in CAC(48) and $|C| = 10$. □

Theorem 4.2 $M(64) = 13$.

Proof The proof is similar to that of Theorem 4.1. We will first prove that there is no code with 14 codewords in CAC(64). Recall that (4.2) is a necessary condition for $|C| = 14$. Let D be the set of doubly even integers in $[1, n/2]$, i.e., when $n = 64$, $D = \{4, 8, 12, 16, 20, 24, 28, 32\}$.

(i) The case $(\beta, |C_o|, |C_d|, |N_{od}|) = (1, 8, 1, 4)$. Since $\beta = 1$, $x(n/4)$ is in the code C. Consequently, the single codeword for C_d will be chosen from $\{x(4), x(12), x(20), x(28)\}$. Note that, regardless of the choice of the codeword for C_d, one of the two elements in $\Delta_2(C_d)$ is congruent to 4 modulo 8 and the other is divisible by 8. Let $D' = D \setminus \Delta_2(x(n/4)) \setminus \Delta_2(C_d)$. Since $|N_{od}| = n/16 = 4$, D' must be exactly the set of the doubly even integers in $\Delta_2(N_{od})$. However, $|\{k : k \equiv 0 \pmod 8, k \in D'\}| = 1$ contradicts Lemma 4.2.

(ii) The case $(\beta, |C_o|, |C_d|, |N_{od}|) = (0, 8, 2, 4)$. It follows from Lemma 4.2 that $n/2 \notin \Delta_2(N_{od})$. Since $|C_d| = 2$, $|D \setminus \{n/2\} \setminus \Delta_2(C_d)| = 3$ holds, which means that we only have 3 doubly even integers which can possibly be in $\Delta_2(N_{od})$. This implies $|N_{od}| \leq 3$ and contradicts $|N_{od}| = 4$.

Since neither the case (i) nor (ii) is admissible, $M(64) \leq 13$. Take the sets C_o and N_{od} as follows:

$$\begin{aligned} C_o &= \{\{0,3,6\},\{0,7,14\},\{0,11,22\},\{0,15,30\},\{0,19,38\},\{0,23,46\},\\ &\qquad \{0,27,54\},\{0,31,62\}\},\\ C_d &= \{\{0,12,24\}\},\\ N_{od} &= \{\{0,1,29\},\{0,5,25\},\{0,9,17\}\}. \end{aligned}$$

Then $C = \{\{0,16,32\}\} \cup C_o \cup C_d \cup N_{od}$ is a code with 13 codewords in CAC(64). □

From Theorems 2.2, 4.1 and 4.2, and Constructions 3.1–3.7, we can finally establish the main theorem.

Theorem 4.3 *Let $n = 16m$. The maximum size $M(n)$ of a code $C \in \mathrm{CAC}(n)$ 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 $M(64) = 13$.

5 Another proof of Theorem 1.1

Theorem 1.1 can be also proved by way of Skolem type sequences. In this section, we will give constructions for optimal codes in CAC$(16m+8)$ by using extended Skolem sequences, which are relatively concise compared with the constructions in [4]. We just provide codewords and leave the verification of their halved differences to the reader. For reference, we list the sizes of subsets of codewords for an optimal code in CAC$(n = 16m+8)$ in Table 2 which can also be found in [4].

Construction 5.1 The case $m \equiv 1 \pmod{6}$, i.e., $n \equiv 24 \pmod{96}$. Note that in this case, we take $x(n/3)$, but not $x(n/4)$ on purpose. Let C_o be the set of the following $n/8$ centered codewords:

$$\{0, 4i-1, 8i-2\}, \quad 1 \leq i \leq (n+8)/16; \tag{5.1}$$

$$\{0, n/2-4i+3, n-8i+6\}, \quad 1 \leq i \leq (n-8)/16, \tag{5.2}$$

Table 2 Sizes of subsets of codewords for an optimal code in CAC$(n = 16m+8)$ [4]

$m \pmod{6}$	α	β	$\|C_o\|$	$\|C_d\|$	$\|N_{od}\|$	$\|C\|$
0, 2	0	0	$n/8$	$(n-8)/32$	$(n-8)/16$	$(7n-24)/32$
3, 5	0	1	$n/8-1$	$(n-24)/32$	$(n+8)/16$	$(7n-8)/32$
1	1	0	$n/8$	$(n-24)/32$	$(n-8)/16$	$(7n-8)/32$
4	1	1	$n/8-1$	$(n-8)/32-1$	$(n+8)/16$	$(7n+8)/32$

C_d be the set of the following $(n-24)/32$ centered codewords:

$$\{0, n/8+4i-3, n/4+8i-6\},\ 1 \le i \le (n+8)/32,\ i \ne (n+72)/96,$$

and N_{od} be the set of the following $(n-8)/16$ non-centered codewords:

$$\{0, n/6, n/2-3\}; \tag{5.3}$$

$$\{0, 4i-3, n/2-4i-3\},\ 1 \le i \le (n-24)/32; \tag{5.4}$$

$$\{0, n/8+4(a_i-i)-c, n/8+4a_i-c\},\ 1 \le i \le (n-24)/32, \tag{5.5}$$

where $(a_1, a_2, \ldots, a_{(n-24)/32})$ is a k-extended Skolem sequence of order $(n-24)/32$ and

$$(c,k) = \begin{cases} (2, (5n-24)/96) \text{ if } m \equiv 1, 7 \pmod{24}, \\ (6, (5n+72)/96) \text{ if } m \equiv 13, 19 \pmod{24}. \end{cases}$$

Then we have

$$|C| = \alpha + |C_o| + |C_d| + |N_{od}| = 1 + \frac{n}{8} + \frac{n-24}{32} + \frac{n-8}{16} = \frac{7n-8}{32},$$

which meets the upper bound on $M(n)$ of Theorem 1.1.

Construction 5.2 The case $m \equiv 0, 2 \pmod 6$, i.e., $n \equiv 8, 40 \pmod{96}$. The construction is almost the same as Construction 5.1. The difference is that we define C_d as the set of the following $(n-8)/32$ codewords:

$$\{0, n/8+4i-1, n/4+8i-2\},\ 1 \le i \le (n-8)/32, \tag{5.6}$$

and N_{od} as the set of $\{0, n/4-5, n/2-3\}$ instead of (5.3), (5.4) for $1 \le i \le (n-8)/32-1$ and (5.5) for $1 \le i \le (n-8)/32$, where

$$(c,k) = \begin{cases} (8, (n+24)/32) \text{ if } m \equiv 0, 6, 8, 14 \pmod{24}, \\ (4, (n-8)/32) \quad \text{if } m \equiv 2, 12, 18, 20 \pmod{24}. \end{cases}$$

Then we have

$$|C| = |C_o| + |C_d| + |N_{od}| = \frac{n}{8} + \frac{n-8}{32} + \frac{n-8}{16} = \frac{7n-24}{32}.$$

Construction 5.3 The case $m \equiv 4, 10 \pmod{24}$, i.e., $n \equiv 72, 168 \pmod{384}$. In this case, we take both of $x(n/3)$ and $x(n/4)$. Let C_o be the set of $\{0, 3n/8+2, 3n/4+4\}$, (5.1) with $i \ne (n-8)/32$, and (5.2) with $i \ne (n+24)/32$, C_d be the set of (5.6) with $i \ne (n+24)/96$, and N_{od} be the set of the following $(n+8)/16$ codewords:

$$\{0, 1, n/6+1\};$$
$$\{0, n/4+2, 3n/8\};$$
$$\{0, 4i+1, n/2-4i+1\},\quad 1 \le i \le (n-8)/32-1;$$
$$\{0, n/8+4(a_i-i)-4, n/8+4a_i-4\},\quad 1 \le i \le (n-8)/32,$$

where $(a_1, a_2, \ldots, a_{(n-8)/32})$ is an $((n+24)/96+1)$-extended Skolem sequence of order $(n-8)/32$. Then it follows that

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

Construction 5.4 The case $m \equiv 16, 22 \pmod{24}$, i.e., $n \equiv 264, 360 \pmod{384}$. We take both of $x(n/3)$ and $x(n/4)$. Let C_o be the set of (5.1), and (5.2) with $i \neq (n+24)/32$, C_d be the set of (5.6) with $i \neq (n+24)/96$, and N_{od} be the set of $\{0, n/4+2, 5n/8\}$, (5.3), (5.4) for $1 \le i \le (n-8)/32-1$ and (5.5) for $1 \le i \le (n-8)/32$, where $(c, k) = (8, (5n+24)/96+1)$. Then $|C| = (7n+8)/32$ holds.

Construction 5.5 The case $m \equiv 5, 15, 21, 23 \pmod{24}$, i.e., $n \equiv 88, 248, 344, 376 \pmod{384}$. In this case, we take $x(n/4)$. Let C_o be the set of (5.1) with $i \neq (n+8)/32$ and (5.2) just as it is, C_d be the set of the following $(n-24)/32$ codewords:

$$\{0, n/8 + 4i + 1, n/4 + 8i + 2\},\ 1 \le i \le (n-24)/32, \tag{5.7}$$

and N_{od} be the set of $\{0, n/8, n/4+2\}$, $\{0, n/8+1, n/2-3\}$, (5.4) and (5.5) with $(c, k) = (6, 2)$. Then we have

$$|C| = \beta + |C_o| + |C_d| + |N_{od}| = 1 + \left(\frac{n}{8} - 1\right) + \frac{n-24}{32} + \frac{n+8}{16} = \frac{7n-8}{32}.$$

Construction 5.6 The case $m \equiv 3, 9, 11, 17 \pmod{24}$, i.e., $n \equiv 56, 152, 184, 280 \pmod{384}$. Let C_o be the set of $\{0, n/8-2, n/4-4\}$, (5.1) and (5.2) both with $i \neq (n+8)/32$, C_d be the set of (5.7) without any modification, N_{od} be the set of $\{0, n/8, 3n/8+2\}$, $\{0, n/8+1, n/2-3\}$, (5.4) and (5.5) with $(c, k) = (2, (n-8)/16)$. Note that $(a_1, a_2, \ldots, a_{(n-24)/32})$ is just a Skolem sequence of order $(n-24)/32$. Counting $x(n/4)$ in, we have $|C| = (7n-8)/32$.

In summary, by Theorem 1.1 and Theorem 4.3, we have determined the exact value of the maximum size $M(n)$ of a conflict-avoiding code of length $n = 8m$ for any positive integer m. Combining with the result obtained by Levenshtein and Tonchev [6], it is left to find $M(n)$ for odd n and for $n \equiv 4 \pmod{8}$. Finding $M(n)$ for these cases is our future work.

Acknowledgments The authors would like to thank the anonymous referees for their comments to improve the readability of the paper. A portion of this research was carried out while the first author was visiting National Chiao Tung University. She is grateful to the Department of Applied Mathematics for their generous support and hospitality. The work of M. Mishima was supported in part by JSPS Scientific Research (C)19500236, and the work of H.-L. Fu was supported in part by NSC-2115-M-009-003.

Appendix

The proof of Lemma 2.4 is given by solving the LP problem defined by (2.1)–(2.3).

(i) The case $m \equiv 0 \pmod{3}$. By introducing slack variables $x_i \ge 0$ $(i = 1, 2, \ldots, 6)$, the system (2.2) of inequalities with $(s, k_1, k_2, k_3) = (1, 0, 0, 2)$ can be replaced by

$$\begin{aligned} &|C_o| + 2|N_{oe}| + 2|N_{od}| + x_1 = \frac{n}{4}, \\ &|C_o| + |C_e| + |N_{oe}| + 2|N_e| + x_2 = \frac{n}{8}, \\ &s\alpha + k_3\beta + |C_e| + 2|C_d| + |N_{od}| + |N_e| + 3|N_d| + x_3 = \frac{n}{8}, \\ &|C_o| + x_4 = \frac{n}{8}, \\ &\alpha + x_5 = 1, \\ &\beta + x_6 = 1. \end{aligned} \tag{A1}$$

Solving the system (A1) of linear equations for variables α, β, $|C_o|$, $|C_d|$, $|N_{od}|$ and x_4, we have

$$\begin{aligned}
\alpha &= 1 - x_5,\\
\beta &= 1 - x_6,\\
|C_o| &= \frac{n}{8} - |C_e| - |N_{oe}| - 2|N_e| - x_2,\\
|C_d| &= \frac{n-48}{32} - \frac{3|C_e|}{4} + \frac{|N_{oe}|}{4} - |N_e| - \frac{3|N_d|}{2} + \frac{x_1}{4} - \frac{x_2}{4} - \frac{x_3}{2} + \frac{x_5}{2} + x_6,\\
|N_{od}| &= \frac{n}{16} + \frac{|C_e|}{2} - \frac{|N_{oe}|}{2} + |N_e| - \frac{x_1}{2} + \frac{x_2}{2},\\
x_4 &= |C_e| + |N_{oe}| + 2|N_e| + x_2.
\end{aligned}$$

Then, (2.1) can be rewritten as follows:

$$|C| = \frac{7n+16}{32} - \frac{|C_e|}{4} - \frac{|N_{oe}|}{4} - |N_e| - \frac{|N_d|}{2} - \frac{x_1}{4} - \frac{3x_2}{4} - \frac{x_3}{2} - \frac{x_5}{2}. \tag{A2}$$

Since all variables are non-negative, (A2) implies that $|C| \leq (7n+16)/32$ and the equality holds if and only if $|C_e| = |N_{oe}| = |N_e| = |N_d| = x_1 = x_2 = x_3 = x_5 = 0$ (thus $x_4 = 0$). Since $|C|$ is an integer,

$$|C| \leq \left\lfloor \frac{7n+16}{32} \right\rfloor$$

holds for the case where $n = 16m$ and $m \equiv 0 \pmod 3$.

(ii) The case $m \equiv 1, 2 \pmod 3$. The proof is analogous to the case (i). In this case, we introduce five slack variables $x_i \geq 0$ ($i = 1, 2, \ldots, 5$) and restate the system (2.2) of inequalities with $(s, k_1, k_2, k_3) = (0, 0, 0, 2)$ as follows:

$$\begin{aligned}
&|C_o| + 2|N_{oe}| + 2|N_{od}| + x_1 = \frac{n}{4},\\
&|C_o| + |C_e| + |N_{oe}| + 2|N_e| + x_2 = \frac{n}{8},\\
&k_3\beta + |C_e| + 2|C_d| + |N_{od}| + |N_e| + 3|N_d| + x_3 = \frac{n}{8},\\
&|C_o| + x_4 = \frac{n}{8},\\
&\beta + x_5 = 1.
\end{aligned} \tag{A3}$$

Solving the system (A3) of linear equations for variables β, $|C_o|$, $|C_d|$, $|N_{od}|$ and x_4, we have

$$\begin{aligned}
\beta &= 1 - x_5,\\
|C_o| &= \frac{n}{8} - |C_e| - |N_{oe}| - 2|N_e| - x_2,\\
|C_d| &= \frac{n}{32} - 1 - \frac{3|C_e|}{4} + \frac{|N_{oe}|}{4} - |N_e| - \frac{3|N_d|}{2} + \frac{x_1}{4} - \frac{x_2}{4} - \frac{x_3}{2} + x_5,\\
|N_{od}| &= \frac{n}{16} + \frac{|C_e|}{2} - \frac{|N_{oe}|}{2} + |N_e| - \frac{x_1}{2} + \frac{x_2}{2},\\
x_4 &= |C_e| + |N_{oe}| + 2|N_e| + x_2.
\end{aligned}$$

With these terms, we can rewrite (2.1) as follows:

$$|C| = \frac{7}{32}n - \frac{|C_e|}{4} - \frac{|N_{oe}|}{4} - |N_e| - \frac{|N_d|}{2} - \frac{x_1}{4} - \frac{3x_2}{4} - \frac{x_3}{2}, \tag{A4}$$

which implies that $|C| \leq 7n/32$. The equality of (A4) holds if and only if $|C_e| = |N_{oe}| = |N_e| = |N_d| = x_1 = x_2 = x_3 = 0$ (thus $x_4 = 0$). Since $|C|$ must be an integer, we have

$$|C| \leq \left\lfloor \frac{7}{32} n \right\rfloor$$

for the case where $n = 16m$ and $m \equiv 1, 2 \pmod{3}$.

References

1. Baker C.: Extended Skolem sequences. J. Combin. Des. **3**(5), 363–379 (1995).
2. Bassalygo L.A., Pinsker M.S.: Limited multiple-access of a nonsynchronous channel (in Russian). Probl. Inf. Transm. **19**(4), 92–96 (1983).
3. Györfi L., Vajda I.: Constructions of protocol sequences for multiple access collision channel without feedback. IEEE Trans. Inform. Theory **39**(5), 1762–1765 (1993).
4. Jimbo M., Mishima M., Janiszewski S., Teymorian A.Y., Tonchev V.D.: On conflict-avoiding codes of length $n = 4m$ for three active users. IEEE Trans. Inform. Theory **53**(8), 2732–2742 (2007).
5. Levenshtein V.I.: Conflict-avoiding codes for three active users and cyclic triple systems. Probl. Inf. Transm. **43**(3), 199–212 (2007).
6. Levenshtein V.I., Tonchev V.D.: Optimal conflict-avoiding codes for three active users. In: Proceedings of the IEEE International Symposium on Information Theory, Adelaide, Australia, 4–9 Sept 2005, pp. 535–537 (2005).
7. Linek V., Jiang Z.: Extended Langford sequences with small defects. J. Combin. Theory A **84**(1), 38–54 (1998).
8. Massey J.L., Mathys P.: The collision channel without feedback. IEEE Trans. Inform. Theory **31**(2), 192–204 (1985).
9. Mathys P.: A class of codes for a T active users out of N multiple-access communication system. IEEE Trans. Inform. Theory **36**(6), 1206–1219 (1990).
10. Momihara K.: Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three. Des. Codes Cryptogr. **45**(3), 379–390 (2007).
11. Momihara K., Müller M., Satoh J., Jimbo M.: Constant weight conflict-avoiding codes. SIAM J. Discrete Math. **21**(4), 959–979 (2007).
12. Nguyen Q.A., Györfi L., Massey J.L.: Constructions of binary constant-weight cyclic codes and cyclically permutable codes. IEEE Trans. Inform. Theory **38**(3), 940–949 (1992).
13. Shalaby M.: Skolem sequences: generalizations and applications. PhD Thesis, MacMaster University, Canada (1992).
14. Tsybakov B.S., Rubinov A.R.: Some constructions of conflict-avoiding codes. Probl. Inf. Transm. **38**(4), 268–279 (2002).