A General Upper Bound on the Size of Constant-Weight Conflict-Avoiding Codes

Kenneth W. Shum, *Member, IEEE*, Wing Shing Wong, *Fellow, IEEE*, and Chung Shue Chen, *Member, IEEE*

Abstract—Conflict-avoiding codes are used in the multiple-access collision channel without feedback. The number of codewords in a conflict-avoiding code is the number of potential users that can be supported in the system. In this paper, a new upper bound on the size of constant-weight conflict-avoiding codes is proved. This upper bound is general in the sense that it is applicable to all code lengths and all Hamming weights. Several existing constructions for conflict-avoiding codes, which are known to be optimal for Hamming weights equal to four and five, are shown to be optimal for all Hamming weights in general.

Index Terms—Conflict-avoiding code, optical orthogonal code, protocol sequence.

I. INTRODUCTION

A set of k binary sequences of length L is called *user-irrepressible* [20] if after cyclically shifting each of them and stacking them together in a $k \times L$ matrix, we can always find a $k \times k$ submatrix which is a permutation matrix, regardless of how we shift the k sequences. (Recall that a permutation matrix is a zero-one square matrix with exactly one 1 in each row and each column [6, p. 25].) A set of N binary sequences is called (N, k)-*conflict-avoiding* [22] if every subset of k sequences out of these N sequences is user-irrepressible.

User-irrepressible and conflict-avoiding sequences find applications in collision channel without feedback [13], [21]. In a system with k active users, the collision channel is a deterministic channel with k inputs and one output defined as follows. Time is assumed to be partitioned into fixed-length time intervals, called *slots*. Here, we consider the *slot-synchronous* case. In each slot, each user either remains silent or transmits a packet. If exactly one user transmits in a time slot, then the packet is successfully received and the channel output is the same as the packet sent by that user. If two or more users transmit in the same time slot, a collision occurs and the channel output is an erasure symbol "*". If none of the users transmits in a time slot, the time slot is idle.

Suppose that there are N potential users, but at most k of them are active at the same time. This model is applicable to communication system in which traffic is bursty and the users transmit signal intermittently. We assign statically each of the N users a binary sequence from a set of (N, k)-conflict-avoiding sequences. Each active user reads out the assigned sequence periodically, and sends a packet if and only if the value of the sequence is equal to 1. Since there is no timing information other than that for slot synchronization, the starting time of the sequences may be different and relative delay offsets are incurred. The user-irrepressible property translates to the following non-blocking property: for each active user we can find at least one time slot in a period in which this user transmits a packet while the remaining $k - 1$ active users are silent, i.e., each active user can transmit at least one packet without collision in L time slots. This provides a worst-case guarantee of bounded delay.

There are two different but complementary design goals in the literature of user-irrepressible and conflict-avoiding sequences. In the first one, we consider the scenario in which all the N users are active, i.e., $N = k$, and we aim at minimizing the length of the binary sequences while keeping the user-irrepressible property [2], [20]. We can add an inner code, such as Reed-Solomon code, in order to recover collided packets and enhance system throughput. In the second one, we consider a fixed sequence length and a given number of k active users, and aim at maximizing the total number of potential users that can be supported. Each active may repeatedly sending the same packet in one sequence period. The packet is guaranteed to be received successfully within the duration of a period. This viewpoint is adopted in [8], [10], [11], [14]–[16]. In this paper, we consider the second design goal and maximize the number of potential users for a given sequence length. Other coding constructions for multiple access in collision channel without feedback, such as constant-weight cyclically permutable codes, can be found in [1], [4], [17].

The number of ones in a binary sequence is called the *Hamming weight*. It is easy to see that in order to support user-irrepressibility, each active user has to send at least k packets in a period of L time slots, 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 property of user-irrepressibility. In this paper, we focus on the extreme case where all sequences have the same Hamming weight w which equals the number of active users, i.e., $w = k$. This is the minimum weight requirement for user-irrepressibility. Under the assumption of $w = k$, many works are devoted to determine the maximal number of potential users for

Hamming weight equal to three, see e.g., [8], [10], [11], [14], [15]. Some optimal constructions for Hamming weight equal to four and five are presented in [16]. However, the maximal number of potential users for general Hamming weight w larger than five is unknown. We address this open question in this paper and provide a general upper bound on the number of potential users for all Hamming weights. An asymptotic version of this general upper bound can be found in [19].

This paper is organized as follows. We define conflict-avoiding codes and set up some notations in Section II. Three known constructions are described in Section III. The main result in this paper is contained in Section IV, which provides an upper bound on the number of potential users that can be supported, given the length L and Hamming weight w. In Section V, we apply this upper bound to the constructions described in Section III. Optimal CAC with Hamming weight $w \geq 6$ are also given in Section V.

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. 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 $t \in \mathcal{I}$, where $|\mathcal{I}|$ denotes the cardinality of $\mathcal{I}$. Subsets of $\mathbb{Z}_L$ with cardinality w are called *codewords*.

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 nonzero 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 $\mathcal{I}$. A collection of M codewords

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

is called a *conflict-avoiding code* (CAC) of length L and weight w if

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

for all $j \neq k$. We use the notation (L, w)-CAC for a conflict-avoiding code of length L and weight w. It is easy to see that an (L, w)-CAC with N codewords is equivalent to a set of (N, w)-conflict-avoiding sequences mentioned in the introduction. We sometime say that $\mathcal{I}$ is a codeword of weight w. Since adding a constant to all elements in a codeword $\mathcal{I}$ does not affect the set of differences $d(\mathcal{I})$, we assume without loss of generality that every codeword in a CAC contains the zero element 0 in $\mathbb{Z}_L$.

Given positive integers L and w, consider the class of all CACs with length L and weight w. A CAC in this class with maximal number of codewords is called *optimal*, and the max-

imal number of codewords is denoted by $M(L, w)$. The objective of this paper is to derive an upper bound on $M(L, w)$ for all L and w.

Example 1: $L = 15$, $w = 3$. The four codewords $\{0, 5, 10\}$, $\{0, 1, 2\}$, $\{0, 7, 11\}$, and $\{0, 6, 12\}$ constitute a $(15, 3)$-CAC. We can verify that the sets of nonzero differences

$$d^*(\{0, 5, 10\}) = \{5, 10\}$$
$$d^*(\{0, 1, 2\}) = \{1, 2, 13, 14\}$$
$$d^*(\{0, 7, 11\}) = \{4, 7, 8, 11\}$$
$$d^*(\{0, 6, 12\}) = \{3, 6, 9, 12\}$$

are disjoint.

Example 2: $L = 26$, $w = 4$. Consider the four codewords $\{0, 1, 2, 3\}$, $\{0, 4, 8, 12\}$, $\{0, 5, 10, 15\}$, and $\{0, 6, 13, 19\}$. Since

$$d^*(\{0, 1, 2, 3\}) = \{1, 2, 3, 23, 24, 25\}$$
$$d^*(\{0, 4, 8, 12\}) = \{4, 8, 12, 14, 18, 22\}$$
$$d^*(\{0, 5, 10, 15\}) = \{5, 10, 11, 15, 16, 21\}$$
$$d^*(\{0, 6, 13, 19\}) = \{6, 7, 13, 19, 20\}$$

are disjoint, we have a $(26, 4)$-CAC with four codewords.

Remark: From the definition of CAC, it follows directly that for $j \neq k$, the Hamming cross-correlation of the two binary sequences associated with two distinct codewords in an (L, w)-CAC is no more than 1 for any cyclic shift. An (L, w)-CAC can thus be viewed as an $(L, w, 1)$-optical orthogonal code (OOC) without any autocorrelation requirement. We refer the readers to, e.g., [3], and the references therein for further information on OOC.

A codeword $\mathcal{I}$ is called *equidifference* 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 a *generator* of this codeword. For an equidifference 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 a CAC C are equidifference, then we say that C is equidifference, and the set of generators is denoted by $\Gamma(\mathsf{C})$.

We adopt the terminology in [16] and say that a codeword $\mathcal{I}$ of weight w is *exceptional* if

$$|d^*(\mathcal{I})| < 2w - 2 \tag{1}$$

or equivalently, if

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

From the discussion above, we see that if a codeword $\mathcal{I}$ is equidifference 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.

The CAC in Example 1 is equidifference, with generators $1, 5$, 6, and 11. The codeword generated by 5 is exceptional, because

$$|d^*(\{0, 5, 10\})| = |\{5, 10\}| = 2 < 2 \cdot 3 - 2.$$

In Example 2, the codewords $\{0, 1, 2, 3\}$, $\{0, 4, 8, 12\}$, and $\{0, 5, 10, 15\}$ are equidifference, generated by 1, 4, and 5, respectively. The codeword $\{0, 6, 13, 19\}$ is not equidifference, but it is exceptional, because

$$|d^*(\{0, 6, 13, 19\})| = |\{6, 7, 13, 19, 20\}| = 5 < 2 \cdot 4 - 2.$$

We see that an exceptional codeword is not necessarily equidifference.

III. EXISTING CONSTRUCTIONS OF CAC IN THE LITERATURE

The following three constructions of CAC are due to [16]. We state them in this section for the convenience of the readers. The optimality of these constructions is known only for some special cases. We will show later in Section V that they are indeed optimal under more general conditions.

The first and second constructions are based on the multiplicative structure of finite field: given a prime p, the set of nonzero elements in $\mathbb{Z}_p$, denoted by $\mathbb{Z}_p^*$, is a cyclic group with order $p - 1$ under multiplication. For a divisor f of $p - 1$, we denote the multiplicative subgroup in $\mathbb{Z}_p^*$ of index f by

$$\mathcal{H}_0^f(p) := \{x \in \mathbb{Z}_p^* : x^{(p-1)/f} \equiv 1 \bmod p\}$$

and its cosets in the multiplicative subgroup $\mathbb{Z}_p^*$ by $\mathcal{H}_j^f(p)$, for $j = 1, \ldots, f-1$. A set of f elements $\{i_0, i_1, \ldots, i_{f-1}\}$ in $\mathbb{Z}_p^*$ is said to form a *system of distinct representatives* of $\{H_j^f(p) : j = 0, 1, \ldots, f-1\}$ if each coset $\mathcal{H}_j^f(p)$ contains exactly one element in $\{i_0, \ldots, i_{f-1}\}$.

Construction 1 ([16, Th. 3.1]): Let $p = 2(w-1)m + 1$ be a prime number and suppose that $\{1, 2, \ldots, w-1\}$ forms a system of distinct representatives of $\{\mathcal{H}_j^{w-1}(p) : j = 0, \ldots, w-2\}$. Let α be a primitive element in the finite field $\mathbb{Z}_p$ and let $g = \alpha^{w-1}$. Then the m codewords of weight w generated by $1, g, g^2, \ldots, g^{m-1}$ form an equidifference $(2(w-1)m + 1, w)$-CAC.

Example 3: Let $w = 6$, and $p = 421$. We can check that 2 is a primitive element in the finite field $\mathbb{Z}_{421}$ and

$$1 \equiv 2^{420} \equiv 2^{84 \cdot 5 + 0} \bmod 421$$
$$2 \equiv 2^1 \equiv 2^{0 \cdot 5 + 1} \bmod 421$$
$$3 \equiv 2^{404} \equiv 2^{80 \cdot 5 + 4} \bmod 421$$
$$4 \equiv 2^2 \equiv 2^{0 \cdot 5 + 2} \bmod 421$$
$$5 \equiv 2^{278} \equiv 2^{55 \cdot 5 + 3} \bmod 421.$$

Hence, $\{1, 2, 3, 4, 5\}$ forms a system of distinct representatives of $\mathcal{H}_0^5(421), \mathcal{H}_1^5(421), \ldots, \mathcal{H}_4^5(421)$. The 42 codewords generated by $2^{5j} \bmod 421$, $j = 0, 1, \ldots, 41$, form a $(421, 6)$-CAC. The generators are: 1, 29, 32, 52, 75, 86, 93, 95, 111, 115, 122, 137, 149, 170, 171, 174, 178, 182, 184, 188, 202,

205, 207, 223, 226, 229, 245, 262, 269, 286, 295, 301, 309, 311, 312, 351, 370, 385, 388, 400, 401, and 415.

Construction 2 [16, Th. 3.7]: Let p be a prime that can be written as $p = 2fm + 1$ for some integers $f \geq 1$ and $m \geq 1$. If $s \geq 2$ is an integer such that each of $\{\pm s, \pm 2s, \ldots, \pm fs\}$ and

$$\{i + js : j = -f, -f+1, \ldots, f-1\}$$

for $i = 1, 2, \ldots, s-1$, forms a system of distinct representatives of the cosets of $\{\mathcal{H}_j^{2f}(p) : j = 0, \ldots, 2f-1\}$, then there exists an equidifference $(s(2fm+1), sf+1)$-CAC with m codewords. Furthermore, the codewords $\mathcal{I}_1, \ldots, \mathcal{I}_m$ satisfies

$$\mathbb{Z}_{sp} \setminus \bigcup_{j=1}^{m} d^*(\mathcal{I}_j) = p\mathbb{Z}_{sp},$$

where $\alpha\mathbb{Z}_L$ represents the set of integral multiples of α in $\mathbb{Z}_L$.

Example 4: Consider $w = 7$, $f = 2$ and $s = 3$. The prime number $p = 37$ satisfies the conditions in Construction 2. We have

$$\mathcal{H}_0^4(37) = \{1, 7, 9, 10, 12, 16, 26, 33, 34\},$$
$$\mathcal{H}_1^4(37) = \{2, 14, 15, 18, 20, 24, 29, 31, 32\},$$
$$\mathcal{H}_2^4(37) = \{3, 4, 11, 21, 25, 27, 28, 30, 36\},$$
$$\mathcal{H}_3^4(37) = \{5, 6, 8, 13, 17, 19, 22, 23, 35\}.$$

We can verify that each of

$$\{\pm 3, \pm 6\} = \{3, 6, 31, 34\},$$
$$\{-5, -2, 1, 4\} = \{1, 4, 32, 35\},$$
$$\{-4, -1, 2, 5\} = \{2, 5, 33, 36\}$$

forms a system of distinct representatives of $\mathcal{H}_0^4(37)$, $\mathcal{H}_1^4(37)$, $\mathcal{H}_2^4(37)$, $\mathcal{H}_3^4(37)$. By Construction 2, we have a $(111, 7)$-CAC consisting of $m = 9$ codewords. Indeed, the generators of this CAC are 1, 7, 10, 16, 34, 46, 39, 70, 100.

The last construction we discuss in this section is a recursive construction.

Construction 3 [16, Th. 6.1]: Let $w \geq 3$, and L_1, L_2, and s be positive integers such that L_1 is divisible by s and $\gcd(\ell, L_2) = 1$ for $\ell = 2, \ldots, w-1$. Let C_1 be an equidifference (L_1, w)-CAC consisting of m_1 nonexceptional codewords $\mathcal{I}_1, \ldots, \mathcal{I}_{m_1}$ so that

$$\mathbb{Z}_{L_1} \setminus \bigcup_{j=1}^{m_1} d^*(\mathcal{I}_j) \supseteq \left(\frac{L_1}{s}\right) \mathbb{Z}_{L_1}.$$

Let C_2 be an equidifference (sL_2, w)-CAC with m_2 codewords. The code C with length L_1L_2 generated by $i + jL_1$, for $i \in \Gamma(\mathsf{C}_1), j = 0, 1, \ldots, L_2 - 1$, and $(L_1/s)k$, for $k \in \Gamma(\mathsf{C}_2)$ is an equidifference (L_1L_2, w)-CAC with $m_1L_2 + m_2$ codewords.

Example 5: The prime numbers $p = 37$ and $p = 53$ satisfy the conditions in Construction 2 with $w = 7$, $f = 2$ and $s = 3$. We have a $(3 \cdot 37, 7)$-CAC consisting of $(37-1)/4 = 9$ codewords, and a $(3 \cdot 53, 7)$-CAC consisting of $(53-1)/4 = 13$ codewords. Using Construction 3 with $L_1 = 3 \cdot 53$, $L_2 = 37$, $s = 3$ and $w = 7$, we obtain a $(3 \cdot 37 \cdot 53, 7)$-CAC with $13 \cdot 37 + 9 = 490$ codewords.

IV. Upper Bound on the Size of CAC

In this section we derive an upper bound on the size of CAC. A tool that we will use is Kneser's theorem [9], 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 notations.

Given two nonempty 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

$$\mathcal{A} + \mathcal{B} := \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}$$
$$\mathcal{A} - \mathcal{B} := \{a - b : a \in \mathcal{A}, b \in \mathcal{B}\}$$

respectively. Thus, $\mathcal{I} - \mathcal{I}$ is just another expression for $d(\mathcal{I})$. We also write $a + \mathcal{B} := \{a\} + \mathcal{B}$, for nonempty subset $\mathcal{B} \subseteq \mathbb{Z}_L$ and $a \in \mathbb{Z}_L$. The negative of $\mathcal{A}$ is defined as

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

Given a nonempty 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 nonempty subset $\mathcal{S}$ of $\mathbb{Z}_L$, and $H(\mathcal{S})$ is a subgroup of $\mathbb{Z}_L$. A subset $\mathcal{S}$ is called *periodic* if it is nonempty and $H(\mathcal{S}) \neq \{0\}$. If $\mathcal{S}$ is periodic with stabilizer H, then we say that $\mathcal{S}$ is *H-periodic*. In other words, a subset of $\mathbb{Z}_L$ is periodic if its stabilizer is a nontrivial subgroup of $\mathbb{Z}_L$.

Lemma 1: For any subset $\mathcal{I} \in \mathbb{Z}_L$, we have $d(\mathcal{I}) \supseteq H(d(\mathcal{I}))$.

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

Note that an H-periodic subset $\mathcal{S}$ of $\mathbb{Z}_L$ can be written as the summation of cosets of H

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

Conversely, any union of cosets of a nontrivial subgroup H of $\mathbb{Z}_L$ is H-periodic.

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.

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 hence $\mathcal{S}$ is $\langle 3 \rangle$-periodic. We can see that $\mathcal{S}$ is a union of H and the coset $\{1, 4\}$.

Theorem 2 (Kneser): Let $\mathcal{A}$ and $\mathcal{B}$ be nonempty 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

$$|\mathcal{A} + \mathcal{B}| = |\mathcal{A} + H| + |\mathcal{B} + H| - |H|. \tag{3}$$

The set $\mathcal{A} + H$ can be considered as the "completion" of $\mathcal{A}$ with respect to H, because $\mathcal{A} + H$ is the smallest H-periodic subset in $\mathbb{Z}_L$ which contains $\mathcal{A}$. Similarly, $\mathcal{B} + H$ can be considered as the completion of $\mathcal{B}$ with respect to H. The conclusion in Kneser's theorem can be rephrased in words as: the cardinality of the sum set of $\mathcal{A}$ and $\mathcal{B}$ is equal to the cardinality of the completion of $\mathcal{A}$ with respective to the stabilizer H, plus the cardinality of the completion of $\mathcal{B}$ with respective to the stabilizer H, minus the size of H.

Proof of Theorem 2 can be found in [12] or [18]. We will apply Kneser's theorem through the following corollary.

Corollary 3: Let $\mathcal{I}$ be an exceptional codeword in an (L, w)-CAC and H be the stabilizer of $d(\mathcal{I})$, then $d(\mathcal{I})$ is periodic, and

$$|d(\mathcal{I})| = 2|\mathcal{I} + H| - |H|. \tag{4}$$

Proof: Suppose that $\mathcal{I}$ is an exceptional codeword in an (L, w)-CAC and let H be the stabilizer of $d(\mathcal{I})$. The condition in Kneser's theorem is satisfied with $\mathcal{A} = \mathcal{I}$ and $\mathcal{B} = -\mathcal{I}$, because

$$|\mathcal{I} + (-\mathcal{I})| = |d(\mathcal{I})| \leq 2w - 2 < 2|\mathcal{I}|. \tag{5}$$

From (3), we obtain

$$\begin{aligned} |d(\mathcal{I})| &= |\mathcal{I} + H| + |-\mathcal{I} + H| - |H| \\ &= |\mathcal{I} + H| + |\mathcal{I} - H| - |H| \\ &= 2|\mathcal{I} + H| - |H|. \end{aligned}$$

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 (4). Since $|\mathcal{I} + H| \geq w$, we obtain

$$|d(\mathcal{I})| \geq 2w - |H|. \tag{6}$$

Putting (5) and (6) together, we have

$$2w - |H| \leq |d(\mathcal{I})| < 2w - 1.$$

We conclude that $|H| > 1$ and therefore $d(\mathcal{I})$ is periodic. ∎

We illustrate Kneser's theorem and Corollary 3 using Example 1 and 2. In Example 1, consider the exceptional codeword

$$\mathcal{I}_1 = \{0, 5, 10\} \subset \mathbb{Z}_{15}.$$

The stabilizer of $d(\mathcal{I}_1) = \{0, 5, 10\}$, which is just equal to $\mathcal{I}_1$ itself, is $\langle 5 \rangle$-periodic. We can verify that

$$|d(\mathcal{I}_1)| = 2|\mathcal{I}_1 + \langle 5 \rangle| - |\langle 5 \rangle| = 2 \cdot 3 - 3 = 3.$$

The codeword $\mathcal{I}_2 = \{0, 1, 2\}$ in Example 1 is equidifference and nonexceptional. The condition in Kneser's theorem is satisfied with $\mathcal{A} = \mathcal{I}_2$ and $\mathcal{B} = -\mathcal{I}_2$, since

$$|d(\mathcal{I}_2)| = |\mathcal{I}_2 - \mathcal{I}_2| = |\{0, \pm 1, \pm 2\}| = 5 < 2|\mathcal{I}_2|.$$

We have $H(d(\mathcal{I}_2)) = \{0\}$, and

$$|d(\mathcal{I}_2)| = |\mathcal{I}_2 + \{0\}| + |\mathcal{I}_2 - \{0\}| - |\{0\}| = 5.$$

In Example 2, consider the exceptional codeword

$$\mathcal{I} = \{0, 6, 13, 19\} \subset \mathbb{Z}_{26}.$$

The corresponding set of differences

$$d(\{0, 6, 13, 19\}) = \{0, 6, 7, 13, 19, 20\}$$

is $\langle 13 \rangle$-periodic. We can check that

$$|d(\mathcal{I})| = 2|\mathcal{I} + \langle 13 \rangle| - |\langle 13 \rangle| = 2 \cdot 4 - 2 = 6.$$

The next theorem provides a recipe for upper bounding the size of a CAC.

Theorem 4: Let C be an (L, w)-CAC in which E codewords are exceptional. For $j = 1, 2, \ldots, E$, denote the jth exceptional codeword by $\mathcal{I}_j$, and let the stabilizer of $d(\mathcal{I}_j)$ be H_j. Define

$$\Delta_j := |\mathcal{I}_j + H_j| - w. \tag{7}$$

Then

$$|\mathsf{C}| \leq \frac{L - 1 + \sum\limits_{j=1}^{E}(|H_j| - 1 - 2\Delta_j)}{2w - 2}. \tag{8}$$

Proof: By definition, $d^*(\mathcal{I})$ and $d^*(\mathcal{J})$ are disjoint for any pair of distinct codewords $\mathcal{I}$ and $\mathcal{J}$ in C. We have the following basic inequality:

$$L - 1 \geq \sum_{\mathcal{I} \in \mathsf{C}} |d^*(\mathcal{I})|. \tag{9}$$

Let the number of nonexceptional codewords be N. Since $d^*(\mathcal{I}) \geq 2w - 2$ for each nonexceptional codeword $\mathcal{I}$, the inequality in (9) becomes

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

From Corollary 3 we get

$$\sum_{j=1}^{E} |d^*(\mathcal{I}_j)| = \sum_{j=1}^{E} \left(|d(\mathcal{I}_j)| - 1\right)$$

$$= \sum_{j=1}^{E} \left(2|\mathcal{I}_j + H_j| - |H_j| - 1\right).$$

Therefore

$$L - 1 \geq N(2w - 2) + \sum_{j=1}^{E} \left(2|\mathcal{I}_j + H_j| - |H_j| - 1\right)$$

$$= (N + E)(2w - 2) + \sum_{j=1}^{E} \left(2\Delta_j - |H_j| + 1\right).$$

After some rearrangement of terms, we get

$$|\mathsf{C}| = N + E \leq \frac{L - 1 + \sum\limits_{j=1}^{E}(|H_j| - 1 - 2\Delta_j)}{2w - 2}.$$

This finishes the proof of the theorem. ∎

We note that the value of Δ_j defined in (7) is nonnegative for all j, because $\Delta_j = |\mathcal{I}_j + H_j| - |\mathcal{I}_j|$, and $\mathcal{I}_j$ is a subset of $\mathcal{I}_j + H_j$. We have the following corollary.

Corollary 5: Let C be an (L, w)-CAC. If there are E exceptional codewords $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_E$, in C, then

$$|\mathsf{C}| \leq \frac{L - 1 + \sum\limits_{j=1}^{E}(|H(d(\mathcal{I}_j))| - 1)}{2w - 2}. \tag{10}$$

We make a few more definitions. The motivation of these definition will be clear after Theorem 6. Let

$$S(L, w) := \Big\{x \in \{2, 3, \ldots, 2w - 2\} : x \text{ divides } L, \tag{11}$$

$$\text{and } 2x \left\lceil \frac{w}{x} \right\rceil - x \leq 2w - 2\Big\}. \tag{12}$$

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

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

Given an integer $L \geq w \geq 2$, if $\mathsf{S}(L, w)$ is nonempty, define

$$F(L, w) := \max_{\mathcal{S} \in \mathsf{S}(L, w)} \sum_{x \in \mathcal{S}} \left(x - 1 - 2x \left\lceil \frac{w}{x} \right\rceil + 2w\right) \tag{13}$$

with the maximum taken over all subsets $\mathcal{S}$ in $\mathsf{S}(L, w)$. If $\mathsf{S}(L, w)$ is empty, we define $F(L, w)$ as zero. We note that the summand in (13) is positive by the condition in (12). Hence, $F(L, w)$ is nonnegative.

Theorem 6: For $L \geq w \geq 2$

$$M(L, w) \leq \left\lfloor \frac{L - 1 + F(L, w)}{2w - 2} \right\rfloor. \tag{14}$$

Proof: Let C be an (L, w)-CAC. If there is no exceptional codeword in C, then $|\mathsf{C}| \leq \lfloor (L - 1)/(2w - 2) \rfloor$ by Theorem 4. Since $F(L, w)$ is nonnegative, the size of C is less than or equal to the right-hand side (RHS) of (14).

Suppose that there are E exceptional codewords in an (L, w)-CAC, denoted by $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_E$. For $j = 1, 2, \ldots, E$, let H_j be the stabilizer of $d(\mathcal{I}_j)$. Let $i \neq j$ and consider two distinct exceptional codewords $\mathcal{I}_j$ and $\mathcal{I}_j$ in C. Both $|H_i|$ and $|H_j|$ are strictly larger than one by Corollary 3. 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 nonzero mod L, because $b > 1$. The two stabilizers H_1 and H_2 thus contain a common nonzero element. By Lemma 1, we have $d(\mathcal{I}_i) \supseteq H_i$ and $d(\mathcal{I}_j) \supseteq H_j$, and so L/b is also a common nonzero element of $d(\mathcal{I}_i)$ and $d(\mathcal{I}_j)$. This contradicts the defining property that $d(\mathcal{I}_i) \cap d(\mathcal{I}_j) = \{0\}$. 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, as we have already noted in the proof of Corollary 3, $|\mathcal{I}_j + H_j|$ is larger than or equal to w because $\mathcal{I}_j + H_j$ contains $\mathcal{I}_j$. We thus have the following:

$$|\mathcal{I}_j + H_j| \geq |H_j| \left\lceil \frac{w}{|H_j|} \right\rceil.$$

The RHS in the above inequality is the smallest integral multiples of $|H_j|$ which is larger than or equal to w.

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 $2w - 2$, otherwise by Corollary 3, we have

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

which is a contradiction to the definition of exceptional codeword in (2). In addition, we must have $|H_j| \geq 2$ because $\mathcal{I}_j$ is periodic by assumption. This shows that $2 \leq |H_j| \leq 2w - 2$.

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

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

Consequently, $|H_j|$ satisfies the conditions in (11) and (12), 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

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

For $j = 1, 2, \ldots, E$, let Δ_j be defined as in Theorem 4. We can upper bound $|H_j| - 1 - 2\Delta_j$, which appears in the summation in (8), by

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

which equals the summand in (13) with x substituted by $|H_j|$. By exhausting all possible choices of $\mathcal{S}$ in $S(L, w)$, we have the following upper bound

$$\sum_{j=1}^{E} (|H_j| - 1 - 2\Delta_j) \leq F(L, w).$$

Substituting it back to (8), we have

$$|C| \leq \left\lfloor \frac{L - 1 + F(L, w)}{2w - 2} \right\rfloor.$$

This completes the proof of Theorem 6. ∎

For CAC with weight $w = 3$ and odd length L, we can check that $S(L, 3)$ is either empty or $\{3\}$. So in the computation of $F(L, 3)$ in (13), the maximum is taken over only one number, namely $x = 3$, and we get

$$F(L, 3) = 3 - 1 - 2 \cdot 3 \left\lceil \frac{3}{3} \right\rceil + 2 \cdot 3 = 2.$$

Hence, from Theorem 6, we obtain

$$M(L, 3) \leq \left\lfloor \frac{L + 1}{4} \right\rfloor.$$

It can be shown that the above bound holds for even length L as well. This yields the upper bound on the size of CAC for three active users in [11]. When $w = 4$ and $w = 5$, the upper bounds obtained from Theorem 6 coincides with the known results in [16, Lemma 2.1, 2.3]. We illustrate Theorem 6 with $w = 6$.

Corollary 7: Let L be an integer factorized as $2^p 3^q 7^r \ell$, where ℓ is not divisible by 2, 3, or 7. Then we have the upper bound at the bottom of the next page.

Proof: The value of $x - 1 - 2x\lceil w/x \rceil + 2w$ for $x \in \{2, 3, \ldots, 10\} \setminus \{4, 5\}$ is shown in the following table:

x	2	3	6	7	8	9	10
$x - 1 - 2x\lceil w/x \rceil + 2w$	1	2	5	4	3	2	1

We note that 4 and 5 are not shown in the above table, because they do not satisfy the condition in (12).

Since the value of $x - 1 - 2x\lceil w/x \rceil + 2w$ for $x = 2$ and $x = 10$ are the same, we can disregard the case $x = 10$ in

TABLE I
VALUES OF $S(L, 6)$ AND $F(L, 6)$

p	q	r	$S(2^p 3^q 7^r \ell, 6)$	$F(2^p 3^q 7^r \ell, 6)$
0	0	0	$\emptyset$	0
1, 2	0	0	$\{2\}$	1
≥ 3	0	0	$\{2, 8\}$	3
0	1	0	$\{3\}$	2
1, 2	1	0	$\{2, 3, 6\}$	5
≥ 3	1	0	$\{2, 8, 3, 6\}$	5
0	≥ 2	0	$\{3, 9\}$	2
1, 2	≥ 2	0	$\{2, 3, 6, 9\}$	5
≥ 3	≥ 2	0	$\{2, 3, 6, 8, 9\}$	5
0	0	≥ 1	$\{7\}$	4
1, 2	0	≥ 1	$\{2, 7\}$	5
≥ 3	0	≥ 1	$\{2, 7, 8\}$	7
0	1	≥ 1	$\{3, 7\}$	6
1, 2	1	≥ 1	$\{2, 3, 6, 7\}$	9
≥ 3	1	≥ 1	$\{2, 3, 6, 7, 8\}$	9
0	≥ 2	≥ 1	$\{3, 7, 9\}$	6
1, 2	≥ 2	≥ 1	$\{2, 3, 6, 7, 9\}$	9
≥ 3	≥ 2	≥ 1	$\{2, 3, 6, 7, 8, 9\}$	9

Fig. 1. Upper bounds on size of CAC for weight 3 to 7.

the computation of $F(L, w)$ without affecting the result. We tabulate $S(L, 6)$ and $F(L, 6)$ in Table I. By Theorem 6, we get

$$M(L, 6) \leq \left\lfloor \frac{L - 1 + F(L, 6)}{10} \right\rfloor.$$

The upper bound in Corollary 7 is obtained after tidying up the data in Table I. ∎

Remark: The value of $F(L, w)$ in Theorem 6 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

$$c_i := i - 1 - 2i \left\lceil \frac{w}{i} \right\rceil + 2w.$$

For each prime number p between 2 and $2w - 2$, impose a constraint
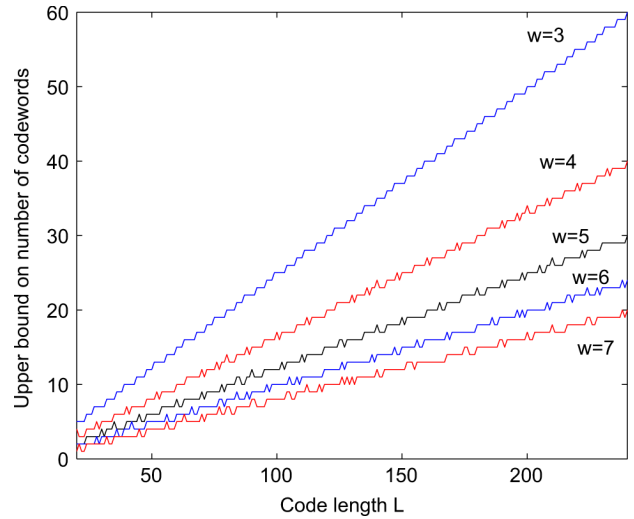
$$\sum_{p | i} z_i \leq 1 \qquad (15)$$

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 (15) for p ranging over all prime numbers between 2 and $2w - 2$, and $0 \leq z_i \leq 1$ for all $i \in S(L, w)$.

Using the linear programming mentioned in the above remark, the upper bounds given by Theorem 6 for weight 3 to 7 and length between 20 and 240 are plotted in Fig. 1. The lines corresponding to $w = 4$ and $w = 5$ are the same as the upper bounds on the size of CAC in [16]. For each w, the growth is roughly linear in L, with slope $(2w - 2)^{-1}$. We note that for $w > 3$, the upper bounds are *not* monotonically increasing with L.

The computation of $F(L, w)$ amounts to solving a linear programming, and it is not obvious from (13) how to get an estimate on the value of $F(L, w)$. The next theorem gives an upper bound on $F(L, w)$ in closed-form expression, from which we can analyze the asymptotic growth rate of $M(L, w)$.

$$M(L, 6) \leq \begin{cases} \left\lfloor \frac{(L-1)}{10} \right\rfloor & \text{if } p = q = r = 0, \\ \left\lfloor \frac{L}{10} \right\rfloor & \text{if } 1 \leq p \leq 2, \ q = r = 0, \\ \left\lfloor \frac{(L+1)}{10} \right\rfloor & \text{if } q > 1, p = r = 0, \\ \left\lfloor \frac{(L+2)}{10} \right\rfloor & \text{if } p \geq 3, q = r = 0, \\ \left\lfloor \frac{(L+3)}{10} \right\rfloor & \text{if } p = q = 0, r \geq 1, \\ \left\lfloor \frac{(L+4)}{10} \right\rfloor & \text{if } p \geq 1, q \geq 1, r = 0, \text{ or } 1 \leq p \leq 2, q = 0, r \geq 1, \\ \left\lfloor \frac{(L+5)}{10} \right\rfloor & \text{if } p = 0, q \geq 1, r \geq 1, \\ \left\lfloor \frac{(L+6)}{10} \right\rfloor & \text{if } p \geq 3, q = 0, r \geq 1, \\ \left\lfloor \frac{(L+8)}{10} \right\rfloor & \text{if } p \geq 1, q \geq 1, r \geq 1. \end{cases}$$

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 8: For $L \geq w \geq 2$

$$M(L, w) \leq \left\lfloor \frac{L-1}{2w-2} + \frac{\pi(2w-2)}{2} \right\rfloor. \quad (16)$$

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

$$\sum_{x \in \mathcal{S}} \left(x - 1 - 2x \left\lceil \frac{w}{x} \right\rceil + 2w \right) \quad (17)$$

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

$$x - 1 - 2x \left\lceil \frac{w}{x} \right\rceil + 2w = x - 1 - 2x + 2w$$
$$= 2w - x - 1$$
$$\leq w - 1$$

and for $w > x$, we have

$$x - 1 - 2x \left\lceil \frac{w}{x} \right\rceil + 2w = x - 1 - 2x + 2w$$
$$= 2w - x - 1$$
$$\leq w - 1.$$

In summary, we obtain

$$x - 1 - 2x \left\lceil \frac{w}{x} \right\rceil + 2w \leq w - 1$$

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

The number of summands in (17) is less than or equal to the maximum number of relatively prime integers in $S(L, w)$. Since $S(L, w) \subseteq \{2, 3, \ldots, 2w - 2\}$, the number of summands in (17) 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 (17) is thus less than or equal to $(w-1)\pi(2w-2)$, and hence

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

Theorem 8 follows by replacing $F(L, w)$ by $(w - 1)\pi(2w - 2)$ in Theorem 6. ∎

Remark:

The celebrated prime number theorem says that $\pi(x) \log(x)/x$ approaches 1 when x approaches infinity. A weaker form of the prime number theorem proved by Chebyshev [5] 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, $\pi(x)$ can be upper bounded by $\left\lceil \pi(x) < \frac{x}{\log(x)-1.5} \right.$ for $x \geq 5$ [23]. Hence, for $w \geq 4$, we have

$$M(L, w) \leq \left\lfloor \frac{L-1}{2w-2} + \frac{(2w-2)}{2\log(2w-2)-3} \right\rfloor. \quad (18)$$

V. OPTIMALITY OF EXISTING CONSTRUCTIONS OF CAC

For Hamming weight $w = 4$ and $w = 5$, Constructions 1 and 2 are shown to be optimal in [16]. In this section, we use the upper bounds on size of CAC given in Section IV to show the optimality of some CACs by Constructions 1, 2, and 3 with general weight.

Theorem 9: All CACs produced by Constuction 1 are optimal. If p and w satisfy the conditions in Construction 1, then we have $M(p, w) = (p - 1)/(2w - 2)$.

Proof: Since p is prime, there is no nontrivial additive subgroup in $\mathbb{Z}_p$, and, hence, there is no exceptional codeword. The upper bound in Theorem 4 reduces to $\lfloor (L-1)/(2w-2) \rfloor$. By definition, $(L - 1)/(2w - 2) = (p - 1)/(2w - 2) = m$, which equals the number of codewords in Construction 1. The number of codewords meets the upper bound and the constructed CAC is therefore optimal. ∎

Theorem 10: If $m > s$, then any CAC with parameters stated in Construction 2 is optimal. In other words, if p, m, s and w satisfy the conditions in Construction 2 and $m > s$, then $M(sp, w) = s(p - 1)/(2w - 2)$.

Proof: Since $m > s$ and $p = 2fm + 1$, we have $s < p$ and hence s and p are relatively prime.

Let C be a CAC with length $L = sp$ and weight $w = sf + 1$. Suppose that there are E exceptional codewords in C, say $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_E$. Let $H_j = \langle \alpha_j \rangle$, for $j = 1, 2, \ldots, E$, respectively, be the stabilizer of $d(\mathcal{I}_j)$, where α_j's are divisors of $L = sp$. Suppose that $\gcd(\alpha_j, p) = 1$ for some j. Because p and s are relatively prime, α_j must divide s, and, hence, we get $\langle s \rangle \subseteq \langle \alpha_j \rangle$ and

$$|H_j| = |\langle \alpha_j \rangle| \geq |\langle s \rangle|.$$

However

$$|\langle s \rangle| = p = 2fm + 1 > 2fs + 1 = 2w - 1 \quad (19)$$

which implies that $|H_j| > 2w - 1$, contradicting the assumption that $\mathcal{I}_j$ is exceptional. [We have used the assumption that $m > s$ in (19).] Consequently, α_j is divisible by p for all $j = 1, 2, \ldots, E$.

We obtain

$$H_j = \langle \alpha_j \rangle \subseteq \langle p \rangle$$

for all j, and $\cup_{j=1}^{E} H_j \subseteq \langle p \rangle$. Since $H_i \cap H_j = \{0\}$ for $i \neq j$, we obtain

$$\sum_{j=1}^{E} (|H_j| - 1) \leq |\langle p \rangle| = s.$$

From Corollary 5, we obtain

$$|\mathsf{C}| \leq \left\lfloor \frac{L - 1 + s - 1}{2w - 2} \right\rfloor$$

$$= \left\lfloor \frac{s(2fm + 1) - 1 + s - 1}{2fs} \right\rfloor$$

$$= \left\lfloor m + \frac{s - 1}{fs} \right\rfloor.$$

From $s - 1 < fs$, we conclude that $|\mathsf{C}| \leq m$. ∎

From Theorem 10, we can construct infinitely many optimal CACs for each $w \geq 3$. The following is an illustration for $w = 7$.

Corollary 11: Let p be a prime number congruent to 31 or 39 mod 40. Then $M(6p, 7) = (p - 1)/2$.

Proof: Apply Construction 2 with $f = 1$ and $s = 6$. We want to find integer m such that $p = 2m + 1$ is prime, and each of the following:

$$\{-5, 1\}, \{-4, 2\}, \{-3, 3\}, \{-2, 4\}, \{-1, 5\}, \{-6, 6\}$$

forms a system of distinct representatives of $\mathcal{H}_0^2(p)$ and $\mathcal{H}_1^2(p)$. Expressed in terms of the Legendre symbol $\left(\frac{\cdot}{p}\right)$, it is equivalent to

$$\left(\frac{-1}{p}\right) = -1 \tag{20}$$

and

$$\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = 1. \tag{21}$$

By the law of quadratic reciprocity [7], (20) and (21) are equivalent to the following conditions:

$$\begin{cases} p \equiv 3 \bmod 4 \\ p \equiv \pm 1 \bmod 8 \\ p \equiv 1, 4 \bmod 5 \end{cases}$$

which can be further simplified to $p \equiv 31$ or $39 \bmod 40$. Hence, for each prime $p \equiv 31$ or $39 \bmod 40$, we have a $(6p, 7)$-CAC consisting of $(p-1)/2$ codewords, which is optimal by Theorem 10. This proves that $M(6p, 7) = (p - 1)/2$. ∎

By Dirichlet's theorem on primes in arithmetic progression [5], there are infinitely many prime p that satisfies $p \equiv 31$ or $39 \bmod 40$. We thereby have infinitely many optimal CACs with weight $w = 7$. The argument for $w = 7$ can be adopted to all weight w to construct infinitely many optimal CACs for each w.

Applying the recursive construction in Construction 3 to $(6p_i, 7)$-CAC, for $i = 1, 2, \ldots, n$, where p_i is prime and congruent to 31 or 39 mod 40, we obtain $(6p_1 p_2 \cdots p_n, 7)$-CAC. By similar argument as in the proof of Theorem 10, we can show that the resulting $(6p_1 p_2 \cdots p_n, 7)$-CAC is optimal. This proves the following corollary.

Corollary 12: Let p_i be prime number that satisfies $p_i \equiv 31$ or $39 \bmod 40$, for $i = 1, 2, \ldots, n$. Then

$$M(6p_1 p_2 \cdots p_n, 7) = \frac{(p_1 p_2 \cdots p_n - 1)}{2}.$$

In the remaining of this section, we apply the upper bound in this paper to show that Construction 3 produces optimal CAC for some special choices of input parameters.

Theorem 13: Suppose p is a prime number such that $p - 1$ is divisible by $2w - 2$ and $p > 2w - 1$. If there is an equidifference (p, w)-CAC with $m = (p - 1)/(2w - 2)$ codewords, then

$$M(p(2w - 1), w) = p + m.$$

Proof: We apply the recursive Construction 3 with $s = 1$, $L_1 = 2w - 1$, $L_2 = p$, and take C_1 to be a trivial $(2w - 1, w)$-CAC consisting of $m_1 = 1$ codeword generated by 1, and C_2 to be the given equidifference (p, w)-CAC with $m_2 = m$ codewords. It is implied by the assumption $p > 2w - 1$ that $\gcd(p, 2w - 1) = 1$. So the condition

$$\gcd(\ell, L_2) = \gcd(\ell, p) = 1$$

is satisfied for $\ell = 2, 3, \ldots, w - 1$. Construction 3 yields a $(p(2w - 1), w)$-CAC with $m_1 p + m_2 = p + m$ codewords.

It remains to show that any $(p(2w - 1), w)$-CAC contains at most $p + m$ codewords. Let C be a $(p(2w - 1), w)$-CAC. Suppose that $\mathcal{I}_j$, for $j = 1, 2, \ldots, E$, are the exceptional codewords in C, and H_j is the stabilizer of $d(\mathcal{I}_j)$. For each j, H_j contains strictly less than $2w - 1$ elements because $|H_j| \leq |d(\mathcal{I}_j)| \leq 2w - 2$.

We claim that any additive subgroup G in $\mathbb{Z}_{p(2w-1)}$ of size strictly less than $2w - 1$ is included in

$$\langle p \rangle = \{0, p, 2p, \ldots, (2w - 2)p\}.$$

Suppose on the contrary that we can find an $a \in G$ not divisible by p. Then $\gcd(a, p(2w - 1))$ is a divisor of $2w - 1$. The order of a in G, which equals

$$\frac{p(2w - 1)}{\gcd(a, p(2w - 1))}$$

is thus larger than or equal to p. Since $p > 2w - 1$ by hypothesis, the integral multiples of a in G already generate more than $2w - 1$ distinct elements, contradicting the assumption that $|G| < 2w - 1$. Therefore, any integer a which is not an integral multiple of p does not belong to G.

By the above claim, we have $H_j \subseteq \langle p \rangle$ for each j. We can write $H_j = \langle \beta_j p \rangle$, for some β_j between 1 and $2w - 2$. However, β_j cannot be relatively prime with $2w - 1$, otherwise, the integral multiples of $\beta_j p$ would generate $\langle p \rangle$ and we would have $|H_j| = |\langle p \rangle| = 2w - 1$, contradicting $|H_j| < 2w - 1$. In particular, we obtain

$$H_j \subseteq \{zp : z = 0, 1, \ldots, 2w - 2, \gcd(z, 2w - 1) > 1\}.$$

Since $H_i \cap H_j = \{0\}$ for $i \neq j$, we get

$$\sum_{j=1}^{E}(|H_j| - 1) \leq |\langle p \rangle| - 1 - \varphi(2w - 1)$$
$$\leq (2w - 2) - \varphi(2w - 1)$$

where $\varphi(x)$ denotes the number of integers in $\{1, 2, \ldots, x-1\}$ which are relatively prime with x. By Corollary 5, we obtain

$$|\mathsf{C}| \leq \left\lfloor \frac{L - 1}{2w - 2} + \frac{2w - 2 - \varphi(2w - 1)}{2w - 2} \right\rfloor.$$

Since

$$\frac{L - 1}{2w - 2} = \frac{p(2w - 1) - 1}{2w - 2} = p + m,$$
and
$$\frac{2w - 2 - \varphi(2w - 1)}{2w - 2} < 1$$

we conclude that $M(p(2w - 1), w) = p + m$. ∎

Example 6: In [16], CAC of length p and weight 4, containing $(p - 1)/6$ codewords, is reported for infinitely many prime number p using Construction 1. We can extend each of them to an optimal $(7p, 4)$-CAC with $p + (p - 1)/6$ codewords. The example with smallest p is a $(37, 4)$-CAC with 6 codewords generated by 1, 8, 27, 31, 26, and 23. It can be lengthened and enlarged to an optimal $(259, 4)$-CAC with 43 codewords.

Theorem 14: Let $w \geq 3$, and p be a prime number satisfying

$$w \leq p \leq w + \frac{\varphi(2w - 1)}{2} \tag{22}$$

where $\varphi(2w - 1)$ denotes the number of integers in $\{1, 2, \ldots, 2w - 2\}$ which are relatively prime with $2w - 1$. We have

$$M(p(2w - 1), w) = p + 1.$$

Proof: We apply Construction 3 with $s = 1$, $L_1 = 2w - 1$ and $L_2 = p$. Let C_1 be a $(2w - 1, w)$-CAC containing only one equidifference codeword generated by 1. Let C_2 be a (p, w)-CAC containing only one equidifference codeword generated by 1. Since $w \leq p$ and p is prime, the condition $\gcd(\ell, p) = 1$ for $\ell = 2, 3, \ldots, w - 1$ is satisfied. By Construction 3, we have a $(p(2w - 1), w)$-CAC containing $p + 1$ codewords.

We now show that this is an optimal CAC with length $L = p(2w - 1)$ and weight w. Let C be any $(p(2w - 1), w)$-CAC with p prime and satisfying the condition in (22). We show that C contains at most $p+1$ codewords by considering the following two cases.

Case 1: there is no exceptional codeword in C. By Theorem 4 we obtain

$$|\mathsf{C}| \leq \left\lfloor \frac{L - 1}{2w - 2} \right\rfloor = \left\lfloor \frac{p(2w - 1) - 1}{2w - 2} \right\rfloor$$
$$= p + \left\lfloor \frac{p - 1}{2w - 2} \right\rfloor. \tag{23}$$

However, by the second inequality in (22)

$$p - 1 \leq w - 1 + \frac{\varphi(2w - 1)}{2}.$$

Since $\varphi(2w - 1) \leq 2w - 2$, we get $p - 1 \leq 2w - 2$, and hence $|\mathsf{C}| \leq p + 1$ by (23).

Case 2: there is at least one exceptional codeword in C. Let $\mathcal{I}$ be an exceptional codeword in C. We first prove the following claim: the stabilizer H of $d(\mathcal{I})$ is either a subset of $\langle p \rangle$ or equal to $\langle 2w - 1 \rangle$. Let $H = \langle \alpha \rangle$, where α is a proper divisor of $L = p(2w - 1)$. If α is divisible by p, then $\langle \alpha \rangle \subseteq \langle p \rangle$, and we have $H \subseteq \langle p \rangle$. Otherwise, if α is not divisible by p, then α divides $2w - 1$. Suppose that $2w - 1$ is factorized as $\alpha\beta$. We have

$$|\langle \alpha \rangle| = \frac{p(2w - 1)}{\alpha} = p\beta.$$

If α is strictly less than $2w - 1$, then $\beta \geq 2$, and thus $|\langle \alpha \rangle| \geq 2p$. As $p \geq w$ by assumption, we obtain

$$|d(\mathcal{I})| \geq |\langle \alpha \rangle| \geq 2p \geq 2w$$

which is a contradiction to the hypothesis that $\mathcal{I}$ is exceptional. Therefore, when α is not divisible by p, the only choice for α is $2w - 1$, and, hence, $H = \langle 2w - 1 \rangle$. This completes the proof of the claim.

Let $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_E$ be the exceptional codewords in C, and H_j be the stabilizer of $d(\mathcal{I}_j)$, for $j = 1, 2, \ldots, E$. It follows from the claim that

$$\bigcup_{j=1}^{E} H_j \subseteq \langle 2w - 1 \rangle \cup \langle p \rangle.$$

The same argument in the proof of Theorem 13 shows that at most $2w - 2 - \varphi(2w - 1)$ nonzero elements in $\langle p \rangle$, which is a subgroup in $\mathbb{Z}_{p(2w-1)}$ of size $2w - 1$, belong to H_j for some j. Hence

$$\sum_{j=1}^{E}(|H_j| - 1) = (p - 1) + (2w - 2 - \varphi(2w - 1))$$
$$\leq p + 2w - 3 - \varphi(2w - 1). \tag{24}$$

Next, we note that p and $2w - 1$ are both relatively prime with w, hence $L = p(2w - 1)$ is also relatively prime with w. Thus, as a divisor of L, $|H_j|$ is relatively prime with w for all $j = 1, 2, \ldots, E$. Since $|\mathcal{I}_j + H_j|$ is an integral multiples of $|H_j|$, we have

$$|\mathcal{I}_j + H_j| > w = |\mathcal{I}_j|.$$

Recall that Δ_j in Theorem 4 is defined as $\Delta_j := |\mathcal{I}_j + H_j| - w$. We thus have $\Delta_j \geq 1$ for $j = 1, 2, \ldots, E$.

By Theorem 4, we obtain the following upper bound on code size:

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

TABLE II
THE NUMBER OF CODEWORDS OF SOME OPTIMAL CACs FROM THEOREM 14

L	w	$M(L,w)$
15	3	4
35	4	6
45	5	6
63	5	8
77	6	8
91	7	8
165	8	12
187	9	12
221	9	14

$$\leq \left\lfloor \frac{L - 1 + p + 2w - 3 - \varphi(2w - 1) - 2E}{2w - 2} \right\rfloor.$$

Note that in the last equality, we have replaced $\sum_j(|H_j| - 1)$ by (24) and each Δ_j by 1. After substituting L by $p(2w - 1)$, we obtain

$$|\mathsf{C}| \leq p + \left\lfloor \frac{2w + 2p - 4 - \varphi(2w - 1) - 2E}{2w - 2} \right\rfloor.$$

Since $2p \leq 2w + \varphi(2w - 1)$ by assumption, we have

$$|\mathsf{C}| \leq p + \left\lfloor \frac{4w - 4 - 2E}{2w - 2} \right\rfloor \leq p + 1.$$

In the last inequality, we have used the fact that $E \geq 1$. This completes the proof of Theorem 14. ∎

Some new values of $M(L, w)$ determined by Theorem 14 is shown in Table II.

VI. CONCLUSION

We derive an upper bound for the size of CAC. This is the first general bound which is applicable to any number of active users. For fixed Hamming weight w, the upper bound increases approximately with slope $(2w - 2)^{-1}$ as a function of length L. The upper bound is applied to some existing constructions of CAC, and many new values of $M(L, w)$ are determined.

REFERENCES

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

[2] C. S. Chen, K. W. Shum, C. W. Sung, W. S. Wong, and G. E. Øien, "User unsuppressible protocol sequences for collision channel without feedback," in *Proc. IEEE Int. Symp. Inf. Theory Appl.*, Auckland, Dec. 2008, pp. 1213–1218.

[3] R. Fuji-Hara and Y. Miao, "Optical orthogonal codes: Their bounds and new optimal construction," *IEEE Trans. Inf. Theory*, vol. 46, pp. 2396–2406, Nov. 2000.

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

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

[6] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1985.

[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. New York: Springer-Verlag, 1990.

[8] M. Jimbo, M. Mishima, S. Janiszewski, A. Y. Teymorian, and V. D. Tonchev, "On conflict-avoiding codes of length $n = 4 \, m$ for three active users," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2732–2742, Aug. 2007.

[9] M. Kneser, "Abschätzungen der asymptotischen dichte von summen-mengen," *Math. Zeit.*, vol. 58, pp. 459–484, 1953.

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

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

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

[13] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 31, pp. 192–204, Mar. 1985.

[14] M. Mishima, H.-L. Fu, and S. Uruno, "Optimal conflict-avoiding codes of length $n \equiv 0$ (mod 16) and weight 3," *Des. Codes Cryptogr.*, vol. 52, pp. 275–291, 2009.

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

[16] 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.

[17] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinov'ev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Inf. Theory*, vol. 41, pp. 448–455, Mar. 1995.

[18] M. B. Nathanson, *Additive Number Theory—Inverse Problems and Geometry of Sumsets, ser. Graduate Texts in Mathematics*. New York: Springer-Verlag, 1996, vol. 165.

[19] K. W. Shum and W. S. Wong, "A tight asymptotic bound on the size of constant-weight conflict-avoiding codes," *Des. Codes Cryptogr.*, 2010.

[20] 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 *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009, pp. 1368–1372.

[21] 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.

[22] B. S. Tsybakov and A. R. Rubinov, "Some constructions of conflict-avoiding codes," *Problemy Peredachi Informatsii*, vol. 38, no. 4, pp. 268–279, 2002.

[23] J. B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers," *Illinois J. Math.*, vol. 6, no. 1, pp. 64–94, 1962.

Kenneth W. Shum (M'00) received the B.Eng. degree in information engineering from the Chinese University of Hong Kong in 1993, and the M.S. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, in 1995 and 2000, respectively.

He is now a Research Fellow with the Department of Information Engineering, the Chinese University of Hong Kong. His research interests include information theory, coding theory, and cooperative communications.

Wing Shing Wong (M'81–SM'90–F'02) received the combined Bachelor and Master degree (*summa cum laude*), from Yale University, New Haven, CT, in 1976, and the M.S. and Ph.D. degrees from Harvard University, Cambridge, MA, in 1978 and 1980, respectively.

After working with AT&T Bell Laboratories, Holmdel, NJ, for 10 years, in 1992, he joined the Chinese University of Hong Kong, Shatin, and is now a Professor of Information Engineering. He was the Chairman of the Department of Information Engineering from 1995 to 2003 and is currently serving as the Dean of the Graduate School. He served as the Science Advisor at the Innovation and Technology Commission of the HKSAR Government from 2003 to 2005. He has participated in a variety of research areas including mobile communication systems, nonlinear filtering, search engine, and estimation and control of finite communication bandwidth systems.

Dr. Wong is a Co-Editor-in-Chief of Communications in Information and Systems.

Chung Shue Chen (S'02–M'05) received the B.Eng., M.Phil., and Ph.D. degrees in information engineering from the Chinese University of Hong Kong, Shatin, in 1999, 2001, and 2005, respectively.

During 2005–2006, he was an Assistant Professor with the Chinese University of Hong Kong. During 2006–2007, he was a Postdoctoral Researcher with the National Center for Scientific Research (CNRS), in Laboratory LORIA, France. During 2007–2009, he was an ERCIM "Alain Bensoussan" Fellow with the Norwegian University of Science and Technology (NTNU), Norway, and the National Center for Mathematics and Computer Science (CWI), The Netherlands. He is now an Ingénieur Expert de Recherche at INRIA, with the Research Group on Network Theory and Communications (TREC), INRIA-ENS, France, and with the INRIA Alcatel-Lucent Bell Labs Joint Research Center. His research interests include radio resource allocation, multiple access control, and QoS management for wireless communication systems.