Strongly Conflict-Avoiding Codes

Yijin Zhang, Kenneth W. Shum and Wing Shing Wong

Abstract— **Strongly conflict-avoiding codes are used in the asynchronous multiple-access collision channel without feedback. The number of codewords in a strongly conflict-avoiding code is the number of potential users that can be supported in the system. In this paper, an upper bound on the size of strongly conflict-avoiding codes is proved. In addition, we provide an improved upper bound if the codes are all equi-difference. This bound is further shown to be tight asymptotically.**

I. Introduction

A set of M binary sequences is called (M, K)-*conflict-avoiding* [1] if every subset of K sequences out of these M sequences is user-irrepressible [2], [3]. Conflict-avoiding codes (CAC) find applications in slot-synchronous collision channel without feedback [4], [5] to guarantee the *non-blocking* property: for each active user in its active period we can find at least one packet of this user without suffering any collision.

In this paper, we consider a more general scenario, in which the collision channel is asynchronous, i.e., all users do not know the slot boundaries of the channel. Suppose that there are M potential users, but at most K of them are active at the same time. We assign statically each of the M users a binary codeword from a set of M codewords. Channel time is assumed to be partitioned into fixed-length time intervals, called *slots*. Each active user reads out the assigned codeword periodically, and sends a packet of one time slot duration if and only if the value of the codeword is equal to 1. If a packet transmission starts or ends in a channel time slot, then this slot is said to be occupied by this packet.

Since there is no feedback from the receiver and no cooperation among the users, the starting time of the codewords may be different and relative delay offsets are incurred. As the channel is asynchronous, the relative delay offset of each user is an arbitrary real number on the unit of one slot time. It implies sometimes one packet would occupy two time slots of the channel. We further assume one packet is received correctly without suffering any collision which results from completely or partially overlapping of packets, and is unrecoverable when collided.

A set of M binary codewords is called (M, K)-*strongly conflict-avoiding* (SCAC) if the non-blocking property holds in the asynchronous channel for each active user. Obviously, given M and K, the collection of all SCACs is a subset of the collection of all CACs. It is because that the the slot-synchronized channel is a special case of the asynchronous channel. In this paper, we consider a fixed codeword length and a given number of K active users, and aim at maximizing the total number of potential users that can be supported in an SCAC. Each active user may repeatedly sending the same packet in one period. The packet is guaranteed to be received successfully within the duration of its sender's active period. This viewpoint is also adopted for studying CAC in [6]–[12].

The number of ones in a binary sequence is called the *Hamming weight*, denoted by w. It is easy to see that in order to support non-blocking property, each active user has to send at least K packets in its active period, i.e., the Hamming weight of the sequence is at least K. Otherwise, if a user sends only $K - 1$ packets in a period, we can always arrange the delay offsets of the other $K - 1$ users so that all these $K - 1$ packets are in collision, violating the non-blocking property. Under the assumption of $w = K$, many works are devoted for CAC and equi-difference CAC to determine the maximal number of potential users, see e.g. [6]–[12]. In this paper, we also focus on the case $w = K$ for SCAC and equi-difference SCAC to determine the maximal number of potential users with given period.

This paper is organized as follows. We define SCAC and equi-difference SCAC with setting up some notations in Section II. The first main result in this paper is contained in Section III, which provides an upper bound on the number of potential users that can be supported in an SCAC, given the length L and Hamming weight w. Furthermore, in Section IV we present the second main result: an upper bound on the size of equi-difference SCAC. The asymptotic version of the upper bounds derived in previous sections is given respectively in Section V. In Section VI, we show the upper bound in section IV is asymptotically tight. Finally, we close in Section VII with some concluding remarks.

II. Definitions and Notations

We represent a binary sequence by specifying the time indices where the sequence value is equal to one. Let $\mathbb{Z}_L = \{0, 1, \ldots, L-1\}$ be the set of integers reduced modulo L. We use $|\mathcal{I}|$ to denote the cardinality of $\mathcal{I}$. Subsets of $\mathbb{Z}_L$ with cardinality w are called *codewords*. We sometime say that $\mathcal{I}$ is a codeword of weight w.

A subset $\mathcal{I}$ of $\mathbb{Z}_L$ is associated with a binary sequence $s(t)$ of length L with Hamming weight $|\mathcal{I}|$, by setting $s(t) = 1$ if and only if $t \in \mathcal{I}$. We also use $w_H(s)$ to denote the Hamming weight of $s(t)$. Given that the delay offset of s is an integer number τ. The *cyclic shift* of s by τ is denoted by

$$s^{(\tau)} := [s(0-\tau)\ s(1-\tau)\ \ldots\ s(L-1-\tau)]$$

with the subtraction $t - \tau$ is performed modulo L for $t = 0, 1, \ldots, L-1$. Given two sequences s_1 and s_2, define the

This work was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region under Project 417909.

Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N. T., Hong Kong. Emails: zyj007@ie.cuhk.edu.hk, wkshum@inc.cuhk.edu.hk, wswong@ie.cuhk.edu.hk.

Hamming crosscorrelation of them by

$$H_{s_1 s_2}(\tau) := \sum_{t=0}^{L-1} s_1(t)s_2(t-\tau).$$

We also define their *logical OR* as

$$(s_1 \vee s_2)(t) := \begin{cases} 1 & \text{if } s_1(t)=1 \text{ or } s_2(t)=1, \\ 0 & \text{otherwise.} \end{cases}$$

For a codeword $\mathcal{I}$, let

$$d(\mathcal{I}) := \{a-b \bmod L :\ a,b \in \mathcal{I}\}$$

denote the *set of differences* between pairs of elements in $\mathcal{I}$. Since a may equal to b in the definition of $d(\mathcal{I})$, it is obvious that 0 is always an element in $d(\mathcal{I})$. Let $d^*(\mathcal{I})$ be the set of non-zero differences in $d(\mathcal{I})$,

$$d^*(\mathcal{I}) := d(\mathcal{I}) \setminus \{0\}.$$

It is the set of differences between pairs of *distinct* elements in $\mathcal{I}$. We also make a few more definitions based on $d^*(\mathcal{I})$,

$$d^*(\mathcal{I})' := \{a-1, a+1, a \bmod L :\ a \in d^*(\mathcal{I})\}.$$

Obviously, we have $d^*(\mathcal{I})' \supseteq d^*(\mathcal{I})$.

Definition 1. A collection of M codewords

$$\mathscr{C} = \{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_M\}$$

is called a CAC of length L and weight w if

$$d^*(\mathcal{I}_j) \cap d^*(\mathcal{I}_k) = \emptyset, \tag{1}$$

or equivalently, if

$$H_{s_j s_k}(\tau) \leq 1 \tag{2}$$

for all $j \neq k$ and τ.

Definition 2. Furthermore it is called an SCAC of length L and weight w if

$$d^*(\mathcal{I}_j)' \cap d(\mathcal{I}_k) = \emptyset, \tag{3}$$

or equivalently, if

$$H_{s_j (s_k \vee s_k^{(1)})}(\tau) \leq 1 \tag{4}$$

for all $j \neq k$ and τ. We use the notation $\mathsf{SCAC}(L,w)$ for an SCAC of length L and weight w.

Remark: (a) From the property in (3), we know

$$\{1, L-1\} \not\subseteq d^*(\mathcal{I}_j)$$

as 0 is always included in $d(\mathcal{I}_k)$. One can check (3) also implies

$$\big(d^*(\mathcal{I}_j) + \{0,1\}\big) \cap \big(d^*(\mathcal{I}_k) + \{0,1\}\big) = \emptyset. \tag{5}$$

(b) From the definition of SCAC and CAC, it is easy to see an $\mathsf{SCAC}^e(L,w)$ can thus be viewed as a CAC or a subset of an $(L,w,1)$-optical orthogonal code (OOC) without any auto-correlation requirement. We refer the readers to, e.g. [13], and the references therein for further information on OOC.

Definition 3. A codeword $\mathcal{I}$ is called *equi-difference* if the elements in $\mathcal{I}$ form an arithmetic progression in $\mathbb{Z}_L$, i.e.,

$$\mathcal{I} = \{0, g, 2g, \ldots, (w-1)g\}$$

for some $g \in \mathbb{Z}_L$. In the above equation, the product jg is reduced mod L, for $j = 2, 3, \ldots, (w-1)$. The element g is called the *generator* of this codeword.

For an equi-difference codeword $\mathcal{I}$ generated by g, the set of differences is equal to

$$d(\mathcal{I}) = \{0, \pm g, \pm 2g, \ldots, \pm(w-1)g\}.$$

We remark that the elements $\pm g, \pm 2g, \ldots, \pm(w-1)g$ may not be distinct mod L. Hence in general we have $|d^*(\mathcal{I})| \leq 2w-2$, with equality holds if $\pm g$, $\pm 2g, \ldots, \pm(w-1)g$ are distinct mod L.

If all codewords in an SCAC are equi-difference, then we say this SCAC is equi-difference. We use the symbol $\mathsf{SCAC}^e(L,w)$ for an equi-difference SCAC of length L and weight w.

Example 1: $L = 30$, $w = 3$. The four codewords $\{0,10,20\}$, $\{0,2,4\}$, $\{0,14,22\}$ and $\{0,12,24\}$ constitute an $\mathsf{SCAC}^e(30,3)$. We can verify that the following

$$\begin{aligned} d(\{0,10,20\}) &= \{0,10,20\} \\ d(\{0,2,4\}) &= \{0,2,4,26,28\} \\ d(\{0,14,22\}) &= \{0,8,14,16,22\} \\ d(\{0,12,24\}) &= \{0,6,12,18,24\} \end{aligned}$$

and

$$\begin{aligned} d^*(\{0,10,20\})' &= \{9,10,11,19,20,21\} \\ d^*(\{0,2,4\})' &= \{1,2,3,4,5,25,26,27,28,29\} \\ d^*(\{0,14,22\})' &= \{7,8,9,13,14,15,16,17,21,22,23\} \\ d^*(\{0,12,24\})' &= \{5,6,7,11,12,13,17,18,19,23,24,25\}. \end{aligned}$$

satisfy the condition in (3). The SCAC is equi-difference, with generators 10, 2, 22 and 12.

Given positive integers L and w, consider the class of all $\mathsf{SCAC}(L,w)$s and $\mathsf{SCAC}^e(L,w)$s. The maximal number of codewords in an $\mathsf{SCAC}(L,w)$ is denoted by $M(L,w)$. We also use $M^e(L,w)$ for the maximal number of codewords in an $\mathsf{SCAC}^e(L,w)$. The objective of this paper is to derive upper bounds on $M(L,w)$ and $M^e(L,w)$ for all L and w.

III. Upper Bound on $M(L,w)$

A. $L < 2w^2$

The result that $M(L,w) = 0$ for $L < w$ is obvious from the definition of Hamming weight. Now we will study the case for $w \leq L < 2w^2$. We first state the following elementary property for Hamming crosscorrelation which is due to [14]. We include the short proof here for the sake of completeness.

Proposition 1 ([14]). *Let $w_H(s)$ and $w_H(s')$ be respectively the Hamming weight of given two binary sequences $s(t)$ and $s'(t)$. Then we have*

$$\sum_{\tau=0}^{L-1} H_{ss'}(\tau) = w_H(s)w_H(s').$$

Proof:

$$\begin{aligned}\sum_{\tau=0}^{L-1} H_{ss'}(\tau) &= \sum_{\tau=0}^{L-1}\sum_{t=0}^{L-1} s(t)s'(t-\tau)\\ &= \sum_{t=0}^{L-1} s(t) \sum_{\tau=0}^{L-1} s'(t-\tau)\\ &= \sum_{t=0}^{L-1} s(t) \sum_{\tau=0}^{L-1} s'(\tau) = w_H(s)w_H(s').\end{aligned}$$

■

Then we have the following tight upper bound on $M(L,w)$ for $w \le L < 2w^2$.

Theorem 2. *For $w \le L < 2w^2$,*

$$M(L,w) = 1. \tag{6}$$

Proof: Let $\mathcal{I}_j$ and $\mathcal{I}_k$ be two distinct codewords in an $\mathsf{SCAC}(L,w)$. We can find $1 \notin d(\mathcal{I}_k)$ otherwise it would violate the condition in (3) since 0 and 1 are always included in $d^*(\mathcal{I}_j)'$. Thus we have the Hamming weight of $(s_k \vee s_k^{(1)})$ is $2w$. From Proposition 1, we know

$$\sum_{\tau=0}^{L-1} H_{s_j(s_k \vee s_k^{(1)})}(\tau) = 2w^2.$$

Then with the condition $w \le L < 2w^2$, we can find some τ_0 such that

$$H_{s_j(s_k \vee s_k^{(1)})}(\tau_0) > 1,$$

which contradicts (4). Therefore, we can conclude that $M(L,w) < 2$ for $L < 2w^2$. Since (3) is vacuous for an $\mathsf{SCAC}(L,w)$ with one codeword, we further have $M(L,w) = 1$ for $w \le L < 2w^2$. ■

B. $L \ge 2w^2$

In this section we derive an upper bound on the size of SCAC for $L \ge 2w^2$ by applying Kneser's theorem [15], which is a result about the sum of subsets in an abelian group G. As we only work with $\mathbb{Z}_L$, we will state Kneser's theorem for $G = \mathbb{Z}_L$. First we introduce some more notations.

Given two non-empty subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{Z}_L$, the *sum set* and *difference set* of $\mathcal{A}$ and $\mathcal{B}$, are defined as

$$\begin{aligned}\mathcal{A}+\mathcal{B} &:= \{a+b : \, a \in \mathcal{A}, b \in \mathcal{B}\}\\ \mathcal{A}-\mathcal{B} &:= \{a-b : \, a \in \mathcal{A}, b \in \mathcal{B}\}\end{aligned}$$

respectively. The negative of $\mathcal{A}$ is defined as

$$-\mathcal{A} := \{-a : \, a \in \mathcal{A}\}.$$

Given a non-empty subset $\mathcal{S} \subseteq \mathbb{Z}_L$, an element $h \in \mathbb{Z}_L$ is called a *period* of $\mathcal{S}$ if $h+\mathcal{S} = \mathcal{S}$. The *stabilizer* of $\mathcal{S}$, denoted by $H(\mathcal{S})$, is the set of all periods of $\mathcal{S}$,

$$H(\mathcal{S}) := \{h \in \mathbb{Z}_L : \, h + \mathcal{S} = \mathcal{S}\}.$$

We note that $0 \in H(\mathcal{S})$ for every non-empty subset $\mathcal{S}$ of $\mathbb{Z}_L$, and $H(\mathcal{S})$ is a subgroup of $\mathbb{Z}_L$.

We use $\langle\alpha\rangle$ to represent the subgroup of $\mathbb{Z}_L$ generated by α, i.e.,

$$\langle\alpha\rangle := \{j\alpha \in \mathbb{Z}_L : \, j = 0,1,2,\ldots\}.$$

If α divides L, then $\langle\alpha\rangle$ consists of L/α elements.

Note that an subset $\mathcal{S}$ of $\mathbb{Z}_L$ with $|H| > 1$ can be written as the union of cosets of H,

$$\mathcal{S} = \bigcup_{a \in \mathcal{S}} (H + a).$$

As an example, consider the subset $\mathcal{S} = \{0,1,3,4\} \subset \mathbb{Z}_6$. The stabilizer of $\mathcal{S}$ is $H = \{0,3\} = \langle 3\rangle$ and $\mathcal{S}$ is a union of H and the coset $\{1,4\}$.

Lemma 3. *For any subset $\mathcal{I} \in \mathbb{Z}_L$ with $0 \in \mathcal{I}$, we have $H(\mathcal{I}) \subseteq \mathcal{I}$.*

Proof: Let h be an element in $H(\mathcal{I})$. Because $0 \in \mathcal{I}$ and $h + \mathcal{I} \subseteq \mathcal{I}$, we have $h = h + 0 \in \mathcal{I}$. This proves that the stabilizer of $\mathcal{I}$ is a subset of $\mathcal{I}$ if $0 \in \mathcal{I}$. ■

Theorem 4 (Kneser)**.** *Let $\mathcal{A}$ and $\mathcal{B}$ be non-empty subsets of $\mathbb{Z}_L$, and let $H = H(\mathcal{A}+\mathcal{B})$ be the stabilizer of $\mathcal{A}+\mathcal{B}$. If $|\mathcal{A}+\mathcal{B}| < |\mathcal{A}| + |\mathcal{B}|$, then*

$$|\mathcal{A}+\mathcal{B}| = |\mathcal{A}+H| + |\mathcal{B}+H| - |H|. \tag{7}$$

Proof of Theorem 4 can be found in [16] or [17]. We will apply Kneser's theorem through the following Corollary.

Definition 4. A codeword $\mathcal{I}$ of weight w is said to be *peculiar* if

$$|d(\mathcal{I}) + \{0,1\}| \le 3w - 2. \tag{8}$$

Corollary 5. *Let $\mathcal{I}$ be a peculiar codeword in an* $\mathsf{SCAC}(L,w)$ *and H be the stabilizer of $d(\mathcal{I}) + \{0,1\}$, then $|H| > 1$ and*

$$|d(\mathcal{I}) + \{0,1\}| = |\mathcal{I} + \{0,1\} + H| + |\mathcal{I} + H| - |H|. \tag{9}$$

Proof: Suppose that $\mathcal{I}$ is a peculiar codeword in an $\mathsf{SCAC}(L,w)$ and let H be the stabilizer of $d(\mathcal{I}) + \{0,1\}$. $|-\mathcal{I}|$ can be easily found as w. By the definition in (3), we know $1 \notin d^*(\mathcal{I})$. Thus we have $|\mathcal{I} + \{0,1\}| = 2w$. The condition in Kneser's theorem is satisfied with $\mathcal{A} = \mathcal{I} + \{0,1\}$ and $\mathcal{B} = -\mathcal{I}$, because

$$\begin{aligned}|\mathcal{I} + \{0,1\} + (-\mathcal{I})| = |d(\mathcal{I}) + \{0,1\}| &\le 3w - 2\\ &< |\mathcal{I} + \{0,1\}| + |-\mathcal{I}| = 3w.\end{aligned}$$

From (7), we obtain

$$\begin{aligned}|d(\mathcal{I}) + \{0,1\}| &= |\mathcal{I} + \{0,1\} + H| + |-\mathcal{I} + H| - |H|\\ &= |\mathcal{I} + \{0,1\} + H| + |\mathcal{I} + H| - |H|.\end{aligned}$$

In the last equality above, we have used the fact that H is an additive subgroup of $\mathbb{Z}_L$ and hence $-H = H$. This proves (9). Since $|\mathcal{I} + H| \geq w$ and $|\mathcal{I} + \{0,1\} + H| \geq 2w$, we obtain

$$|d(\mathcal{I}) + \{0,1\}| \geq 3w - |H|.$$

Thus we have

$$3w - |H| \leq |d(\mathcal{I}) + \{0,1\}| \leq 3w - 2.$$

We conclude that $|H| \geq 2$. ■

In the next theorem we give a recipe for upper bounding the size of an SCAC.

Theorem 6. *Let $\mathscr{C}$ be an $\mathsf{SCAC}(L,w)$ in which E codewords are peculiar. For $j = 1, 2, \dots, E$, denote the j-th peculiar codeword by $\mathcal{I}_j$, and let the stabilizer of $d(\mathcal{I}_j) + \{0,1\}$ be H_j. Define*

$$\Delta_j := |\mathcal{I}_j + \{0,1\} + H_j| + |\mathcal{I}_j + H_j| - 3w. \tag{10}$$

Then for $L \geq 2w^2$,

$$|\mathscr{C}| \leq \left\lfloor \frac{L - 2 + \sum_{j=1}^{E}(|H_j| - \Delta_j - 1)}{3w - 3} \right\rfloor. \tag{11}$$

Proof: By the definition in (3), we have the following

$$\big(d^*(\mathcal{I}_j) + \{0,1\}\big) \cap \big(d^*(\mathcal{I}_k) + \{0,1\}\big) = \emptyset$$

for all distinct j and k. It implies $\big(d^*(\mathcal{I}_j) + \{0,1\}\big)$ and $\big(d^*(\mathcal{I}_k) + \{0,1\}\big)$ are disjoint for any pair of distinct codewords $\mathcal{I}_j$ and $\mathcal{I}_k$ in $\mathscr{C}$.

By the definition in (3), we have $\{0, 1, L-1\} \notin d^*(\mathcal{I}_j)$. Furthermore, we have

$$\{0,1\} \nsubseteq d^*(\mathcal{I}_j) + \{0,1\}$$

for all j. We thus have the following basic inequality,

$$L - 2 \geq \sum_{\mathcal{I} \in \mathscr{C}} |d^*(\mathcal{I}_j) + \{0,1\}|. \tag{12}$$

We also know $\{0,1\} \cup (d^*(\mathcal{I}_j) + \{0,1\}) = d(\mathcal{I}_j) + \{0,1\}$ for all j, which implies

$$|d^*(\mathcal{I}_j) + \{0,1\}| = |d(\mathcal{I}_j) + \{0,1\}| - 2.$$

Thus the inequality in (12) becomes

$$L - 2 \geq \sum_{\mathcal{I} \in \mathscr{C}} (|d(\mathcal{I}_j) + \{0,1\}| - 2).$$

From Corollary 5 we get

$$\begin{aligned} L - 2 &\geq \sum_{j=1}^{E}(|\mathcal{I}_j + \{0,1\} + H_j| + |\mathcal{I}_j + H_j| - |H_j| - 2) \\ &\quad + (|\mathscr{C}| - E)(3w - 1 - 2) \\ &= \sum_{j=1}^{E}(\Delta_j - |H_j| + 3w - 2) + (|\mathscr{C}| - E)(3w - 3) \end{aligned}$$

After some rearrangement of terms, we get

$$|\mathscr{C}| \leq \frac{L - 2 + \sum_{j=1}^{E}(|H_j| - \Delta_j - 1)}{3w - 3}.$$

This finishes the proof of the theorem. ■

We introduce a few more definitions which will be useful in Theorem 7.

Definition 5. Let

$$S(L,w) := \Big\{x \in \{2, 3, \dots, 3w-2\} : x \text{ divides } L, \tag{13}$$

$$\text{and } x(\lceil w/x \rceil + \lceil 2w/x \rceil) - x \leq 3w - 2\Big\}. \tag{14}$$

$S(L,w)$ may be empty, for example when L is prime. Let $\mathscr{S}(L,w)$ be the collection of subsets of $S(L,w)$, such that each pair of distinct elements in $\mathcal{S} \in \mathscr{S}(L,w)$ are relatively prime, i.e.,

$$\mathscr{S}(L,w) := \{\mathcal{S} \subseteq S(L,w) : \gcd(i,j) = 1, \forall i, j, \in \mathcal{S}, i \neq j\}.$$

Given an integer $L \geq w \geq 2$, if $\mathscr{S}(L,w)$ is non-empty, define

$$F(L,w) := \max_{\mathcal{S} \in \mathscr{S}(L,w)} \sum_{x \in \mathcal{S}} \Big(x - 1 - x(\lceil 2w/x \rceil + \lceil w/x \rceil) + 3w\Big) \tag{15}$$

with the maximum taken over all subsets $\mathcal{S}$ in $\mathscr{S}(L,w)$. If $\mathscr{S}(L,w)$ is empty, we define $F(L,w)$ as zero. We note that the summand in (15) is positive by the condition in (14). Hence, $F(L,w)$ is non-negative.

Theorem 7. *For $L \geq 2w^2$ and $w \geq 2$,*

$$M(L,w) \leq \left\lfloor \frac{L - 2 + F(L,w)}{3w - 3} \right\rfloor. \tag{16}$$

Proof: Suppose that there are E peculiar codewords in an $\mathsf{SCAC}(L,w)$, denoted by $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_E$. For $j = 1, 2, \dots, E$, let H_j be the stabilizer of $d(\mathcal{I}_j) + \{0,1\}$. Consider two distinct codewords $\mathcal{I}_i$ and $\mathcal{I}_j$ in these E codewords. Both $|H_i|$ and $|H_j|$ are strictly larger than one by Corollary 5. We claim that $|H_i|$ and $|H_j|$ are relatively prime. As subgroups of $\mathbb{Z}_L$, H_i and H_j can be written as $\langle \alpha_i \rangle$ and $\langle \alpha_j \rangle$ respectively, for some proper divisors α_i and α_j of L, so that $|H_i| = L/\alpha_i$ and $|H_j| = L/\alpha_j$. If $|H_i|$ and $|H_j|$ are not relatively prime, say, if $b > 1$ is a common divisor of $|H_i|$ and $|H_j|$, then

$$bx_i = \frac{L}{\alpha_i}, \; bx_j = \frac{L}{\alpha_j},$$

for some integers x_i and x_j, and we get

$$b\alpha_i x_i = L = b\alpha_j x_j.$$

After dividing the above equation by b, we see that L/b is an integral multiple of both α_i and α_j, and hence is a common element in H_i and H_j. Moreover, L/b is non-zero mod L, because $b > 1$. The two stabilizers H_i and H_j thus contain a common non-zero element. By Lemma 3, we have $d(\mathcal{I}_i) + \{0,1\} \supseteq H_i$ and $d(\mathcal{I}_j) + \{0,1\} \supseteq H_j$, and so L/b is also a common non-zero element of $d(\mathcal{I}_i) + \{0,1\}$ and $d(\mathcal{I}_j) + \{0,1\}$. If $L/b = 1$, we have $\alpha_i = \alpha_j = 1$ and $|H_i| = |H_j| = L$. It implies $H_i = H_j = \{0, 1, \dots, L-1\}$ and

$$d(\mathcal{I}_i) + \{0,1\} = d(\mathcal{I}_j) + \{0,1\} = \{0, 1, \dots, L-1\},$$

which contradicts the defining property of (3). Hence nonzero L/b is not equal to one. We thus find L/b is also a common element of $d^*(\mathcal{I}_i)+\{0,1\}$ and $d^*(\mathcal{I}_j)+\{0,1\}$. This contradicts (5) which is necessary for (3), This completes the proof of the claim.

For each j, $|\mathcal{I}_j+H_j|$ is an integral multiple of $|H_j|$ because $\mathcal{I}_j+H_j$ is a union of H_j and its cosets. Furthermore, we have $|\mathcal{I}_j+H_j|$ is larger than or equal to w because $\mathcal{I}_j+H_j$ contains $\mathcal{I}_j$. Similarly, we also have $|\mathcal{I}_j+\{0,1\}+H_j|$ is an integral multiple of $|H_j|$ and is not less than $2w$ as $|\mathcal{I}_j+\{0,1\}|=2w$ which has already been noted in the proof of Corollary 5.

We thus have the following inequality,

$$|\mathcal{I}_j+\{0,1\}+H_j|+|\mathcal{I}_j+H_j|\geq |H_j|\big(\left\lceil\frac{2w}{|H_j|}\right\rceil+\left\lceil\frac{w}{|H_j|}\right\rceil\big).$$

The two parts of right hand side in the above inequality are the smallest integral multiples of $|H_j|$ which is not less than $2w$ and w respectively.

We next show that $|H_j|\in S(L,w)$, for $j=1,2,\ldots,E$. For each j, the subgroup H_j cannot have size strictly larger than $3w-2$, otherwise by Corollary 5, we have

$$\begin{aligned}|d(\mathcal{I}_j)+\{0,1\}| &= |\mathcal{I}_j+\{0,1\}+H_j|+|\mathcal{I}_j+H_j|-|H_j|\\ &\geq 2|H_j|-|H_j|\\ &= |H_j|>3w-2,\end{aligned}$$

which is a contradiction to the definition of peculiar codeword in (8). In addition, we must have $|H_j|\geq 2$ by Corollary 5. This shows that $2\leq |H_j|\leq 3w-2$.

As a subgroup of $\mathbb{Z}_L$, we see that $|H_j|$ is a divisor of L. Moreover, for $j=1,2,\ldots,E$, $|H_j|$ satisfies

$$\begin{aligned}3w-2 &\geq |d(\mathcal{I}_j)+\{0,1\}|\\ &= |\mathcal{I}_j+\{0,1\}+H_j|+|\mathcal{I}_j+H_j|-|H_j|\\ &\geq |H_j|\big(\left\lceil\frac{2w}{|H_j|}\right\rceil+\left\lceil\frac{w}{|H_j|}\right\rceil\big)-|H_j|.\end{aligned}$$

Consequently, $|H_j|$ satisfies the conditions in (13) and (14), and hence belong to the set $S(L,w)$. We have already shown that $|H_i|$ and $|H_j|$ are relatively prime for $i\neq j$. Therefore

$$\{|H_1|,|H_2|,\ldots,|H_E|\}\in\mathscr{S}(L,w).$$

For $j=1,2,\ldots,E$, let Δ_j be defined as in Theorem 6. We can upper bound $|H_j|-1-\Delta_j$, which appears in the summation in (11), by

$$|H_j|-1-\Delta_j\leq |H_j|-1-|H_j|\left\lceil\frac{w}{|H_j|}\right\rceil-|H_j|\left\lceil\frac{2w}{|H_j|}\right\rceil+3w,$$

which equals the summand in (15) with x substituted by $|H_j|$. By exhausting all possible choices of $\mathcal{S}$ in $\mathscr{S}(L,w)$, we have the following upper bound

$$\sum_{j=1}^{E}(|H_j|-1-\Delta_j)\leq F(L,w).$$

Substituting it back to (11), we have

$$|\mathscr{C}|\leq\left\lfloor\frac{L-2+F(L,w)}{3w-3}\right\rfloor$$

This completes the proof of Theorem 7. ■

p	q	r	S	F
0	0	0	$\emptyset$	0
1	0	0	$\{2\}$	1
≥ 2	0	0	$\{2,4\}$	3
0	≥ 1	0	$\{9\}$	2
1	≥ 1	0	$\{2,9\}$	3
≥ 2	≥ 1	0	$\{2,4,9\}$	5
0	0	≥ 1	$\{5\}$	1
1	0	≥ 1	$\{2,5\}$	2
≥ 2	0	≥ 1	$\{2,4,5\}$	4
0	≥ 1	≥ 1	$\{5,9\}$	3
1	≥ 1	≥ 1	$\{2,5,9\}$	4
≥ 2	≥ 1	≥ 1	$\{2,4,5,9\}$	6

TABLE I
VALUES OF $S(L,4)$ AND $F(L,4)$

We illustrate Theorem 7 with $w=4$.

Corollary 8. *Let L be an integer factorized as $2^p9^q5^r\ell$, where ℓ is not divisible by 2, 9 or 5. Then for $L\geq 32$ we have*

$$M(L,4)\leq\begin{cases}\lfloor (L-2)/9\rfloor & \textit{if } p=q=r=0,\\ \lfloor (L-1)/9\rfloor & \textit{if } p=1,q=r=0, \textit{or}\\ & \quad p=0,q=0,r\geq 1,\\ \lfloor L/9\rfloor & \textit{if } p=r=0,q\geq 1, \textit{or}\\ & \quad p=1,q=0,r\geq 1,\\ \lfloor (L+1)/9\rfloor & \textit{if } p\geq 2,q=r=0, \textit{or}\\ & \quad p=1,q\geq 1,r=0, \textit{or}\\ & \quad p=0,q\geq 1,r\geq 1,\\ \lfloor (L+2)/9\rfloor & \textit{if } p\geq 2,q=0,r\geq 1\textit{or}\\ & \quad p=1,q\geq 1,r\geq 1,\\ \lfloor (L+3)/9\rfloor & \textit{if } p\geq 2,q\geq 1,r=0\\ \lfloor (L+4)/9\rfloor & \textit{if } p\geq 2,q\geq 1,r\geq 1.\end{cases}$$

Proof: The value of $x-1-x(\lceil 2w/x\rceil+\lceil w/x\rceil)+3w$ for $x\in\{2,3,\ldots,10\}\setminus\{3,6,7\}$ is shown in the following table:

x	2	4	5	8	9	10
$x-1-x(\lceil 2w/x\rceil+\lceil w/x\rceil)+3w$	1	3	1	3	2	1

We note that 3, 6 and 7 are not shown in the above table, because they do not satisfy the condition in (14).

Since the value of $x-1-x(\lceil 2w/x\rceil+\lceil w/x\rceil)+3w$ for $x=2$ and $x=10$ are the same, we can disregard the case $x=10$ in the computation of $F(L,w)$ without affecting the result. By the same reason, we can ignore the case $x=8$. We tabulate $S(L,4)$ and $F(L,4)$ in Table I. By Theorem 7, we get

$$M(L,4)\leq\left\lfloor\frac{L-2+F(L,4)}{9}\right\rfloor.$$

The upper bound in Corollary 8 is obtained after tidying up the data in Table I. ■

IV. Upper Bound on $M^e(L,w)$

The result in Theorem 2 can be applied for the upper bound on $M^e(L,w)$ if $L<2w^2$. This section will be devoted to establishing an upper bound on $M^e(L,w)$ for $L\geq 2w^2$.

Definition 6. We adopt the terminology in [8] and say that a codeword $\mathcal{I}$ of weight w is *exceptional* if

$$|d^*(\mathcal{I})| < 2w-2, \tag{17}$$

or equivalently, if

$$|d(\mathcal{I})| \le 2w-2. \tag{18}$$

From the discussion above, we see that if a codeword $\mathcal{I}$ is equi-difference with generator g, then it is exceptional if and only if $\pm g$, $\pm 2g, \ldots, \pm(w-1)g$ are *not* distinct mod L.

Lemma 9. *Let $\mathcal{I}$ of weight w be an exceptional and equi-difference codeword with generator g, then we have*

(i) g is not relatively prime to L;

(ii) $d(\mathcal{I})$ is a subgroup of $\mathbb{Z}_L$.

Proof: If an equi-difference $\mathcal{I}$ is exceptional, i.e., $|d(\mathcal{I})| \le 2w-2$, then there exists two distinct integers m_1 and m_2 ranged in $[-(w-1), w-1]$ satisfying

$$m_1 g = m_2 g \mod L$$

which implies g is not relatively prime to L.

By the above equation, we further have

$$tg = 0 \mod L$$

for $t = |m_1 - m_2|$ and

$$d(\mathcal{I}) = \{0, g, \ldots, (t-1)g\}.$$

from which we find $d(\mathcal{I})$ is a subgroup of $\mathbb{Z}_L$. ■

We illustrate Lemma 9 using Example 1.

Example 1 continued: The equi-difference codeword generated by 10 is exceptional, because

$$|d^*(\{0,10,20\})| = |\{10,20\}| = 2 < 2\cdot 3 - 2.$$

We can verify that $d(\{0,10,20\})| = \{0,10,20\}$ is a subgroup of $\mathbb{Z}_{30}$.

Lemma 10. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be two distinct exceptional codewords in an* $\mathsf{SCAC}^e(L,w)$*. Then $|d(\mathcal{I}_1)|$ and $|d(\mathcal{I}_2)|$ are two distinct relatively prime integers between w and $2w-2$ such that they both divide L.*

Proof: First by Lemma 9 we know $|d(\mathcal{I}_1)|$ and $|d(\mathcal{I}_2)|$ are both subgroups of $\mathbb{Z}_L$ and thus both divide L. If $|d(\mathcal{I}_1)|$ and $|d(\mathcal{I}_2)|$ are not relatively prime, as proved in Theorem 7, we find $d(\mathcal{I}_1)$ and $d(\mathcal{I}_2)$ contain a common non-zero element. This contradicts the defining property in (3). Here, they can also be found in the range $[w, 2w-2]$ from the definition of exceptional codes. This completes the proof of Lemma 10. ■

Definition 7. A codeword $\mathcal{I}$ is said to be *dispersive* if any two distinct elements in $d(\mathcal{I})$ are not consecutive. Otherwise, it is *non-dispersive*.

Lemma 11. *Let $\mathcal{I}$ of weight w be a non-dispersive and equi-difference codeword with generator g. If there are k $(k>0)$ pairs of consecutive elements in $d(\mathcal{I})$, then we have*

(i)

$$(2w-k-1)g = 1 \textit{ or} -1 \mod L \tag{19}$$

with $k \le w-1$;

(ii) g and $2w-k-1$ are both relatively prime to L;

(iii) $\mathcal{I}$ is non-exceptional.

Proof: If there are k $(k>0)$ pairs of consecutive elements in $d(\mathcal{I})$, then there exists at least one solution of m in $[-2w+2, 2w-2]$ for the following:

$$mg = 1 \mod L. \tag{20}$$

We first have g and m are both relatively prime to L, otherwise (20) does not hold. Then by the condition g is relatively prime to L, we find there exists at most one solution of m in $[-2w+2, 2w-2]$ for (20).

Furthermore, the solution range of $[-w+1, w-1]$ can be ruled out here, otherwise we can find $1 \in d(\mathcal{I})$ which violate the condition in (3). Hence we must have one unique solution of m in $[w, 2w-2] \cup [-2w+2, -w]$. The value of m can be easily found as $2w-k-1$ or $-(2w-k-1)$ from $d(\mathcal{I}) = \{0, g, \ldots, (w-1)g\}$. Then $2w-k-1$ is also relatively prime to L. From the range of m, we proves $k \le w-1$.

In addition, we obtain $\mathcal{I}$ must be non-exceptional, otherwise g is not relative prime to L following (i) of Lemma 9, which contradicts the condition g is relatively prime to L for non-dispersive $\mathcal{I}$. ■

We illustrate Lemma 11 by the following example.

Example 2: $L = 28$, $w = 3$. The three codewords $\{0,2,4\}$, $\{0,7,14\}$ and $\{0,9,18\}$ constitute an $\mathsf{SCAC}^e(28,3)$. We can verify that the following holds for (3).

$$\begin{aligned} d(\{0,2,4\}) &= \{0,2,4,24,26\} \\ d(\{0,7,14\}) &= \{0,7,14,21\} \\ d(\{0,9,18\}) &= \{0,9,10,18,19\}. \end{aligned}$$

The SCAC is equi-difference, with generators 2, 7 and 9. The codeword generated by 9 is non-dispersive, because $(9,10)$ and $(18,19)$ are two pairs of consecutive elements in $d(\{0,9,18\})$. Furthermore, one can check

$$(2\cdot 3 - 2 - 1)\cdot 9 = -1 \mod 28$$

with $k = 2 \le 3-1$, 9 and $2\cdot 3 - 2 - 1 = 3$ are both relatively prime to 28.

Lemma 12. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be two distinct non-dispersive codewords in an* $\mathsf{SCAC}^e(L,w)$*. If there are k_1 and k_2 pairs of consecutive elements respectively in $d(\mathcal{I}_1)$ and $d(\mathcal{I}_2)$, then $2w-k_1-1$ and $2w-k_2-1$ are two distinct relatively prime integers between w and $2w-2$ such they are both relatively prime to L.*

Proof: Let g_1 and g_2 be the generator of $\mathcal{I}_1$ and $\mathcal{I}_2$ respectively. By Lemma 11, if there are k_1 and k_2 pairs of consecutive elements respectively in $d(\mathcal{I}_1)$ and $d(\mathcal{I}_2)$, then we have the following result for $\mathcal{I}_1$ and $\mathcal{I}_2$ respectively.

First, we know $2w-k_1-1$ and $2w-k_2-1$ are both relatively prime to L. By letting $r_1 = 2w-k_1-1$, we have the following two possible cases for $\mathcal{I}_1$.

$$r_1 g_1 = 1 \bmod L; \tag{21}$$

$$r_1 g_1 = -1 \bmod L. \tag{22}$$

By letting $r_2 = 2w - k_2 - 1$, we also have the following two possible cases for $\mathcal{I}_2$.

$$r_2 g_2 = 1 \bmod L; \tag{23}$$

$$r_2 g_2 = -1 \bmod L. \tag{24}$$

Consider (21) and (23) first. Combining them we have

$$r_1 g_1 - r_2 g_2 = 0 \bmod L.$$

Let v_1 be the largest common factor of r_1 and r_2. Now we will prove $v_1 = 1$ by contradiction. v_1 is relatively prime to L from the fact that r_1 and r_2 are both relatively prime to L. Given v_1, we thus have

$$(r_1/v_1)g_1 = (r_2/v_1)g_2 \bmod L.$$

If $v_1 > 1$, we can find (r_1/v_1) and (r_2/v_1) are both smaller than w from $r_1, r_2 \leq 2w - 2$. It further implies that there is a common element between $d^*(\mathcal{I}_1)$ and $d^*(\mathcal{I}_2)$, which contradicts the condition in (3). Therefore we find that $v_1 = 1$, i.e., r_1 and r_2 are relatively prime.

Then consider (21) and (24). Combining them we have

$$r_1 g_1 + r_2 g_2 = 0 \bmod L.$$

We also can find r_1 and r_2 are relatively prime. The proof is similar. Given v_1, we thus have

$$(r_1/v_1)g_1 = L - (r_2/v_1)g_2 \bmod L.$$

If $v_1 > 1$, we can find (r_1/v_1) and (r_2/v_1) are both smaller than w. It further implies that there is a common element between $d^*(\mathcal{I}_1)$ and $d^*(\mathcal{I}_2)$, which contradicts (3). Therefore from (21) and (24) we also find that $v_1 = 1$.

For (22) and (23), similarly we also can get that r_1 and r_2 are relatively prime. The result is also true for (22) and (24).

Therefore, by the above argument we can conclude that r_1 and r_2 must be relatively prime. We further obtain $2w - k_1 - 1$ and $2w - k_2 - 1$ are two distinct relatively prime integers between w and $2w - 2$ such they are both relatively prime to L. ■

The next theorem establishes an upper bound on the size of an equi-difference SCAC.

Theorem 13. *Let $\mathscr{C}$ be an $\mathsf{SCAC}^e(L, w)$ in which E_1 codewords are exceptional and E_2 codewords are non-dispersive. For $j = 1, 2, \dots, E_1$, denote the j-th exceptional codeword by $\mathcal{I}_j$, and let the stabilizer of $d(\mathcal{I}_j)$ be H_j. For $j = 1, 2, \dots, E_2$, denote the j-th non-dispersive codeword by $\mathcal{J}_j$, and let the number of pairs of consecutive elements in $d(\mathcal{J}_j)$ be k_j. Then for $L \geq 2w^2$,*

$$|\mathscr{C}| \leq \left\lfloor \frac{L - 2 + 2\sum_{j=1}^{E_1}(2w - |d(\mathcal{I}_j)| - 1) + \sum_{j=1}^{E_2} k_j}{4w - 4} \right\rfloor. \tag{25}$$

Proof: From (iii) of Lemma 11, we know in an $\mathsf{SCAC}^e(L, w)$, the set of exceptional codewords and the set of non-dispersive codewords are mutually exclusive.

Let the number of non-exceptional and dispersive codewords be N. Since any two elements in $d(\mathcal{I})$ are not consecutive and $d^*(\mathcal{I}) = 2w - 2$ for each non-exceptional and dispersive equi-difference codeword $\mathcal{I}$, by definition we have the following inequality:

$$L - 2 \geq 2N(2w - 2) + \sum_{j=1}^{E_1} 2|d^*(\mathcal{I}_j)| + \sum_{j=1}^{E_2}(4w - 4 - k_j).$$

By the fact that $|d^*(\mathcal{I}_j)| = |d(\mathcal{I}_j)| - 1$, the above inequality becomes:

$$\begin{aligned} L - 2 &\geq 2N(2w - 2) + \sum_{j=1}^{E_1} 2(|d(\mathcal{I}_j)| - 1) + \sum_{j=1}^{E_2}(4w - 4 - k_j) \\ &= 2(N + E_1 + E_2)(2w - 2) \\ &\quad - 2\sum_{j=1}^{E_1}(2w - |d(\mathcal{I}_j)| - 1) - \sum_{j=1}^{E_2} k_j \end{aligned}$$

After some rearrangement of terms, we get

$$\begin{aligned} |\mathscr{C}| &= N + E_1 + E_2 \\ &\leq \frac{L - 2 + 2\sum_{j=1}^{E_1}(2w - |d(\mathcal{I}_j)| - 1) + \sum_{j=1}^{E_2} k_j}{2(2w - 2)}. \end{aligned}$$

This finishes the proof of the theorem. ■

We make a few more definitions which will be useful in Theorem 14.

Definition 8. Let

$$S_1(L, w) := \Big\{ x \in \{w, w + 1, \dots, 2w - 2\} : x \text{ divides } L \Big\} \tag{26}$$

$S_1(L, w)$ may be empty, for example when L is prime. Let

$$S_2(L, w) := \Big\{ x \in \{w, w + 1, \dots, 2w - 2\} : \gcd(x, L) = 1 \Big\} \tag{27}$$

Let $\mathscr{S}_1(L, w)$ be the collection of subsets of $S_1(L, w)$, such that each pair of distinct elements in $\mathcal{S}_1 \in \mathscr{S}_1(L, w)$ are relatively prime, i.e.,

$$\begin{aligned} \mathscr{S}_1(L, w) := \{\mathcal{S}_1 \subseteq S_1(L, w) : &\gcd(i, j) = 1, \\ &\forall i, j, \in \mathcal{S}_1, i \neq j\}. \end{aligned}$$

Let $\mathscr{S}_2(L, w)$ be the collection of subsets of $S_2(L, w)$, such that each pair of distinct elements in $\mathcal{S}_2 \in \mathscr{S}_2(L, w)$ are relatively prime, i.e.,

$$\begin{aligned} \mathscr{S}_2(L, w) := \{\mathcal{S}_2 \subseteq S_2(L, w) : &\gcd(i, j) = 1, \\ &\forall i, j, \in \mathcal{S}_2, i \neq j\}. \end{aligned}$$

Given an integer $L \geq w \geq 2$, if $\mathscr{S}_1(L, w)$ is non-empty, define

$$F_1(L, w) := \max_{\mathcal{S}_1 \in \mathscr{S}_1(L, w)} \sum_{x \in \mathcal{S}_1} (2w - x - 1) \tag{28}$$

with the maximum taken over all subsets $\mathcal{S}_1$ in $\mathscr{S}_1(L, w)$. If $\mathscr{S}_1(L, w)$ is empty, we define $F_1(L, w)$ as zero. We note that the summand in (28) is positive by the condition in (26). Hence, $F_1(L, w)$ is non-negative.

p	q	r	S_1	S_2	F_1, F_2	$2F_1 + F_2$
0	0	0	$\emptyset$	$\{4,5,6\}$	$0,5$	5
1	0	0	$\emptyset$	$\{5\}$	$0,2$	2
≥ 2	0	0	$\{4\}$	$\{5\}$	$3,2$	8
0	≥ 1	0	$\emptyset$	$\{4,5\}$	$0,5$	5
1	≥ 1	0	$\{6\}$	$\{5\}$	$1,2$	4
≥ 2	≥ 1	0	$\{4,6\}$	$\{5\}$	$3,2$	8
0	0	≥ 1	$\{5\}$	$\{4,6\}$	$2,3$	7
1	0	≥ 1	$\{5\}$	$\emptyset$	$2,0$	4
≥ 2	0	≥ 1	$\{4,5\}$	$\emptyset$	$5,0$	10
0	≥ 1	≥ 1	$\{5\}$	$\{4\}$	$2,3$	7
1	≥ 1	≥ 1	$\{5,6\}$	$\emptyset$	$3,0$	6
≥ 2	≥ 1	≥ 1	$\{4,5,6\}$	$\emptyset$	$5,0$	10

TABLE II
VALUES OF $S_1(L,4), S_2(L,4), F_1(L,4)$ AND $F_2(L,4)$

Similarly, we also define the following if $\mathscr{S}_2(L,w)$ is non-empty for a given integer $L \geq w \geq 2$,

$$F_2(L,w) := \max_{\mathcal{S}_2 \in \mathscr{S}_2(L,w)} \sum_{x \in \mathcal{S}_2} (2w - x - 1) \qquad (29)$$

Theorem 14. *For $L \geq 2w^2$ and $w \geq 2$,*

$$M^e(L,w) \leq \left\lfloor \frac{L - 2 + 2F_1(L,w) + F_2(L,w)}{4w-4} \right\rfloor . \qquad (30)$$

Proof: Following Lemma 10, we have

$$\sum_{j=1}^{E_1} (2w - |d(\mathcal{I}_j)| - 1) \leq F_1(L,w).$$

Following Lemma 12, we have

$$\sum_{j=1}^{E_2} k_j \leq F_2(L,w).$$

Substituting them back to (25), we have

$$M^e(L,w) \leq \left\lfloor \frac{L - 2 + 2F_1(L,w) + F_2(L,w)}{4w-4} \right\rfloor .$$

This completes the proof of Theorem 14. ■

We illustrate Theorem 14 with $w = 4$.

Corollary 15. *Let L be an integer factorized as $2^p 3^q 5^r \ell$, where ℓ is not divisible by 2, 3 or 5. Then for $L \geq 32$ we have*

$$M^e(L,4) \leq \begin{cases} \lfloor L/12 \rfloor & \textit{if } p=1, q=r=0, \\ \lfloor (L+2)/12 \rfloor & \textit{if } p=1, q \geq 1, r=0, \textit{or} \\ & \ p=1, q=0, r \geq 1, \\ \lfloor (L+3)/12 \rfloor & \textit{if } p=r=0, q \geq 0 \\ \lfloor (L+4)/12 \rfloor & \textit{if } p=1, q \geq 1, r \geq 1, \\ \lfloor (L+5)/12 \rfloor & \textit{if } p=0, q \geq 0, r \geq 1 \\ \lfloor (L+6)/12 \rfloor & \textit{if } p \geq 2, q \geq 0, r=0 \\ \lfloor (L+8)/12 \rfloor & \textit{if } p \geq 2, q \geq 0, r \geq 1. \end{cases}$$

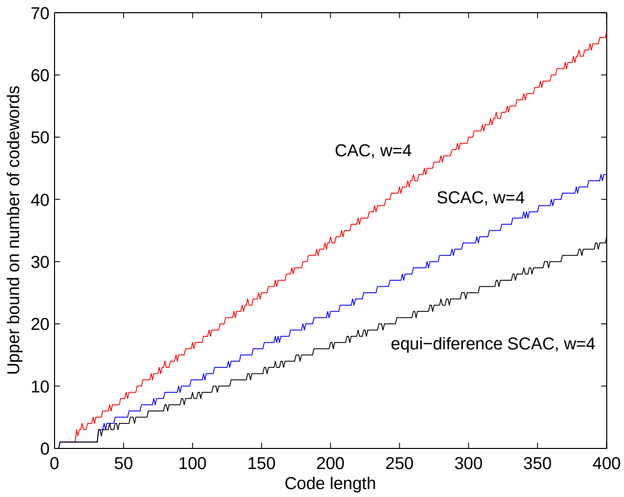

Fig. 1. Upper bounds on size of CAC, SCAC and equi-difference SCAC for weight 4.

Proof: We tabulate $S_1(L,4)$, $S_2(L,4)$, $F_1(L,4)$ and $F_2(L,4)$ in Table II. By Theorem 14, we get

$$M^e(L,4) \leq \left\lfloor \frac{L - 2 + 2F_1(L,4) + F_2(L,4)}{12} \right\rfloor .$$

The upper bound in Corollary 15 is obtained after applying the data in Table II to the above inequality case by case. ■

Example 3: $L = 74$, $w = 4$. The following six codewords constitute an SCAC$^e(74,4)$:

$$\{0,2,4,6\}, \{0,16,32,48\},$$
$$\{0,20,40,60\}, \{0,12,24,36\},$$
$$\{0,22,44,66\}, \{0,28,56,10\}.$$

We find this SCAC enjoys maximum code size of SCAC$^e(74,4)$, since $M^e(74,4) \leq \lfloor 74/12 \rfloor = 6$ following Corollary 15.

V. ASYMPTOTIC UPPER BOUNDS

The value of $F(L,w)$ in Theorem 7 can be computed by linear programming as follows. For each element i in $S(L,w)$, define a variable z_i. Let the objective function be $\sum_{i \in S(L,w)} c_i z_i$, with c_i defined by

$$c_i := i - 1 - i(\lceil w/i \rceil + \lceil 2w/i \rceil) + 3w.$$

For each prime number p between 2 and $3w-2$, impose a constraint

$$\sum_{p|i} z_i \leq 1, \qquad (31)$$

where the summation is taken over all i that is divisible by p. Then $F(L,w)$ is the optimal solution if we maximize $\sum_{i \in S(L,w)} c_i z_i$ subjective to the constraint in (31) for p ranging over all prime numbers between 2 and $3w-2$, and $0 \leq z_i \leq 1$ for all $i \in S(L,w)$. Using the linear programming, the upper bounds on $M(L,w)$ given by Theorem 7 for weight 4 and length between 32 and 400 are plotted in Fig. 1.

The value for length smaller than 32 is found directly by Theorem 2.

By similar linear programming, the value of $F_1(L,w)$ and $F_2(L,w)$ in Theorem 14 can both be obtained. The upper bound on $M^e(L,w)$ given by Theorem 14 for weight 4 and length between 32 and 400 are also contained in Fig. 1.

The upper bounds on size of CAC are due to [18]. We plot the value for weight 4 in Fig. 1 for the convenience of the readers to compare with SCAC and equi-difference SCAC.

The computation of $F(L,w)$, $F_1(L,w)$ and $F_2(L,w)$ amounts to solving a linear programming, and it is not obvious from (15), (28) and (29) how to get an estimate on the value of them. The next theorem gives an upper bound on $F(L,w)$, $F_1(L,w)$ and $F_2(L,w)$ in closed-form expression, from which we can analyze the asymptotic growth rate of upper bounds on $M(L,w)$ and $M^e(L,w)$ respectively.

Given a positive integer $x \geq 2$, let $\pi(x)$ denote the number of distinct prime numbers between 2 and x,

$$\pi(x) := |\{i : 2 \leq i \leq x, i \text{ is prime}\}|.$$

Note that $\pi(x)$ also counts the maximum number of relatively prime integers between 2 and x.

Theorem 16. *For $L \geq 2w^2$ and $w \geq 2$, we have*

$$M(L,w) \leq \left\lfloor \frac{L-2}{3w-3} + \frac{\pi(3w-2)}{3} \right\rfloor, \tag{32}$$

$$M^e(L,w) \leq \left\lfloor \frac{L-2}{4w-4} + \frac{3\pi(2w-2)}{4} \right\rfloor. \tag{33}$$

Proof: Recall that $F(L,w)$ is the maximum of

$$\sum_{x\in\mathcal{S}} (x - 1 - x(\lceil w/x\rceil + \lceil 2w/x \rceil) + 3w), \tag{34}$$

taken over all subsets $\mathcal{S}$ in $\mathscr{S}(L,w)$. For $x/2 < w \leq x$, we observe that

$$\begin{aligned} x - 1 - x(\lceil w/x\rceil + \lceil 2w/x \rceil) + 3w &= x - 1 - 3x + 3w \\ &= 3w - 2x - 1 \\ &\leq w - 1, \end{aligned}$$

and for $w > x$, we have

$$\begin{aligned} x - 1 - x(\lceil w/x\rceil + \lceil 2w/x \rceil) + 3w &\leq x - 1 - x(3w/x) + 3w \\ &= x - 1 < w - 1, \end{aligned}$$

and for $w \leq x/2$, we have

$$\begin{aligned} x - 1 - x(\lceil w/x\rceil + \lceil 2w/x \rceil) + 3w &\leq x - 1 - 2x + 3w \\ &= 3w - x - 1 \leq w - 1. \end{aligned}$$

In summary, we obtain

$$x - 1 - x(\lceil w/x\rceil + \lceil 2w/x \rceil) + 3w \leq w - 1$$

for all $x \in S(L,w)$.

The number of summands in (34) is less than or equal to the maximum number of relatively prime integers in $S(L,w)$. Since $S(L,w) \subseteq \{2,3,\ldots,3w-2\}$, the number of summands in (34) is less than or equal to the maximal number of relatively prime integers between 2 and $3w-2$, namely $\pi(3w-2)$. The summation in (34) is thus less than or equal to $(w-1)\pi(3w-2)$, and hence

$$F(L,w) \leq (w-1)\pi(3w-2).$$

The result of (32) in Theorem 16 follows by replacing $F(L,w)$ by $(w-1)\pi(3w-2)$ in Theorem 7.

Now we will prove (33) in Theorem 16. From the definition of $S_1(L,w)$, we obtain

$$2w - x - 1 \leq w - 1$$

for all $x \in S_1(L,w)$.

The number of summands in (28) is less than or equal to the maximum number of relatively prime integers in $S_1(L,w)$. Since $S_1(L,w) \subseteq \{w, w+1, \ldots, 2w-2\}$, the number of summands in (28) is less than or equal to the maximal number of relatively prime integers between 2 and $2w-2$, namely $\pi(2w-2)$. The summation in (28) is thus less than or equal to $(w-1)\pi(2w-2)$, and hence

$$F_1(L,w) \leq (w-1)\pi(2w-2).$$

By the same argument, we also can find

$$F_2(L,w) \leq (w-1)\pi(2w-2).$$

Inequity (33) follows by replacing $F_1(L,w)$ and $F_2(L,w)$ by $(w-1)\pi(2w-2)$ in Theorem 14. ■

The following is an asymptotical version of Theorem 16 which implies for each w, the growth of $M(L,w)$ and $M^e(L,w)$ are roughly linear in L, with slope $(3w-3)^{-1}$ and $(4w-4)^{-1}$ respectively.

Theorem 17. *For $w \geq 2$, we have*

$$\limsup_{L\to\infty} \frac{M(L,w)}{L} \leq \frac{1}{3w-3}, \tag{35}$$

$$\limsup_{L\to\infty} \frac{M^e(L,w)}{L} \leq \frac{1}{4w-4}. \tag{36}$$

Proof: A weaker form of the prime number theorem proved by Chebyshev [19] states that for some constants $B_1 < 1$ and $B_2 > 1$, we can bound $\pi(x)$ by

$$B_1 \frac{x}{\log(x)} < \pi(x) < B_2 \frac{x}{\log(x)},$$

for all x. Furthermore, we can take $B_2 = 1.25506$ [20].

Hence, we have the following by dividing L on both sides in (32):

$$\frac{M(L,w)}{L} \leq \left\lfloor \frac{L-2}{(3w-3)L} + \frac{1.25506(3w-2)}{3L\log(3w-2)} \right\rfloor.$$

The result in (35) follows from taking lim sup on both sides. We also can find (36) by the similar argument. ■

VI. Tightness of Asymptotic Upper Bound on $M^e(L,w)$

In this section, we will show that for each w, there exists an $\mathsf{SCAC}^e(L,w)$ asymptotically achieving the upper bound in (36) of Theorem 17. First we introduce the following method to construct $\mathsf{SCAC}(L,w)$ from CAC.

Theorem 18. *If there exists a (M,w)-CAC with period l, then there exists an $\mathsf{SCAC}(2l,w)$ with M codewords.*

Proof: By doubling all elements in each $\mathcal{I}$ of a given (M,w)-CAC and period l, we can construct a new (M,w)-CAC with period $2l$. All elements in the set of differences of each codeword in this new CAC can be found as even. We thus have

$$d^*(\mathcal{I}_j)' \cap d(\mathcal{I}_k) = \emptyset$$

for all $j \neq k$. It implies the new CAC is an $\mathsf{SCAC}^e(2l,w)$ with M codewords. ■

The following asymptotic result of CAC is due to [12]. It can be used to directly construct asymptotically optimal $\mathsf{SCAC}^e(L,w)$.

Theorem 19 ([12, Prop. 3])**.** *There exists an equi-difference CAC with $\Phi(w)$ codewords for any $w \geq 2$ such that*

$$\limsup_{L\to\infty} \frac{\Phi(L,w)}{L} \geq \frac{1}{2w-2}.$$

For general w, we have the following

Theorem 20. *For $w \geq 2$,*

$$\limsup_{L\to\infty} \frac{M^e(L,w)}{L} = \frac{1}{4w-4}.$$

Proof: Following Theorem 18 and Theorem 19, we have

$$\limsup_{L\to\infty} \frac{M^e(L,w)}{L} \geq \frac{1}{4w-4}.$$

This shows that the asymptotic lower bound in (36) is tight and proves Theorem 20. ■

VII. Conclusion

In this paper, we introduce SCAC used in the asynchronous multiple-access collision channel without feedback. It is a special class of CAC, which is for the slot-synchronous channel. We obtain upper bounds on the size of SCAC and equi-difference SCAC, which hold for all weights in general.

For each w, we find the asymptotic upper bounds on $M(L,w)$ and $M^e(L,w)$ are linear in L, with slope $(3w-3)^{-1}$ and $(4w-4)^{-1}$ respectively. By constructing asymptotically optimal equi-difference SCAC with existing CAC, we show that the asymptotic upper bound on $M^e(L,w)$ is tight. However, the tightness of upper bound on $M(L,w)$ is still unknown and would be a challenging direction for further studies.

References

[1] B. S. Tsybakov and A. R. Rubinov, "Some constructions of conflict-avoiding codes," *Problemy Peredachi Informatsii*, vol. 38, no. 4, pp. 268–279, 2002, [Problem of Inform. Trans. (English Transl.) pp.268–279].

[2] W. S. Wong, "New protocol sequences for random access channels without feedback," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2060–2071, Jun. 2007.

[3] K. W. Shum, W. S. Wong, C. W. Sung, and C. S. Chen, "Design and construction of protocol sequences: Shift invariance and user irrepressibility," in *IEEE Int. Symp. Inform. Theory*, Seoul, Jun. 2009, pp. 1368–1372.

[4] B. S. Tsybakov and N. B. Likhanov, "Packet communication on a channel without feedback," *Problemy Peredachi Informatsii*, vol. 19, no. 2, pp. 69–84, 1983, [Problem of Inform. Trans. (English Transl.) pp.147–161].

[5] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. 31, no. 2, pp. 192–204, Mar. 1985.

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

[7] V. I. Levenshtein, "Conflict-avoiding codes and cyclic triple systems," *Problems of Information Transmission*, vol. 43, no. 3, pp. 199–212, 2007.

[8] 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.

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

[10] 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, pp. 2732–2742, Aug. 2007.

[11] M. Mishima, H.-L. Fu, and S. Uruno, "Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3," *Design, Codes and Cryptography*, vol. 52, pp. 275–291, 2009.

[12] K. W. Shum and W. S. Wong, "A tight asymptotic bound on the size of constant-weight conflict-avoiding codes," *Des. Codes Cryptogr.*, 2010, DOI 10.1007/s10623-009-9345-4, to be published.

[13] R. Fuji-Hara and Y. Miao, "Optical orthgonal codes: their bounds and new optimal construction," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2396–2406, Nov. 2000.

[14] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, 1980.

[15] M. Kneser, "Abschätzungen der asymptotischen dichte von summenmengen," *Math. Zeit.*, vol. 58, pp. 459–484, 1953.

[16] H. B. Mann, *Addition Theorems: the Addition Theorems of Group Theory and Number Theory*. New York: Interscience Publisher, 1965.

[17] M. B. Nathanson, *Additive Number Theory – Inverse Problems and Geometry of Sumsets*, ser. Graduate Texts in Mathematics. New York: Springer-Verlag, 1996, no. 165.

[18] K. W. Shum, W. S. Wong, and C. S. Chen, "A general upper bound on the size of constant-weight conflict-avoiding codes," *to appear in IEEE Trans. Inform. Theory*.

[19] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed. Oxford: Oxford University Press, 2008.

[20] J. B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers," *Illinois J. Math.*, vol. 6, pp. 64–94, 1962.