CONSTANT WEIGHT CONFLICT-AVOIDING CODES[*]

KOJI MOMIHARA[†], MEINARD MÜLLER[‡], JUNYA SATOH,[§], AND MASAKAZU JIMBO[¶]

Abstract. A conflict-avoiding code (CAC) C of length n with weight k is a family of binary sequences of length n and weight k satisfying $\sum_{0\le t\le n-1} x_{it}x_{j,t+s} \le 1$ for any distinct codewords $x_i = (x_{i0}, x_{i1}, \ldots, x_{i,n-1})$ and $x_j = (x_{j0}, x_{j1}, \ldots, x_{j,n-1})$ in C and for any integer s, where the subscripts are taken modulo n. A CAC with maximal code size for given n and k is said to be optimal. A CAC has been studied for sending messages correctly through a multiple-access channel. The use of an optimal CAC enables the largest possible number of asynchronous users to transmit information efficiently and reliably. In this paper, various direct and recursive constructions of optimal CACs for weight $k = 4$ and 5 are obtained by providing constructions of CACs for general weight k. In particular, the maximum code size of CACs satisfying certain sufficient conditions is determined through number theoretical and combinatorial approaches.

Key words. conflict-avoiding codes, cyclotomic cosets, Kronecker density, halving starters, recursive constructions

AMS subject classifications. 94B25, 94C30, 11R45.

1. Introduction.

Several authors in [14, 15, 1, 6, 10, 17, 11, 12] have investigated protocol sequences for a multiple-access channel without feedback. In such a multiple-access channel model, the time axis is partitioned into slots whose duration corresponds to the transmission time for one packet and all users are supposed to have slot synchronization, but no other synchronization is assumed. If more than one users are sending packets in a particular slot simultaneously, then there is a conflict and the channel output in that slot is the unreadable collision symbol, called an *erasure*.

If the binary protocol sequence $x_i = (x_{i0}, x_{i1}, \ldots, x_{i,n-1})$ has Hamming weight k, then user i sends k packets in each frame of n slots, where his protocol sequence appears. When a user i is sending a message by using a protocol sequence x_i, different message from the other user may be sent by a protocol sequence x_j or its cyclic shift since only slot synchronization is assumed. The set $C = \{x_1, x_2, ..., x_N\}$ of N binary sequences is called an (N, u, n, σ) *protocol sequence set* if any $x_i \in C$ is of length n and has the property that at least σ successful packet transmissions in a frame are guaranteed for each active user, provided that at most u users out of N asynchronous users are active. In order to guarantee each user that at least σ information packets in a frame are survived from collision, the weight k of an (N, u, n, σ) protocol sequence set satisfies $k \ge u + \sigma - 1$. If there are more than one packets survived from collision, there may be a chance to use an inner code for erasure correction. In [1, 6], an $(n' = k, k' = \sigma, d' = k - \sigma + 1)$ shortened Reed-Solomon (RS) code over GF(q) was proposed as a code for each user to code his σ information packets into w transmitted packets, since a $(k, \sigma, k - \sigma + 1)$ shortened RS code can correct at most $w - \sigma$ position erasures where the user's packets suffer from collision

[*] The work of M. Jimbo was supported by JSPS Scientific Research (B)18340024 and by Monbu Kagakusyo Exploratory Research 17650080.

[†] Graduate School of Information Science, Nagoya University, Furo-cho, Chikusa-ku, 464-8601, Japan, (momihara@math.cm.is.nagoya-u.ac.jp).

[‡] Department of Computer Science, University of Bonn, Römerstr. 164, 53117, Bonn, German (meinard@cs.uni-bonn.de).

[§] Graduate School of Information Science, Nagoya University, Furo-cho, Chikusa-ku, 464-8601, Japan, (jsatoh@math.human.nagoya-u.ac.jp).

[¶] Graduate School of Information Science, Nagoya University, Furo-cho, Chikusa-ku, 464-8601, Japan, (jimbo@is.nagoya-u.ac.jp).

and then the σ information packets are recovered at the receiver. In order to use an inner code, every protocol sequence of C should have constant weight k, and such an (N, u, n, σ) protocol sequence set C is also called a *conflict-avoiding code* (CAC) *of length n with weight k*. In this paper, it is not objective to discuss inner codes for erasure correction but to provide an upper bound on N for given n and k in the case of $k = u + \sigma - 1$ and to construct "optimal" conflict-avoiding codes attaining the bound.

Let $\mathcal{P}(n, k)$ denote the set of all k-subsets of the set $[0 : n-1] = \{0, 1, \ldots, n-1\}$. In this paper, if necessary, elements of the set $[0 : n-1]$ may be identified with those of $\mathbb{Z}_n$, the residue ring of integers modulo n, or $\mathrm{GF}(n)$, the Galois field for a prime n. Each element $x \in \mathcal{P}(n, k)$ can be identified with a binary vector in $\{0, 1\}^n$ of Hamming weight k with x representing the indices of the nonzero positions. Each element x is also called a *codeword* of *length* n and *weight* k. Given such a codeword x, we define the *difference set* of x by

$$\Delta(x) = \big\{ j - i \pmod{n} : i, j \in x, i \neq j \big\}. \tag{1.1}$$

Note that all elements of $\Delta(x)$ are positive and that $\Delta(x)$ contains at most $k(k-1)$ differences. Furthermore, $i \in \Delta(x)$ implies $(n-i) \in \Delta(x)$, i.e., $\Delta(x)$ is symmetric with respect to $n/2$. We also define the *halved difference set* $\Delta_2(x) = \Delta(x) \cap [1 : \lceil n/2 \rceil]$. In mathematical notation, a conflict-avoiding code of length n with weight k is a subset $C \subset \mathcal{P}(n, k)$ satisfying the following condition:

$$\forall x, y \in C, x \neq y : \ \Delta(x) \cap \Delta(y) = \emptyset. \tag{1.2}$$

For given n and k, let $\mathrm{CAC}(n, k)$ denote the class of all conflict avoiding codes of length n with weight k. The maximal size of some code in $\mathrm{CAC}(n, k)$ will be denoted by $\mathrm{M}(n, k)$, i.e.,

$$\mathrm{M}(n, k) = \max\{|C| : C \in \mathrm{CAC}(n, k)\}. \tag{1.3}$$

A code $C \in \mathrm{CAC}(n, k)$ is said to be *optimal*, if $|C| = \mathrm{M}(n, k)$. The advantage of using an optimal CAC is that it enables the largest number of asynchronous users to transmit packets efficiently and reliably in such a multiple-access channel model.

In case of weight $k = 3$, Levenshtein [11] showed a construction of optimal CACs of length n for every $n \equiv 2 \pmod 4$ and for sufficiently large odd integer n. Jimbo et al. [8] obtained a construction of an optimal CAC in the case when $n = 4m$ and $m \equiv 2 \pmod 4$ for $k = 3$. In case of general k, Levenshtein [12] gave an infinite series of CACs with $n = p^r$, $k = (p+1)/2$ and code size $|C| = (n-1)/(2(k-1))$ for any prime $p \geq 3$ and integer $r \geq 2$. In the remainder of this paper, we will describe various direct and recursive constructions, making use of cyclotomic cosets of Galois fields and combinatorial notions such as halving starters, to obtain optimal CACs. In Section 2, we show upper bounds on code size of CACs with weight $k = 4$ and 5. In Section 3, some sufficient conditions to construct CACs from cyclotomic cosets of Galois fields are obtained, where the resultant CACs are optimal in case of $k = 4$ and 5. In particular, we use the well known Chebotarëv's density theorem in class field theory to show the infinite existence of optimal CACs of length prime $n = 6m + 1$ with weight $k = 4$ attaining the upper limit obtained in Section 2. In Section 4, we see the asymptotic behavior for the maximum size of codewords of CACs of length $n \equiv 0 \pmod 3$ with weight $k = 4$ by using the Euler's φ-function and some sufficient condition to construct such optimal CACs is obtained. In Section 5, we can give sufficient conditions to construct optimal CACs $C \in \mathrm{CAC}(n,4)$ with $\mathrm{M}(n,4) = \frac{n+2}{6}$ for $n \equiv 0 \pmod 4$. Moreover, we show that such optimal CACs exist infinitely many by using the Chebotarëv's density theorem, again. Furthermore, by utilizing a recursive construction which is obtained in Section 6, we determine the value of $\mathrm{M}(n,4)$ for length $n = 3p_1p_2\cdots p_r$ and weight $k = 4$, where each p_i, $i \in [1:r]$, is a prime such that $p_i \equiv 7 \pmod 8$. In case of weight $k = 5$, we obtain a construction of an optimal CAC of length $n = 2p_1p_2\cdots p_r$ where each p_i, $i \in [1:r]$, is a prime such that $p_i \equiv 5 \pmod{24}$ and an optimal CAC of length $n = 4p_1p_2\cdots p_r$ where each p_i, $i \in [1:r]$, is a prime such that $p_i \equiv 11 \pmod{12}$.

2. Equi-Difference CACs and Upper Bounds on Code Size. In order to find codes of large size, the condition given in (1.2) suggests to use many codewords that possess a difference set of small size. This motivates the following definition. A codeword $x \in \mathcal{P}(n,k)$ is said to be *equi-difference* with *generator* $i \in [1:n-1]$, if it is of the form

$$x = x_i = \{0, i, 2i, \ldots, (k-1)i\}, \tag{2.1}$$

where each term is reduced modulo n. Note that the assumption that $x = x_i$ is k-subset implies the condition $ji \not\equiv 0 \pmod n$ holds for every $j \in [1:k-1]$. Furthermore, for an equi-difference codeword x_i one has $\Delta(x_i) = \{\pm ji \,(\mathrm{mod}\; n) : j \in [1:k-1]\}$ and $|\Delta(x_i)| \leq 2(k-1)$. A codeword with $|\Delta(x)| < 2(k-1)$ is said to be *exceptional.* It should be noted that there may exist exceptional codewords which are not equi-difference. A code $C \in \mathrm{CAC}(n,k)$ is said to be *equi-difference* if it entirely consists of equi-difference codewords. The set of generators of such a code will be denoted by $\Gamma(C)$. Furthermore, the subclass of equi-difference codes in $\mathrm{CAC}(n,k)$ will be denoted by $\mathrm{CAC}^{\mathrm{e}}(n,k)$, and the maximal size of some equi-difference CACs by $\mathrm{M}^{\mathrm{e}}(n,k)$. Obviously, one has $\mathrm{M}^{\mathrm{e}}(n,k) \leq \mathrm{M}(n,k)$.

Now we consider the case of equi-difference conflict-avoiding codes with weight $k = 4$. The equi-difference codewords with weight $k = 4$ are of the form $x_i = \{0, i, 2i, 3i\}$ for $i \in [1:n-1] \setminus \{n/2, n/3, 2n/3\}$, where the notation $[1:n-1] \setminus \{n/2, n/3, 2n/3\}$ implies that $n/2$, $n/3$ and $2n/3$ are removed from $[1:n-1]$ only when these numbers are integers. It is not hard to see that for a general codeword x of weight four one has $3 \leq |\Delta(x)| \leq 12$ and $|\Delta(x)| \leq 6$ if and only if x is an equi-difference codeword. Furthermore, for an exceptional codeword x one tediously checked that $|\Delta(x)| = 3 \Leftrightarrow x = \{0, n/4, n/2, 3n/4\}$, $|\Delta(x)| = 4 \Leftrightarrow x = \{0, n/5, 2n/5, 3n/5\}$, and $|\Delta(x)| = 5 \Leftrightarrow x = \{0, d, n/2, n/2+d\}$ or $x = \{0, d, n/2, n-d\}$ for any $d \in [1:n-1] \setminus \{0, n/4, n/2, 3n/4\}$. Note that for a given $C \in \mathrm{CAC}(n,4)$, the difference sets $\Delta(x)$ for $x \in C$ are pairwise disjoint subsets of $[1:n-1]$. From this fact, one obtains the following upper bound on code size.

Lemma 2.1. *Let $n = 2^r5^sm$, where m is not divisible by 2 and 5. Then it holds that*

$$\mathrm{M}(n,4) \leq \begin{cases} \lfloor n/6 \rfloor, & \textit{if } r = 1,\ s = 0, \\ \lfloor (n+1)/6 \rfloor, & \textit{if } r = 0,\ s \geq 1, \\ \lfloor (n+2)/6 \rfloor, & \textit{if } r \geq 2,\ s = 0,\ \textit{or } r = 1,\ s \geq 1, \\ \lfloor (n+4)/6 \rfloor, & \textit{if } r \geq 2,\ s \geq 1, \\ \lfloor (n-1)/6 \rfloor, & \textit{if } r = s = 0. \end{cases}$$

For example, if $r \geq 2$ and $s \geq 1$, since some $C \in \mathrm{CAC}(n,4)$ can contain two exceptional codewords, $x_{n/4} = \{0, n/4, n/2, 3n/4\}$ and $x_{5/n} = \{0, n/5, 2n/5, 3n/5\}$, we have $\mathrm{M}(n,4) \le \lfloor (n-1-|\Delta(x_{n/4})|-|\Delta(x_{5/n})|)/6 \rfloor + 2 = \lfloor (n+4)/6 \rfloor$. The other cases are checked similarly.

Since $\Delta(x_i) = \Delta(x_{n-i})$, we only need to consider the equi-difference codwords for $i \in [1 : \lfloor (n-1)/2 \rfloor] \setminus \{n/3\}$. The halved difference set $\Delta_2(x_i)$ is given by

$$\Delta_2(x_i) = \begin{cases} \{i, 2i, 3i\}, & 1 \le i \le \lfloor n/6 \rfloor, \\ \{i, 2i, n-3i\}, & \lfloor n/6 \rfloor < i \le \lfloor n/4 \rfloor, \\ \{i, n-2i, n-3i\}, & \lfloor n/4 \rfloor < i \le \lfloor n/3 \rfloor, \\ \{i, n-2i, 3i-n\}, & \lfloor n/3 \rfloor < i \le \lfloor n/2 \rfloor. \end{cases} \tag{2.2}$$

Example 2.2. *For $n = 21$ one has $\mathrm{M}(n,4) \le 3$ by Lemma 2.1. The difference sets of the equi-difference codewords x_1, x_4, and x_5 are given by $\Delta(x_1) = \{1,2,3,20,19,18\}$, $\Delta(x_1) = \{4,8,12,17,13,9\}$, and $\Delta(x_1) = \{5,10,15,16,11,6\}$, respectively. Thus, we have $\{x_1, x_4, x_5\} \in \mathrm{CAC}^{\mathrm{e}}(21,4)$ and $\mathrm{M}(n,4) = \mathrm{M}^{\mathrm{e}}(n,4) = 3$.*

In case of $k = 5$, for exceptional codewords we have

$$|\Delta(x)| = \begin{cases} 4 & \text{iff} \quad x = \{0, n/5, 2n/5, 3n/5, 4n/5\}, \\ 5 & \text{iff} \quad x = \{0, n/6, n/3, n/2, 2n/3\}, \\ 6 & \text{iff} \quad x = \{0, n/7, 2n/7, 3n/7, 4n/7\},\ x = \{0, n/7, 2n/7, 3n/7, 5n/7\} \\ & \qquad \text{or } x = \{0, n/7, 2n/7, 4n/7, 5n/7\}, \\ 7 & \text{iff} \quad x = \{0, n/8, n/4, 3n/8, n/2\},\ x = \{0, n/8, 2n/8, 3n/8, 5n/8\}, \\ & \qquad x = \{0, n/8, n/4, n/2, 5n/8\},\ x = \{0, n/8, n/4, n/2, 3n/4\} \\ & \qquad \text{or } x = \{0, n/8, 3n/8, n/2, 3n/4\}, \end{cases}$$

and obtain the following upper bound on code size, similar to the case $k = 4$.

Lemma 2.3. *Let $n = 2^r 3^s 5^t 7^u m$, where m is not divisible by $2, 3, 5$ and 7. Then it holds that*

$$\mathrm{M}(n,5) \le \begin{cases} \lfloor n/8 \rfloor, & \text{if } r \ge 3, s = t = u = 0, \\ \lfloor (n+1)/8 \rfloor, & \text{if } s \ge 0, u \ge 1, r = t = 0, \text{ or } 1 \le r \le 2, u \ge 1, s = t = 0, \\ \lfloor (n+2)/8 \rfloor, & \text{if } r, s \ge 1, t = u = 0, \text{ or } r \ge 3, u = 1, s = t = 0, \\ \lfloor (n+3)/8 \rfloor, & \text{if } s \ge 0, t \ge 1, r = u = 0, \text{ or } 1 \le r \le 2, t \ge 1, s = u = 0, \\ \lfloor (n+4)/8 \rfloor, & \text{if } r, s \ge 1, t = 0, u \ge 1, \text{ or } r \ge 3, t = 1, s = u = 0, \\ \lfloor (n+5)/8 \rfloor, & \text{if } t, u \ge 1, r = 0, s \ge 0, \text{ or } t, u \ge 1, 1 \le r \le 2, s = 0, \\ \lfloor (n+6)/8 \rfloor, & \text{if } r, s, t \ge 1, u = 0, \text{ or } t, u \ge 1, r \ge 3, s = 0, \\ \lfloor (n+8)/8 \rfloor, & \text{if } r, s, t, u \ge 1, \\ \lfloor (n-1)/8 \rfloor, & \text{if } s \ge 0, r = t = u = 0, \text{ or } 0 \le r \le 2, s = t = u = 0. \end{cases}$$

Our aim is to give an explicit construction of codes $C \in \mathrm{CAC}^{\mathrm{e}}(n,k)$ for certain parameters n such that $|C|$ attains the upper bound given in Lemmas 2.2 and 2.3 implying $\mathrm{M}(n,k) = \mathrm{M}^{\mathrm{e}}(n,k) = |C|$. However, note that the upper bounds on $\mathrm{M}(n,k)$ for general weight k are not known.

3. Direct Constructions of CACs from Finite Fields. For given $n, k \in \mathbb{N}$, let $m = \lfloor n/2(k-1) \rfloor$ and $c = n - 2(k-1)m$. In the case $c = 1$, one can construct optimal codes $C \in \mathrm{CAC}^{\mathrm{e}}(n,k)$ with $|C| = m$ for primes $n = 2(k-1)m + 1$ satisfying certain sufficient conditions. The techniques are similar to Wilson's construction of difference families obtained from Galois fields. (For example, see [3, 4, 9, 18].)

In the rest of this paper, we use the following notation. Given a primitive element $\alpha \in \mathrm{GF}(p)$ and some divisor $e|(p-1)$, let $\gamma = \alpha^e$ and denote the multiplicative subgroup with generator γ by $\langle \gamma \rangle$. The cosets $H_j^e(p) = \alpha^j \langle \gamma \rangle$, $0 \le j < e$, are called the *cyclotomic cosets* of $\mathrm{GF}(p)$ of index e denoted by $\mathcal{H}^e(p)$. Given a list $(i_1, i_2, \ldots, i_e)$

of integers, if each coset $H_j^e(p)$, $0 \le j < e$, contains exactly one element of the list as an element of $\mathrm{GF}(p)$, then we say that the list forms a *system of distinct representative* of $\mathcal{H}^e(p)$, denoted by $\mathrm{SDR}(\mathcal{H}^e(p))$. Let ζ_k be a primitive e-th root of unity. We denote the e-th power residue symbol in $\mathbb{Q}(\zeta_e)$ by $\left(\frac{\mathfrak{a}}{\mathfrak{p}}\right)_e$, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\zeta_e)$ lying over (p) and $\mathfrak{a}$ is an ideal in $\mathbb{Q}(\zeta_e)$ prime to $\mathfrak{p}$. (See [7, 13] for the definition and basic properties.) Furthermore, if the integer ring of $\mathbb{Q}(\zeta_e)$ is a principal ideal ring, we may denote an ideal $\mathfrak{p}$ in $\mathbb{Q}(\zeta_e)$ by an algebraic number π generating $\mathfrak{p}$.

For the case $n = 2(k-1)m+1$, we consider an equi-difference code $C \in \mathrm{CAC^e}(n,k)$ of the form $C = \{x_{i_1}, x_{i_2}, \dots, x_{i_m}\}$ with m equi-difference codewords x_{i_j}. To ease the notation, we will use the concept of difference lists as defined, e. g., in [2] or [18]. In this notation, the union of all differences $\Delta(x_{i_j})$ can be written as the following product of lists:

$$\Delta(C) = \bigcup_{j=1}^{m} \Delta(x_{i_j}) = (i_1, i_2, \dots, i_m) \cdot (1, 2, \dots, k-1, -1, -2, \dots, -(k-1)),$$

where the calculation is over $\mathbb{Z}_n$. Now, if $n = 2(k-1)m+1$ is a prime, we have $|\Delta(x_{i_j})| = 2(k-1)$ and the list $\Delta(C)$ must cover each element of $\mathbb{Z}_n^\times$ exactly once in order that $|C| = m$. The following theorem gives some sufficient conditions for the existence of such equi-difference CACs.

Theorem 3.1. *Let $p = 2(k-1)m+1$ be a prime such that $(1, 2, \dots, k-1)$ forms an $\mathrm{SDR}(\mathcal{H}^{k-1}(p))$. Then there exists an equi-difference code $C \in \mathrm{CAC^e}(n = p, k)$ with $|C| = \mathrm{M^e}(n,k) = m$.*

Proof. Let p satisfy the conditions of the theorem, and let $\gamma = \alpha^{k-1}$ for a primitive element $\alpha \in \mathrm{GF}(p)^\times$. Since $(p-1)/2 = (k-1)m$ is a multiple of $k-1$, we have $-1 = \alpha^{(k-1)m} = \gamma^m \in H_0^{k-1}(p)$. Let $\Gamma(C) = \{1, \gamma, \dots, \gamma^{m-1}\}$, then the list of all differences of C is given by

$$\begin{aligned}\Delta(C) &= (1, \gamma, \dots, \gamma^{m-1})(1, 2, \dots, k-1, -1, -2, \dots, -(k-1)) \\ &= (1, \gamma, \dots, \gamma^{m-1})(1, \gamma^m)(1, 2, \dots, k-1) \\ &= (1, \gamma, \dots, \gamma^{2m-1})(1, 2, \dots, k-1) \\ &= H_0^{k-1}(p)(1, 2, \dots, k-1) \\ &= \mathrm{GF}(p)^\times,\end{aligned}$$

where the calculation is over $\mathrm{GF}(p)$. In other words, all elements of $\mathrm{GF}(p)^\times$ appear exactly once as difference in $\Delta(C)$, which proves the theorem. □

Note that equi-difference CACs of $k = 4$ and 5 constructed by this theorem are optimal by Lemmas 2.1 and 2.3 since $n = p$ is a prime. Now the statements of Theorem 3.1 can be expressed in another way by the following lemma.

Lemma 3.2. *Let p be a rational prime and e a rational integer prime to p. Then (i) a list of integers $(i_1, i_2, \dots, i_e)$ forms an $\mathrm{SDR}(\mathcal{H}^e(p))$ if and only if (ii) $\left(\frac{i_j}{\mathfrak{p}}\right)_e$, $1 \le j \le e$, are distinct from each other, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\zeta_e)$ lying over (p).*

Proof. Let i be a rational integer prime to p. We define $x_i, y_i \in \mathbb{Z}$ by

$$i \equiv \alpha^{x_i} \pmod{p} \quad \text{and} \quad \left(\frac{i}{\mathfrak{p}}\right)_e = \zeta_e^{y_i}.$$

We note that x_i and y_i are uniquely determined by i modulo $p-1$ and e, respectively. By the definition of e-th power residue symbol, that is $\left(\frac{i}{\mathfrak{p}}\right)_e \equiv i^{\frac{N_\mathfrak{p}-1}{e}} \pmod{\mathfrak{p}}$, we have

$$\zeta_e^{y_i} \equiv i^{\frac{N_\mathfrak{p}-1}{e}} \equiv \alpha^{x_i \frac{N_\mathfrak{p}-1}{e}} \pmod{\mathfrak{p}},$$

where $N_\mathfrak{p}$ is the norm of $\mathfrak{p}$. In particular, if $i = \alpha$, then $x_\alpha \equiv 1 \pmod{p-1}$ and $\zeta_e^{y_\alpha} \equiv \alpha^{\frac{N_\mathfrak{p}-1}{e}} \pmod{\mathfrak{p}}$. Hence we have

$$\zeta_e^{y_i} \equiv \zeta_e^{y_\alpha x_i} \pmod{\mathfrak{p}}. \tag{3.1}$$

Since p and e are relatively prime, the congruence (3.1) is exactly equality. Hence we have $y_i \equiv y_\alpha x_i \pmod{e}$.

((i)⇒(ii)) If $(i_1, i_2, \ldots, i_e)$ forms an SDR$(\mathcal{H}^e(p))$, x_{i_j}, $1 \le j \le e$, are distinct from each other modulo e and from the above argument,

$$y_{i_j} \equiv y_\alpha x_{i_j} \pmod{e} \tag{3.2}$$

holds. Furthermore, we have $N_\mathfrak{p} = p$ and $\zeta_e^{y_\alpha} \equiv \alpha^{\frac{p-1}{e}} \pmod{\mathfrak{p}}$ since obviously $p \equiv 1 \pmod{e}$ by the definition of $\mathcal{H}^e(p)$. This implies $(y_\alpha, e) = 1$. Therefore, y_{i_j}, $1 \le j \le e$, are distinct from each other modulo e, i.e., $\left(\frac{i_j}{\mathfrak{p}}\right)_e$, $1 \le j \le e$, are distinct from each other.

((ii)⇒(i)) If $\left(\frac{i_j}{\mathfrak{p}}\right)_e$, $1 \le j \le e$, are distinct from each other, we have $(y_\alpha, e) = 1$ since (3.2) holds for any i_j , $1 \le j \le e$, and y_{i_j} are distinct from each other modulo e. This implies that x_{i_j}, $1 \le j \le e$, are distinct from each other modulo e, i.e., $(i_1, i_2, \ldots, i_e)$ forms an SDR$(\mathcal{H}^e(p))$. □

In particular, in the case of $k = 4$, we can obtain the following statements by using Lemma 3.2.

Corollary 3.3. *Let $p = 6m + 1$ be a prime and let $\pi = a + b\zeta_3 \in \mathbb{Z}[\zeta_3]$ be a prime element such that $p = \pi\bar{\pi}$ satisfying*

$$\begin{cases} a \equiv 2 \pmod{6}, \\ b \equiv 3 \pmod{18}, \end{cases} \text{or} \begin{cases} a \equiv 5 \pmod{6}, \\ b \equiv 15 \pmod{18}, \end{cases}$$

where $\bar{\pi}$ means the complex conjugate of π. Then there exists an optimal equi-difference code $C \in \mathrm{CAC^e}(n = p, 4)$ with $|C| = \mathrm{M}(n, 4) = \mathrm{M^e}(n, 4) = m$.

Proof. By Lemma 3.2, it is sufficient to show that $\left(\frac{i}{\pi}\right)_3$, $1 \le i \le 3$, are distinct from each other iff π satisfies the above conditions. Without loss of generality, We can assume that $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$ for a prime element $\pi = a + b\zeta_3 \in \mathbb{Z}[\zeta_3]$ which satisfies $p = \pi\bar{\pi}$. It is obvious that $\left(\frac{1}{\pi}\right)_3 = 1$. By the cubic reciprocity law, we have

$$\left(\frac{2}{\pi}\right)_3 \equiv \begin{cases} 1, & \text{if } (a, b) \equiv (1, 0) \pmod{2}, \\ \zeta_3, & \text{if } (a, b) \equiv (0, 1) \pmod{2}, \\ \zeta_3^2, & \text{if } (a, b) \equiv (1, 1) \pmod{2}, \end{cases}$$

since 2 is also a prime element of $\mathbb{Z}[\zeta_3]$ (see [7, 13]). Also we have

$$\left(\frac{3}{\pi}\right)_3 \equiv \zeta_3^{\frac{ab}{3}} \pmod{\pi}$$

by using $3 = -\zeta_3^2(1-\zeta_3^2)^2$ and the supplement law of cubic reciprocity. Then one can readily checked that $\left(\frac{2}{\pi}\right)_3 = \zeta_3$ and $\left(\frac{3}{\pi}\right)_3 = \zeta_3^2$ iff $(a,b) \equiv (2,3) \pmod{(6,18)}$, and $\left(\frac{2}{\pi}\right)_3 = \zeta_3^2$ and $\left(\frac{3}{\pi}\right)_3 = \zeta_3$ iff $(a,b) \equiv (5,15) \pmod{(6,18)}$. Thus the assertion holds. □

Let K be an abelian extension of an algebraic number field F. We define a set M_σ of prime ideals in F for a fixed $\sigma \in \mathrm{Gal}(K/F)$ as follows:

$$M_\sigma = \{\mathfrak{P} \cap F : \mathfrak{P} \text{ is a prime ideal in } K \text{ such that } \sigma_{\mathfrak{P}} = \sigma\},$$

where $\sigma_{\mathfrak{P}}$ is a Frobenius substitution with respect to $\mathfrak{P}$ in K/F. Since K is an abelian extension, $\sigma_{\mathfrak{P}}$ depends only on the prime ideal $\mathfrak{p}$ of F lying under $\mathfrak{P}$. So $\sigma_{\mathfrak{P}}$ may be denoted by the Artin symbol $\left(\frac{K/F}{\mathfrak{p}}\right)$.

By utilizing the following proposition, we can show that the primes satisfying the condition of Corollary 3.3 exist infinitely many. The proposition is well known as Chebotarëv's density theorem [16].

Proposition 3.4. *If K/F is an abelian extension, the Kronecker density $\delta(M_\sigma)$ of the set of prime ideals such that $\left(\frac{K/F}{\mathfrak{p}}\right) = \sigma$ for each $\sigma \in \mathrm{Gal}(K/F)$ is equal to $\frac{1}{[K:F]}$, i.e.,*

$$\delta(M_\sigma) = \lim_{s\to 1+0} \sum_{\mathfrak{p}\in M_\sigma} \frac{1}{(N_{\mathfrak{p}})^s} / \log\frac{1}{s-1} = \frac{1}{[K:F]}.$$

In particular, there exist infinitely many those prime ideals $\mathfrak{p}$ in F.

Note that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_k = 1 \Longleftrightarrow \left(\frac{\mathbb{Q}(\zeta_k, \sqrt[k]{\alpha})/\mathbb{Q}(\zeta_k)}{\mathfrak{p}}\right) = 1.$$

By utilizing Proposition 3.4, we can show that the primes satisfying the condition of Corollary 3.3 exist infinitely many as follows:

Corollary 3.5. *The Kronecker density of the set of all primes satisfying the conditions of Corollary 3.3 is equal to $\frac{1}{9} = 0.11\cdots$, and there exist infinitely many those primes.*

Proof. By Lemma 3.2, $(1,2,3)$ forms an $\mathrm{SDR}(\mathcal{H}^3(p))$ iff

$$\left(\frac{6}{\pi}\right)_3 = 1 \text{ and } \left(\frac{2}{\pi}\right)_3 \neq 1, \tag{3.3}$$

where $\mathfrak{p} = (\pi)$ is a prime ideal in $\mathbb{Q}(\zeta_3)$ lying over (p). By class field theory, if $\mathfrak{P}$ is a prime ideal in $\mathbb{Q}(\zeta_3, \sqrt[3]{6})$ lying over (p), then a necessary and sufficient condition for (3.3) is

$$\left(\frac{\mathbb{Q}(\zeta_3, \sqrt[3]{2}, \sqrt[3]{6})/\mathbb{Q}(\zeta_3, \sqrt[3]{6})}{\mathfrak{P}}\right) \neq 1$$

and the density of $\{\mathfrak{P}\}$ in $\mathbb{Q}(\zeta_3, \sqrt[3]{6})$ is equal to

$$\frac{[\mathbb{Q}(\zeta_3, \sqrt[3]{2}, \sqrt[3]{6}) : \mathbb{Q}(\zeta_3, \sqrt[3]{6})] - 1}{[\mathbb{Q}(\zeta_3, \sqrt[3]{2}, \sqrt[3]{6}) : \mathbb{Q}(\zeta_3, \sqrt[3]{6})]} = \frac{2}{3}.$$

It is sufficient to consider only rational primes which split completely in $\mathbb{Q}(\zeta_3, \sqrt[3]{6})$. It follows that the Kronecker density of the set of all those primes is equal to

$$\frac{2}{3}\frac{1}{[\mathbb{Q}(\zeta_3, \sqrt[3]{6}) : \mathbb{Q}]} = \frac{2}{3}\frac{1}{[\mathbb{Q}(\zeta_3, \sqrt[3]{6}) : \mathbb{Q}(\zeta_3)] \cdot [\mathbb{Q}(\zeta_3) : \mathbb{Q}]} = \frac{1}{9}. \qquad \square$$

In fact by computer search, the frequency ratio of those primes in the first $1,000$ primes is equal to $\frac{110}{1000} \fallingdotseq \frac{1}{9}$. Table 7.1 in Section 7 shows such 110 primes.

Example 3.6. *Let $p = 37$ and $k = 4$, then $\alpha = 2 \in \mathrm{GF}(37)^\times$ is a primitive element. Since $1 \in H^3(p)$, $2 = \alpha \in H^3_1(p)$, and $3 = \alpha^{26} \in H^3_2(p)$, $(1, 2, 3)$ forms an $\mathrm{SDR}(\mathcal{H}^3(p))$, and p satisfies the conditions of Theorem 3.1. Let $\gamma = \alpha^3 = 8$, then $(1, \gamma, \dots, \gamma^m) = (1, 8, 27, 31, 26, 23)$ defines a list of generators for an optimal code $C \in \mathrm{CAC^e}(37, 4)$ with $|C| = \mathrm{M}(37, 4) = 6$.*

Note that when $k = 5$ and $p = 8m + 1$ is a prime, $(1, 2, 3, 4)$ does not form an $\mathrm{SDR}(\mathcal{H}^4(p))$. The fact is easily seen. Since 2 is a square in $\mathrm{GF}(p)$, we obtain $2 \in H^4_0(p) \cup H^4_2(p)$. This implies $4 = 2^2 \in H^4_0(p)$. Since we also have $1 \in H^4_0(p)$, $(1, 2, 3, 4)$ cannot form an $\mathrm{SDR}(\mathcal{H}^4(p))$.

We can give another sufficient condition to construct an equi-difference code $C \in \mathrm{CAC}(n = sp, k = es + 1)$, where $e \geq 1$ and $s > 1$ are positive integers and p is a prime, which satisfies $\mathbb{Z}_n \setminus \Delta(C) = p\mathbb{Z}_n$.

Theorem 3.7. *Let $e \geq 1$ and $s > 1$ be positive integers and let $p = 2em + 1$ a prime such that each of $(i - es, i - (e - 1)s, \dots, i + (e - 1)s)$, $i \in [1 : s - 1]$, and $(\pm s, \pm 2s, \dots, \pm es)$ forms an $\mathrm{SDR}(\mathcal{H}^{2e}(p))$. Then there exists an equi-difference code $C \in \mathrm{CAC^e}(n = sp, k = es + 1)$ with $|C| = \mathrm{M^e}(n, k) = m$, which satisfies $\mathbb{Z}_n \setminus \Delta(C) = p\mathbb{Z}_n$.*

Proof. For e, s and p satisfying the conditions of the theorem, let $\gamma = \alpha^{2e}$ for a primitive element $\alpha \in \mathrm{GF}(p)^\times$. Since p is a prime, $\mathbb{Z}_s \times \mathrm{GF}(p)$ can be identified with $\mathbb{Z}_{sp}$. Let $\Gamma(C) = \{1\} \times \{1, \gamma, \dots, \gamma^{m-1}\}$ over $\mathbb{Z}_s \times \mathrm{GF}(p)$. The differences arised from each codeword of C, for example a codeword $x_{(1,\gamma^j)}$ with generator $(1, \gamma^j)$, are

$$\Delta^i(x_{(1,\gamma^j)}) = \begin{cases} \{0\} \times \{\pm s, \pm 2s, \dots, \pm es\}, & i = 0, \\ \{i\} \times \{i - es, i - (e - 1)s, \dots, i + (e - 1)s\}, & 1 \leq i \leq s - 1, \end{cases}$$

where $\Delta^i(x_{(1,\gamma^j)})$ is the set of differences of the form $(i, -)$ arised from $x_{(1,\gamma^j)}$. Then the list of all differences of C is given by

$$\begin{aligned} \Delta(C) &= ((1, 1), (1, \gamma), \dots, (1, \gamma^{m-1}))(1, 2, \dots, k - 1, -1, -2, \dots, -(k - 1)) \\ &= \Big(\bigcup_{i \in [1:s-1]} \{i\} \times ((1, \gamma, \dots, \gamma^{m-1})(i - es, i - (e - 1)s, \dots, i + (e - 1)s)) \Big) \\ &\quad \cup \Big(\{0\} \times ((1, \gamma, \dots, \gamma^{m-1})(\pm s, \pm 2s, \dots, \pm es)) \Big) \\ &= \bigcup_{i \in [0:s-1]} (\{i\} \times \bigcup_{j \in [0:2e-1]} H^{2e}_j(p)) \\ &= \mathbb{Z}_s \times \mathrm{GF}(p)^\times, \end{aligned}$$

where the calculation is over $\mathbb{Z}_s \times \mathrm{GF}(p)$. In other words, all elements of $\mathbb{Z}_s \times \mathrm{GF}(p)^\times$ appear exactly once as difference in $\Delta(C)$, which proves the theorem. Note that $(\mathbb{Z}_s \times \mathrm{GF}(p)) \setminus \Delta(C) = \mathbb{Z}_s \times \{0\} \simeq p\mathbb{Z}_{sp}$. $\square$

Note that equi-difference CACs of $k = 4$ and 5 constructed by this theorem are optimal by Lemmas 2.1 and 2.3. In the case of $k = 4$ and 5, the statements of

Theorem 3.7 can expressed in another way by using quadratic desidue. In case of $e = 1$ and $s = 3$, we obtain the following infinite series of an optimal CAC for $k = 4$.

Corollary 3.8. *Let $p = 2m + 1$ be a prime such that $p \equiv 7 \pmod 8$. Then there exists an optimal code $C \in \mathrm{CAC^e}(n = 3p, 4)$ with $|C| = \mathrm{M}(n, 4) = \mathrm{M^e}(n, 4) = m$, which satisfies $\mathbb{Z}_n \setminus \Delta(C) = p\mathbb{Z}_n$.*

Proof. By Theorem 3.7 and Lemma 3.2, it is sufficient to show that $\left(\frac{i}{p}\right)_2$ are distinct for each of $i \in \{1, -1\}$ and $i \in \{1, -2\}$ iff $p \equiv 7 \pmod 8$. Obviously $\left(\frac{1}{p}\right)_2 = 1$. And $\left(\frac{-1}{p}\right)_2 = -1$ iff $p \equiv 3 \pmod 4$. By the supplement of quadratic reciprocity,

$$\left(\frac{2}{p}\right)_2 = \begin{cases} 1, & \text{iff } p \equiv 1, 7 \pmod 8, \\ -1, & \text{iff } p \equiv 3, 5 \pmod 8 \end{cases} \tag{3.4}$$

holds. Hence, $\left(\frac{-1}{p}\right)_2 = -1$ and $\left(\frac{-2}{p}\right)_2 = -1$ iff $p \equiv 7 \pmod 8$. Thus each of $\{1, -1\}$ and $\{1, -2\}$ forms an $\mathrm{SDR}(\mathcal{H}^2(p))$ iff $p \equiv 7 \pmod 8$. □

Example 3.9. *Let $p = 7$, $s = 3$ and $e = 1$. Note that 3 is the primitive elements of $\mathrm{GF}(7)^\times$ and $H_0^2(7) = \{1, 2, 4\}$. Then, $((1, 1), (1, 2), (1, 4))$ over $\mathbb{Z}_3 \times \mathbb{Z}_7$ (or $(1, 16, 4)$ over $\mathbb{Z}_{21}$) defines a list of generators for an optimal code $C \in \mathrm{CAC^e}(21, 4)$ with $|C| = \mathrm{M}(21, 4) = 3$.*

In the case of $k = 5$, in particular the case of $e = 2$ and $s = 2$, we can obtain an infinite series of optimal CACs as follows:

Corollary 3.10. *Let $p = 4m + 1$ be a prime such that $p \equiv 5 \pmod{24}$. Then there exists an optimal code $C \in \mathrm{CAC^e}(n = 2p, 5)$ with $|C| = \mathrm{M}(n, 5) = \mathrm{M^e}(n, 5) = m$, which satisfies $\mathbb{Z}_n \setminus \Delta(C) = p\mathbb{Z}_n$*

Proof. By Theorem 3.7, we show that each of $\{2, 4, -2, -4\}$ and $\{1, 3, -1, -3\}$ forms an $\mathrm{SDR}(\mathcal{H}^4(p))$ iff $p \equiv 5 \pmod{24}$. Since $-1 \in H_2^4(p)$ iff $p \equiv 5 \pmod 8$, it is sufficient to show that each of $\{2, 4\}$ and $\{1, 3\}$ forms an $\mathrm{SDR}(\mathcal{H}^2(p))$, i.e, $\left(\frac{i}{p}\right)_2$ are distinct for each of $i \in \{2, 4\}$ and $\in \{1, 3\}$. iff $p \equiv 5 \pmod{24}$. Obviously $\left(\frac{1}{p}\right)_2 = 1$ and $\left(\frac{4}{p}\right)_2 = 1$. By (3.4), $\left(\frac{2}{p}\right)_2 = -1$ iff $p \equiv 3, 5 \pmod 8$. Furthermore, by quadratic reciprocity, we have

$$\left(\frac{3}{p}\right)_2 = \begin{cases} 1, & \text{iff } p \equiv 1, 11 \pmod{12}, \\ -1, & \text{iff } p \equiv 5, 7 \pmod{12}. \end{cases} \tag{3.5}$$

Hence each of $\{2, 4\}$ and $\{1, 3\}$ forms an $\mathrm{SDR}(\mathcal{H}^2(p))$ iff $p \equiv 5 \pmod{24}$. □

Furthemore, in the case of $e = 1$ and $s = 4$, we obtain the following result.

Corollary 3.11. *Let $p = 2m+1$ be a prime such that $p \equiv 11 \pmod{12}$. Then there exists an optimal $C \in \mathrm{CAC^e}(n = 4p, 5)$ with $|C| = \mathrm{M}(n, 5) = \mathrm{M^e}(n, 5) = m$, which satisfies $\mathbb{Z}_n \setminus \Delta(C) = p\mathbb{Z}_n$*

Proof. By Theorem 3.7 and Lemma 3.2, it is sufficient to show that $\left(\frac{i}{p}\right)_2$ are distinct for each of $i \in \{1, -1\}$ and $i \in \{1, -3\}$ iff $p \equiv 11 \pmod{12}$. Obviously $\left(\frac{1}{p}\right)_2 = 1$, and $\left(\frac{-1}{p}\right)_2 = -1$ iff $p \equiv 3 \pmod 4$. Furthermore, $\left(\frac{3}{p}\right)_2 = -1$ iff $p \equiv 1, 11 \pmod{12}$ by (3.5). Thus each of $\{1, -1\}$ and $\{1, -3\}$ forms an $\mathrm{SDR}(\mathcal{H}^2(p))$ iff $p \equiv 11 \pmod{12}$. □

In the case of $k \geq 6$, we can obtain some infinite serieses of CACs by similar calculations, however, we can not judge that the resultant CACs are optimal or not.

Remark 3.12. *We note that in the case $n = 6m + 1$ and for some optimal equi-difference code $C \in \mathrm{CAC}^{\mathrm{e}}(n, 4)$ with $|C| = m$, the halved difference sets $\Delta_2(x)$, $x \in C$, form a partition of the set $[1 : 3m]$. Then, it follows from (2.2) that the triples $\Delta_2(x)$, $x \in C$, are a solution to the first Heffter difference problem [5]. In the case $n = 6m + 3$ with $n/3$ is a prime and for some optimal equi-difference code $C \in \mathrm{CAC}^{\mathrm{e}}(n, 4)$ with $|C| = m$, the halved difference sets $\Delta_2(x)$, $x \in C$, form a partition of the set $[1 : 3m+1] \setminus \{2m+1\}$. Again, it follows from (2.2) that the triples $\Delta_2(x)$, $x \in C$, are a solution to the second Heffter difference problem [5]. The notions of Heffter difference problems were introduced for generating Steiner triple systems.*

4. Halving Starters. In this section, we show the asymptotic behavior of the maximum size of codewords of an equi-difference CAC of length $n = (k-1)p$ for the case of $k = 4$ and obtain further sufficient conditions to construct such optimal CACs.

In the beginning of this section, we introduce a general problem. For a given odd integer $p = 2m + 1$ and a collection $\mathcal{A}$ of unordered pairs of $\mathbb{Z}$, if there exists an h-subset S_p, $h \le m$, of $\mathbb{Z}_p \setminus \{0\}$ such that for every $\{x, y\} \in \mathcal{A}$,

$$xS_p \cap yS_p = \emptyset, \text{ and } \{0\} \notin xS_p \cup yS_p$$

over $\mathbb{Z}_p$, S_p is called a *halving starter* of size h for $\mathcal{A}$.

The following is a natural generalization of the case when $e = 1$ and $s = k - 1$ of Theorem 3.7.

Lemma 4.1. *Let $p = 2m + 1$ be a positive integer such that $(p, \ell) = 1$ for $\ell \in [1 : k-1]$, and let*

$$\mathcal{A}_k = \{\{k-1, -(k-1)\}\} \cup \{\{i, -(k-1-i)\} : 1 \le i \le k-2\}.$$

If there exists a halving starter of size h for $\mathcal{A}_k$, then there exists an equi-difference code $C \in \mathrm{CAC}^{\mathrm{e}}(n = (k-1)p, k)$ with $|C| = h$ and $\mathbb{Z}_n \setminus \Delta(C) \supseteq p\mathbb{Z}_n$.

Proof. Let S_p be a halving starter of size h for $\mathcal{A}_k$ and let $\Gamma(C) = \{(1, a) : a \in S_p\}$ over $\mathbb{Z}_{k-1} \times \mathbb{Z}_p$. Note that $\mathbb{Z}_{k-1} \times \mathbb{Z}_p \simeq \mathbb{Z}_{(k-1)p}$ and $|S_p| = |xS_p| = |yS_p|$ for every $\{x, y\} \in \mathcal{A}_k$ by the assumption $(p, \ell) = 1$ for $\ell \in [1 : k-1]$. (This also implies $(p, \ell) = 1$ for $\ell \in \pm[1 : k-1]$.) Then $\Gamma(C)$ is our desired generating set of an equi-difference CAC with $|C| = h$. In fact, the differences arised from each codeword of C, for example a codeword $x_{(1,a)}$ with generator $(1, a)$, are

$$\Delta^i(x_{(1,a)}) = \begin{cases} \{(0, (k-1)a), (0, -(k-1)a)\}, & i = 0, \\ \{(i, ia), (1, -(k-1-i)a)\}, & 1 \le i \le k-2. \end{cases}$$

By the definition of S_p, we have

$$\begin{aligned} \Delta(C) &= \bigcup_{a \in S_p} ((1, a))(1, 2, \ldots, k-1, -1, -2, \ldots, -(k-1)) \\ &= \Big(\bigcup_{i \in [1:k-2]} \bigcup_{a \in S_p} \{i\} \times ((a)(i, -(k-i-1))) \Big) \cup \Big(\bigcup_{a \in S_p} \{0\} \times ((a)(k-1, -(k-1))) \Big) \\ &= \bigcup_{i \in [1:k-2]} \Big(\{i\} \times S_p \cdot (i, -(k-1-i)) \Big) \cup \Big(\{0\} \times S_p \cdot (k-1, -(k-1)) \Big) \\ &\subseteq \bigcup_{i \in [0:k-2]} (\{i\} \times (\mathbb{Z}_p \setminus \{0\})) = \mathbb{Z}_{k-1} \times (\mathbb{Z}_p \setminus \{0\}), \end{aligned}$$

where the calculation is over $\mathbb{Z}_{k-1}\times\mathbb{Z}_p$. In other words, all elements of $\mathbb{Z}_{k-1}\times(\mathbb{Z}_p\backslash\{0\})$ appear at most once as difference in $\Delta(C)$. Note that $\mathbb{Z}_{k-1}\times\{0\}\simeq p\mathbb{Z}_{(k-1)p}$. □

We are interested in the asymptotic behavior of the size of a halving starter. We use a graph theoretical approach to see the maximal size of a halving starter for $\mathcal{A}_4$, in other words, the maximal size of codewords of $\mathrm{CAC}^{\mathrm{e}}(n=3p,4)$ constructed in Lemma 4.1. The result in the following theorem implies $\mathrm{M}(n=3p,4)\simeq\frac{n}{6}$ for sufficiently large odd p such that $(p,3)=1$. The similar techniques in the proof were used by Levenshtein in [11].

Let p be an odd integer such that $(p,3)=1$. A graph $G(p)$ has a vertex set $V=[1:p-1]$ and an edge set E, where $\{a,b\}\in E$ when $a\equiv-2b \pmod p$, $b\equiv-2a \pmod p$ or $a\equiv-b \pmod p$. Then the degree of each vertex of $G(p)$ is exactly three and the connected component containing a vertex $a\in V$ of $G(p)$ is either $G_a^1(p)=(V_a^1,E_a^1)$ or $G_a^2(p)=(V_a^2,E_a^2)$ of Figure 4.1. Let

$$r_a(p)=\min\{r>0:(2^r-1)a\equiv0 \text{ or } (2^r+1)a\equiv0 \pmod p\}$$

and

$$r(p)=\min\{r>0:2^r-1\equiv0 \text{ or } 2^r+1\equiv0 \pmod p\}.$$

Theorem 4.2. *Let p be an odd integer such that $(p,3)=1$ and $n=3p$. Then*

$$\mathrm{M}(3p,4)\geq\mathrm{M}^{\mathrm{e}}(3p,4)\geq\frac{p}{2}+O\left(\frac{p}{\log_2 p}\right).$$

Proof. By the definition of $G(p)$, the maximum size of a halving starter for $\mathcal{A}_4$ equals to the maximum size of an independent set of $G(p)$. Now we construct a halving starter S_p by choosing an independent set with maximum size from each connected component of $G(p)$. Note that, by the definition of $r_a(p)$, $r_a(p)=|V_a^1|/2$, i.e., $(-2)^{r_a(p)}a'\equiv a' \pmod p$ for $a,a'\in V_a^1$, and $r_a(p)=|V_a^2|/2$, i.e., $(-2)^{r_a(p)}a'\equiv-a' \pmod p$ for $a,a'\in V_a^2$. If $|V_a^1|\equiv0 \pmod 4$, we can choose $|V_a^1|/2=r_a(p)$ vertices as an independent set of $G_a^1(p)$, for example $\{a,2a,2^2a,\ldots,2^{r_a(p)-1}a\}$, otherwise we can choose $|V_a^1|/2-1=r_a(p)-1$ vertices, for example $\{a,2a,2^2a,\ldots,2^{r_a(p)-2}a\}$. Furthermore, if $|V_a^2|\equiv0 \pmod 4$, we can choose $|V_a^2|/2-1=r_a(p)-1$ vertices as an independent set of $G_a^2(p)$, for example $\{a,2a,2^2a,\ldots,2^{r_a(p)-2}a\}$, otherwise we can choose $|V_a^2|/2=r_a(p)$ vertices, for example $\{a,2a,2^2a,\ldots,2^{r_a(p)-1}a\}$. In other words, we can choose $r_a(p)$ vertices as an independent set of $G_a^1(p)$ or $G_a^2(p)$ depending on whether $r_a(p)$ is even or odd iff $(2^{r_a(p)}-1)a\equiv0 \pmod p$, and we can choose $r_a(p)-1$ vertices as an independent set of $G_a^1(p)$ or $G_a^2(p)$ depending on whether $r_a(p)$ is odd or even iff $(2^{r_a(p)}+1)a\equiv0 \pmod p$.

Here, let $V(b)=\{a\in V:(a,p)=b\}$ for each divisor b, $1\leq b\leq(p-1)/2$, of p and let $d=p/b$. For each integer h, $1\leq h<d$, such that $(h,d)=1$, hb and $(d-h)b$ belong to $V(b)$. Therefore, $|V(b)|=\varphi(d)$, where $\varphi(d)$ is the Euler's φ-function. By the definition of $r(d)$, all vertices of $V(b)$ are partitioned into some connected components with same size $2r(d)$. Hence, we have

$$\begin{aligned}|S_p|&=\sum_{1<d|p;\,2^{r(d)}-1\equiv0 \bmod d}\frac{\varphi(d)}{2r(d)}\cdot r(d)+\sum_{1<d|p;\,2^{r(d)}+1\equiv0 \bmod d}\frac{\varphi(d)}{2r(d)}\cdot(r(d)-1)\\&=\frac{1}{2}\sum_{1<d|n}\varphi(d)-\sum_{1<d|p;\,2^{r(d)}+1\equiv0 \bmod d}\frac{\varphi(d)}{2r(d)}\geq\frac{p-1}{2}-\sum_{1<d|p}\frac{\varphi(d)}{2r(d)}.\end{aligned}$$

By applying the Levenshtein's results in [11], that is,

$$\sum_{1<d|p} \frac{\varphi(d)}{2r(d)} < \frac{2p}{\log_2 p} + p^{1/2} p^{\Theta(1)},$$

we obtain the desired assertion. □

The following corollary gives a sufficient condition to construct optimal CACs of length $n = 3p$ for $k = 4$, where p is a prime such that $p \equiv 3, 5 \pmod 8$.

Corollary 4.3. *Let $p = 2m+1$ be a prime such that $p \equiv 3, 5 \pmod 8$ and 2 is a primitive element of* $\mathrm{GF}(p)$*. Then there exists an optimal code $C \in \mathrm{CAC^e}(n = 3p, 4)$ with $|C| = \mathrm{M^e}(n, 4) = \mathrm{M}(n, 4) = m - 1$.*

Proof. Assume that p satisfies the conditions of the corollary. Note that p satisfies the conditions of Theorem 4.2. And $2 \in H_1^2(p)$ iff $p \equiv 3, 5 \pmod 8$. Since 2 is a primitive element of $\mathrm{GF}(p)$, $2^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$ and $2^i + 1 \not\equiv 0 \pmod p$ for all $i \in [1 : \frac{p-1}{2} - 1]$. Here, by Theorem 4.2, there exists a halving starter S_p of maximum size

$$|S_p| = \frac{p-1}{2} - \sum_{1<d|p;\, 2^{r(d)}+1\equiv 0 \bmod d} \frac{\varphi(d)}{2r(d)} = \frac{p-1}{2} - \frac{\varphi(p)}{2r(p)} = \frac{p-1}{2} - 1 = m - 1.$$

This follows that there exists an equi-difference code $C \in \mathrm{CAC^e}(3p, 4)$ with $|C| = m - 1$. Hence, it is sufficient to show that $\mathrm{M}(3p, 4) = m - 1$. Note that $\mathrm{M}(3p, 4) \leq m$ by Lemma 2.1. Suppose that there is a code C^* with $|C^*| = m$. Then C^* must contain at most one codeword x with $|\Delta(x)| = 8$ and the remaining codewords must be all equi-difference by Lemma 2.1. Let E be the set of equi-difference codewords contained in C^* and let $|E| = t$, where $t = m - 1$ or m, depending on whether C^* contains x or not. Each of such t equi-difference codewords has a generator of the form $(0, a_0)$, $(1, a_1)$ or $(2, a_2)$ for some $a_0, a_1, a_2 \in \mathbb{Z}_p^\times$ since $\mathbb{Z}_{3p} \simeq \mathbb{Z}_3 \times \mathbb{Z}_p$. If C^* has $\ell > 0$ codewords with generators $(0, a_0)$'s for some $a_0 \in \mathbb{Z}_p^\times$, since C^* must have at most $(2m - 6\ell)/2$ equi-difference codewords with generators $(1, a_1)$'s or $(2, a_2)$'s for some $a_1, a_2 \in \mathbb{Z}_p^\times$, $t \leq \ell + (2m - 6\ell)/2 = m - 2\ell < m - 1$. This contradicts to $t = m-1$ or m. Hence, C^* contains no equi-difference codeword with generator $(0, a_0)$ for any $a_0 \in \mathbb{Z}_p^\times$. Furthermore, since we can regard the equi-difference codeword with generator $(2, a_2)$ as that with generator $(1, -a_2)$ for arbitrary $a_2 \in \mathbb{Z}_p^\times$, in order that $|E| = t$, the maximum number of equi-difference codewords with generators $(1, a_1)$, $a_1 \in \mathbb{Z}_p^\times$, must equal to t, i.e., the maximum size of halving starters for $\mathcal{A}_4$ equals to t. Since $t = m$ contradicts to our first arguements, we can assume that C^* contains exactly one codeword x with $|\Delta(x)| = 8$ and $t = m - 1$ equi-difference codewords with generators $(1, a_1)$'s, $a_1 \in \mathbb{Z}_p^\times$, obtained from a halving starter S_p of maximum size $m - 1$. Let $A = ((\mathbb{Z}_3 \times \mathbb{Z}_p) \setminus \{(0, 0)\}) \setminus \Delta(E)$. Then, by the definition of S_p,

$$A = \{(1, 0), (2, 0), (0, 3a), (0, -3a), (1, a), (1, 2a), (2, -a), (2, -2a)\} \tag{4.1}$$

for some $a \in \mathbb{Z}_p^\times$ and x must cover the eight elements of A as differences. Note that the graph $G(p)$ consists of exactly one connected component since 2 is a primitive element of $\mathrm{GF}(p)$. In particular, $r_a(p) = (p - 1)/2$ holds for every $a \in V$, and the connected component is $G_a^1(p)$ or $G_a^2(p)$ depending on whether $p \equiv 3$ or $5 \pmod 8$. Then one can tediously check (4.1) since $|S_p| = m - 1$. Hence, for every $y \in A$, there should be at least one element of A, say $y' \in A$, such that $y + y' \in A$. However, by using the fact that n is a prime and $a \not\equiv 0 \pmod p$, it is easily checked that such

y' does not exist in A for any $y \in A \setminus \{(1,0),(2,0)\}$. Hence A can not be the set of differences of x. Thus $\mathrm{M}(3p,4) = m-1$. □

Small primes p, $p < 1000$, satisfying the condition of Corollary 4.3 are listed below:

$p =$ 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181,
197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491,
509, 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661, 677, 701, 709, 757, 773,
787, 797, 821, 827, 829, 853, 859, 877, 883, 907, 941, 947.

5. Constructions of Optimal CACs of Length $n = 4p$ with Weight $k = 4$. In this section, we obtain some sufficient conditions in order to obtain optimal CACs of length $n = 4p$ with weight $k = 4$. The following construction is another application of halving starters. Let $\mathcal{A}'_k = \mathcal{A}_k \setminus \{\{k-1, -(k-1)\}\}$, where $\mathcal{A}_k$ was defined in Section 4.

Theorem 5.1. *Let $p = 2m+1$ be a positive integer such that $(p,\ell) = 1$ for $\ell \in [1:k]$. If there exist an equi-difference code $C \in \mathrm{CAC^e}(p,k)$ with $m_1 = |C|$ and a halving starter S_p of size m_2 for $\mathcal{A}'_{k+1}$, then there exists an equi-difference code $C' \in \mathrm{CAC^e}(n = kp, k)$ with $|C'| = m_1 + m_2 + 1$.*

Proof. Let p, k, C and S_p as stated in the theorem. Since $(p,k) = 1$, $\mathbb{Z}_k \times \mathbb{Z}_p$ can be identified with $\mathbb{Z}_{kp}$. Furthermore, $|S_p| = |xS_p| = |yS_p|$ for every $\{x,y\} \in \mathcal{A}'_{k+1}$ by the assumption $(p,\ell) = 1$ for $\ell \in [1:k-1]$. Let

$$\Gamma(C') = (\{0\} \times \Gamma(C)) \cup (\{1\} \times S_p) \cup \{(1,0)\},$$

where the elements of $\Gamma(C')$ are considered over $\mathbb{Z}_k \times \mathbb{Z}_p$. Note that the differences arised from each codeword with generator from $\{1\} \times S_p$, for example a codeword $x_{(1,a)}$ with generator $(1,a)$, are $\Delta^i(x_{(1,a)}) = \{(i, ia), (i, -(k-i)a)\}$ for each $i \in [1:k-1]$. It can be checked that $\Gamma(C')$ is a generating set of $C' \in \mathrm{CAC^e}(kp,k)$ with $|C'| = m_1 + m_2 + 1$. Obviously, $|C'| = |\Gamma(C')| = m_1 + m_2 + 1$. By the definition of S_p and the assumption $C \in \mathrm{CAC^e}(p,k)$, we have

$$\bigcup_{a \in \Gamma(C)} ((0,a))(1, 2, \ldots, k-1, -1, -2, \ldots, -(k-1)) \subseteq \{0\} \times (\mathbb{Z}_p \setminus \{0\})$$

and

$$\begin{aligned}
&\bigcup_{a \in S_p} ((1,a))(1, 2, \ldots, k-1, -1, -2, \ldots, -(k-1)) \\
&= \bigcup_{i \in [1:k-1]} \bigcup_{a \in S_p} \{i\} \times ((a)(i, -(k-i))) \\
&= \bigcup_{i \in [1:k-1]} \{i\} \times S_p \cdot (i, -(k-i)) \\
&\subseteq \bigcup_{i \in [1:k-1]} (\{i\} \times (\mathbb{Z}_p \setminus \{0\})) = (\mathbb{Z}_k \setminus \{0\}) \times (\mathbb{Z}_p \setminus \{0\}),
\end{aligned}$$

where the calculation is over $\mathbb{Z}_k \times \mathbb{Z}_p$. Finally, the differences of the form $(\ell, 0)$, $\ell \in [1:k-1]$, occur only in the codewords $x_{(1,0)}$ with generator $(1,0)$. Thus, all elements of $(\mathbb{Z}_{k-1} \times \mathbb{Z}_p) \setminus \{(0,0)\}$ appear at most once as differences in $\Delta(C)$. □

Now, we give two sufficient conditions to construct optimal CACs of length $n = 4p$ with weight $k = 4$. We use the quartic residue to give the first sufficient condition. The following lemma is a preparation of the first assertion.

LEMMA 5.2. *Let p be a rational prime and ρ a prime element of $\mathbb{Z}[\zeta_4]$ lying over (p). Then $-1,-3 \in H_2^4(p)$ if and only if $\left(\frac{-1}{\rho}\right)_4 \equiv -1$ and $\left(\frac{-3}{\rho}\right)_4 \equiv -1$.*

Proof. By the definition of the quartic residue symbol, we have

$$\left(\frac{-1}{\rho}\right)_4 \equiv (-1)^{\frac{N_\rho-1}{4}} = \begin{cases} (-1)^{\frac{p-1}{4}}, & \text{iff } p \equiv 1 \pmod 4, \\ (-1)^{\frac{p^2-1}{4}}, & \text{iff } p \equiv 3 \pmod 4. \end{cases}$$

Then one can tediously check that $\left(\frac{-1}{\rho}\right)_4 \equiv -1$ iff $p \equiv 5 \pmod 8$. On the other hand, it is obvious that $-1 \in H_2^4(p)$ iff $p \equiv 5 \pmod 8$. We define $i \in \mathbb{Z}$ by $-3 \equiv \alpha^i \pmod p$, where α is a primitive element of $\mathrm{GF}(p)$. Then we have

$$\begin{aligned}\left(\frac{-3}{\rho}\right)_4 &\equiv (-3)^{\frac{N_\rho-1}{4}} \equiv \alpha^{i\frac{N_\rho-1}{4}} = \alpha^{\frac{i}{2}\cdot\frac{p-1}{2}} \equiv (-1)^{\frac{i}{2}} \\ &\equiv \begin{cases} 1, & \text{iff } i \equiv 0 \pmod 4, \\ -1, & \text{iff } i \equiv 2 \pmod 4, \end{cases}\end{aligned}$$

by using $N_\rho = p$ and $\alpha^{\frac{p-1}{2}} \equiv -1 \pmod \rho$. Hence $\left(\frac{-1}{\rho}\right)_4 \equiv -1$ and $\left(\frac{-3}{\rho}\right)_4 \equiv -1$ iff $-1,-3 \in H_2^4(p)$. □

Now, we give the first sufficient condition.

COROLLARY 5.3. *Let $p = 24m+13$ be a prime satisfying the conditions of Corollary 3.3 and let $\rho = a + b\zeta_4 \in \mathbb{Z}[\zeta_4]$ be a prime element such that $p = \rho\bar{\rho}$ satisfying*

$$\begin{cases} a \equiv 3 \pmod{12}, \\ b \equiv 2 \pmod{12}, \end{cases} \quad or \quad \begin{cases} a \equiv 3 \pmod{12}, \\ b \equiv 10 \pmod{12}. \end{cases}$$

Then there exists an optimal code $C \in \mathrm{CAC}^{\mathrm{e}}(n = 4p, 4)$ with $|C| = \mathrm{M}^{\mathrm{e}}(n,4) = \mathrm{M}(n,4) = 16m+9$.

Proof. Without loss of generality, we can assume that $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$ for a prime element $\rho = a+b\zeta_4 \in \mathbb{Z}[\zeta_4]$ which satisfies $p = \rho\bar{\rho}$. By Lemma 5.2, $\left(\frac{-1}{\rho}\right)_4 \equiv -1$ iff $p \equiv 5 \pmod 8$. By quartic reciprocity,

$$\left(\frac{-3}{\rho}\right)_4 \equiv \begin{cases} 1, & \text{if } (a,b) \equiv (\pm 1, 0) \pmod 3, \\ -1, & \text{if } (a,b) \equiv (0, \pm 1) \pmod 3, \\ -\zeta_4, & \text{if } (a,b) \equiv (\pm 1, \pm 1) \pmod 3, \\ \zeta_4, & \text{if } (a,b) \equiv (\pm 1, \mp 1) \pmod 3. \end{cases}$$

Hence, $-1,-3 \in H_2^4(p)$ iff $(a,b) \equiv (3,2)$ or $(3,10) \pmod{12}$. Then $S_p = H_0^4(p) \cup H_1^4(p)$ defines a halving starter of size $12m+6$ for $\mathcal{A}_5'$ if p and ρ satisfy the conditions of the corollary. In fact, since $-S_p = -H_0^4(p) \cup -H_1^4(p) = H_2^4(p) \cup H_3^4(p)$ and $-3S_p = -3H_0^4(p) \cup -3H_1^4(p) = H_2^4(p) \cup H_3^4(p)$ hold, we have $S_p \cap -S_p = \emptyset$ and $S_p \cap -3S_p = \emptyset$. By combing Corollary 3.3 and Theorem 5.1, we have an equi-difference code $C \in \mathrm{CAC}^{\mathrm{e}}(4p,4)$ with $|C| = 16m+9$. By Lemma 2.1, we also have $\mathrm{M}(4p,4) = 16m+9$, i.e., the resultant CAC is optimal. □

By utilizing Proposition 3.4, we can show that the primes satisfying the condition of Corollary 5.3 exist infinitely many as follows:

COROLLARY 5.4. *The Kronecker density of the set of all primes satisfying the conditions of Corollary 5.3 is equal to $\frac{1}{2^3 \cdot 3^2} = 0.0138\cdots$, and there exist infinitely many those primes.*

Proof. By Lemmas 3.2 and 5.2, $(1, 2, 3)$ forms an $\mathrm{SDR}(\mathcal{H}^3(p))$ and $-1, -3 \in H_2^4(p)$ iff

$$\left(\frac{6}{\pi}\right)_3 = 1, \left(\frac{3}{\rho}\right)_4 = 1 and \tag{5.1}$$

$$\left(\frac{2}{\pi}\right)_3 \neq 1, \text{ and } \left(\frac{-1}{\rho}\right)_4 = -1, \tag{5.2}$$

where $\mathfrak{p} = (\pi)$ is a prime ideal in $\mathbb{Q}(\zeta_3)$ lying over (p) and $\mathfrak{r} = (\rho)$ is a prime ideal in $\mathbb{Q}(\zeta_4)$ lying over (p). Let $\mathfrak{P}$ be a prime ideal in $\mathbb{Q}(\zeta_4, \sqrt[3]{6}, \sqrt[4]{3})$ lying over (p) and

$$\sigma = \left(\frac{\mathbb{Q}(\zeta_8, \sqrt[3]{6}, \sqrt[3]{2}, \sqrt[4]{3})/\mathbb{Q}(\zeta_4, \sqrt[3]{6}, \sqrt[4]{3})}{\mathfrak{P}}\right).$$

Note that $\zeta_3 \in \mathbb{Q}(\zeta_4, \sqrt[4]{3})$. Then a necessary and sufficient condition such that (5.2) holds under (5.1) is

$$\sigma(\zeta_8) \neq \zeta_8 \text{ and } \sigma(\sqrt[3]{2}) \neq \sqrt[3]{2}. \tag{5.3}$$

Hence the density of prime ideals $\mathfrak{P}$ satisfying (5.3) in $\mathbb{Q}(\zeta_4, \sqrt[3]{6}, \sqrt[4]{3})$ is equal to $\frac{1}{3}$ and the density of rational primes p satisfying the condition of the corollary is equal to $\frac{1}{2^3 \cdot 3^2}$. □

By our computer search, the frequency ratio of those primes in the first $3,000,000$ primes is equal to $\frac{41684}{3,000,000} \fallingdotseq \frac{1}{2^3 \cdot 3^2}$.

Next, we give the second sufficient condition to construct optimal CACs of length $n = 4p$ with weight $k = 4$.

COROLLARY 5.5. *Let $p = 12m + 7$ be a prime satisfying the conditions of Corollary 3.3 such that 3 is a primitive element of* $\mathrm{GF}(p)$. *Then there exists an optimal code $C \in \mathrm{CAC}(n = 4p, 4)$ with $|C| = \mathrm{M}^{\mathrm{e}}(n, 4) = \mathrm{M}(n, 4) = 8m + 4$.*

Proof. Let p satisfy the conditions of the corollary, and let $\alpha = 3 \in \mathrm{GF}(p)$. Then we can take a halving starter of maximum size $6m + 2$ for $\mathcal{A}'_5$, for examle $S_p = \{\alpha^0, \alpha^1, \ldots, \alpha^{6m+1}\} \subset \mathrm{GF}(p)$. In fact, since

$$-S_p = \alpha^{\frac{p-1}{2}} \cdot S_p = \{\alpha^{6m+3}, \alpha^{6m+4}, \ldots, \alpha^{12m+4}\}$$

and

$$-3S_p = \alpha^{\frac{p+1}{2}} \cdot S_p = \{\alpha^{6m+4}, \alpha^{6m+5}, \ldots, \alpha^{12m+5}\}$$

hold, we have $S_p \cap -S_p = \emptyset$ and $S_p \cap -3S_p = \emptyset$. Furthermore, since $-3 \in H_0^2(p)$ and $\frac{p-1}{2}$ is odd, the maximum size of halving starters for $\mathcal{A}'_5$ is at most $6m + 2$. Now, by combining Corollary 3.3 and Theorem 5.1, we obtain an equi-difference code $C \in \mathrm{CAC}(n = 4p, 4)$ with $|C| = \mathrm{M}^{\mathrm{e}}(n, 4) = 8m + 4$. Note that $p = 12m + 7$ is a necessary condition for $3 \in H_1^2(p)$. Hence, it is sufficient to show that $\mathrm{M}(n, 4) = 8m + 4$. Here, $\mathrm{M}(n, 4) \leq 8m + 5$ by Lemma 2.1. Suppose that there is a code C^* with $|C^*| = 8m + 5$. Then again by Lemma 2.1 $\Delta(C^*) = \mathbb{Z}_{4p} \setminus \{0\}$ holds. In particular, C^* must contain exceptional codeword $x_{(1,0)}$ and $8m + 4$ equi-difference codewords, which have generators of the form $(0, a_0)$, $(1, a_1)$, $(2, a_2)$ or $(3, a_3)$ for some $a_0, a_1, a_2, a_3 \in \mathbb{Z}_p^{\times}$, since $\mathbb{Z}_{4p} \simeq \mathbb{Z}_4 \times \mathbb{Z}_p$. If C^* has $\ell > 0$ codewords with generators $(2, a_2)$ for some $a_2 \in \mathbb{Z}_p^\times$, since C^* must have at most $(12m + 6 - 4\ell)/2$ equi-difference codewords with generators $(1, a_1)$ or $(3, a_3)$ for some $a_1, a_3 \in \mathbb{Z}_p^\times$ and at most $(12m + 6 - 2\ell)/6$ equi-difference codewords with generators $(0, a_0)$ for some $a_0 \in \mathbb{Z}_p^\times$, $|C^*| \le \ell + (12m + 6 - 4\ell)/2 + (12m + 6 - 2\ell)/6 + 1 < 8m + 5$. This contradicts to the assumption, that is, $|C^*| = 8m + 5$. Hence, C^* contains no equi-difference codeword with generator $(2, a_2)$ for any $a_2 \in \mathbb{Z}_p^\times$. Furthermore, since the maximum number of codewords with generators $(0, a_0)$, $a_0 \in \mathbb{Z}_p^\times$, equals to $2m+1$ by Corollary 3.3 and we can regard the equi-difference codeword with generator $(3, a_3)$ as that with generator $(1, -a_3)$ for arbitrary $a_3 \in \mathbb{Z}_p^\times$, in order that $|C^*| = 8m + 5$, the maximum number of codewords with generators $(1, a_1)$'s, $a_1 \in \mathbb{Z}_p^\times$, must equal to $6m + 3$. This follows that the maximum size of halving starters for $\mathcal{A}'_5$ must equal to $6m+3$. However, this also contradicts to our first arguements. Thus $\mathrm{M}(n, 4) = 8m+4$. □

Small primes p safisfying the conditions of Corollary 5.3 or Corollary 5.5 are listed in Table 7.1.

Example 5.6. *Let $p = 7$ and $k = 4$, then $4p = 28$. Note that 3 is a primitive element of $\mathrm{GF}(7)$ and $S_p = \{1, 3\}$ is a halving starter of size 2 for $\mathcal{A}'_5$. Let $C \in \mathrm{CAC^e}(7, 4)$ which has one generator 1. Then, $((0, 1), (1, 1), (1, 3), (1, 0))$ over $\mathbb{Z}_4 \times \mathbb{Z}_7$ (or $(1, 8, 17, 21)$ over $\mathbb{Z}_{28}$) defines a list of generators for an equi-difference code $C' \in \mathrm{CAC^e}(28, 4)$ with $|C| = \mathrm{M}(28, 4) = 4$.*

6. A Recursive Construction of Equi-Difference CACs. In this section, we give some recursive construction of equi-difference CACs.

Theorem 6.1. *Let $k \ge 3$ and n_1, n_2 and s be positive integers satisfying $s \mid n_1$ and $(n_2, \ell) = 1$ for $\ell \in [1 : k - 1]$. Let C_1 be an equi-difference code in $\mathrm{CAC^e}(n_1, k)$ with $t_1 = |C_1|$ non-exceptional codewords satisfying*

$$\mathbb{Z}_{n_1} \setminus \Delta(C_1) \supseteq (\frac{n_1}{s})\mathbb{Z}_{n_1}. \tag{6.1}$$

And let C_2 be an equi-difference code in $\mathrm{CAC^e}(n_2, k)$ with $t_2 = |C_2|$ codewords. Then there exists an equi-difference code $C \in \mathrm{CAC^e}(n_1 n_2, k)$ with $t = |C| = n_2 t_1 + t_2$.

Proof. Let

$$\Gamma_1 = \{i + jn_1 : i \in \Gamma(C_1), j \in [0 : n_2 - 1]\} \text{ and } \Gamma_2 = \left\{j(\frac{n_1}{s}) : j \in \Gamma(C_2)\right\},$$

where each element is reduced modulo $n_1 n_2$. Then $\Gamma(C) = \Gamma_1 \cup \Gamma_2$ defines the code C consisting of equi-difference codewords. Obviously, $|\Gamma(C)| = n_2 t_1 + t_2$. We now prove C is a conflict-avoiding code by showing that the difference sets of any two codewords of C are disjoint. By (6.1) and the definition of Γ_1, it is shown that

$$\mathbb{Z}_{n_1 n_2} \setminus \bigcup_{\ell \in \pm[1:k-1]} \ell \cdot \Gamma_1 \supseteq (\frac{n_1}{s})\mathbb{Z}_{n_1 n_2}$$

holds. Furthermore, since every element of Γ_2 is a multiple of $(\frac{n_1}{s})$, it is obvious

$$\bigcup_{\ell \in \pm[1:k-1]} \ell \cdot \Gamma_2 \subseteq (\frac{n_1}{s})\mathbb{Z}_{n_1 n_2}$$

holds. These imply that

$$(\bigcup_{\ell \in \pm[1:k-1]} \ell \cdot \Gamma_1) \cap (\bigcup_{\ell \in \pm[1:k-1]} \ell \cdot \Gamma_2) = \emptyset.$$

Now we see that the difference sets of any two codewords with generators from Γ_1 are disjoint. Assume $\ell(i + jn_1) \equiv \ell'(i' + j'n_1) \pmod{n_1 n_2}$ for some $\ell, \ell' \in \pm[1 : k - 1]$ and two generators $i+jn_1$ and $i'+j'n_2$ from Γ_1, then we need to show that $i = i'$ and $j = j'$. By the above assumption, since $(\ell i - \ell' i') + (\ell j - \ell' j')n_1 \equiv 0 \pmod{n_1 n_2}$, we have $\ell i \equiv \ell' i' \pmod{n_1}$. By the definition of C_1, $\ell i \neq 0, \ell' i' \neq 0$ and $i = i'$ hold. Furthermore, since C_1 has no exceptional codewords, we also have $\ell = \ell'$ and $(\ell j - \ell j')n_1 \equiv 0 \pmod{n_1 n_2}$, i.e., $\ell(j - j') \equiv 0 \pmod{n_2}$. Then $(n_2, \ell) = 1$ implies $j = j'$. Similarly, the difference sets of any two codewords with generators from Γ_2 are disjoint, since $C_2 \in \mathrm{CAC}^{\mathrm{e}}(n_2, k)$. □

Corollary 6.2. *$\mathrm{M}(35, 4) = 6$, $\mathrm{M}(77, 4) = 12$, and $\mathrm{M}(91, 4) = 14$.*

Proof. For $n_1 = 7$ one has an equi-difference CAC with $\Gamma(C_1) = \{1\}$ consisting of one non-exceptional codeword x_1. For $n_2 = 5$, $\Gamma(C_2) = \{1\}$ defines an equi-difference CAC with an exceptional codeword. From Theorem 6.1, we obtain a code C for $n = 35$ with $|C| = 6$. Then Lemma 2.1 implies $\mathrm{M}(35, 4) = \mathrm{M}^{\mathrm{e}}(35, 4) = 6$.

Similarly, for $n_2 = 11$ and $\Gamma(C_2) = \{1\}$, one obtains an optimal code C for $n = 77$ with $|C| = 12$, and $\mathrm{M}(77, 4) = \mathrm{M}^{\mathrm{e}}(77, 4) = 12$.

For $n_2 = 13$, one easily sees that $\mathrm{M}(n_2, 4) = 1$. Using $\Gamma(C_2) = \{1\}$ one obtains code C for $n = 91$ with $|C| = 14$. Note that $\mathrm{M}(91, 4) \leq 15$ by Lemma 2.1. Suppose there is a code C' with $|C'| = 15$. Since there are no exceptional codewords for $n = 91$, C' must be an equi-difference code. Consider the set $A = \{\frac{\ell n}{7} : \ell \in [1 : 12]\} \simeq \mathbb{Z}_{13}^{\times}$. Now, for an equi-difference codeword x_i of C', the difference set $\Delta(x_i)$ intersects with A iff $i \in A$. In other words, A is covered by differences iff $\mathrm{M}^{\mathrm{e}}(13, 4) = 2$, whereas $\mathrm{M}^{\mathrm{e}}(13, 4) = 1$ by Table 7.2, contradiction. Hence it follows that $\mathrm{M}(91, 4) = 14 = |C|$. □

When p is an odd prime, 1 is a generator of an equi-difference code $C \in \mathrm{CAC}^{\mathrm{e}}(p, (p-1)/2)$. By applying Theorem 6.1 to C recursively, we obtain the following.

Corollary 6.3. *(Levenshtein [12]) Let p be an odd prime and r be a positive integer. Then there exists an optimal code $C \in \mathrm{CAC}^{\mathrm{e}}(n, k)$ with parameters $n = p^r$, $k = \frac{p+1}{2}$ and $|C| = \frac{n-1}{2(k-1)}$.*

Furthermore, some infinite serieses of optimal CACs are obtained.

Corollary 6.4. *Let $p_1, p_2, \ldots, p_r$ be primes such that $p_i \equiv 1 \pmod 6$ and assume that there exists an optimal code $C_i \in \mathrm{CAC}^{\mathrm{e}}(p_i, 4)$ satisfying the conditions of Corollary 3.3 for each $i \in [1 : r]$. Then there exists an optimal equi-difference code $C \in \mathrm{CAC}^{\mathrm{e}}(n = \prod_{i \in [1:r]} p_i, 4)$ with $|C| = \frac{n-1}{6}$.*

Proof. We have only to check the number of codewords for the code given by the recursive construction in Theorem 6.1. Each code C_i has $m_i = \frac{p_i - 1}{6}$ codewords, which attains the upper limit of Lemma 2.1. By applying the recursive construction to C_1 and C_2, we have an equi-difference code of length $p_1 p_2 = 6(6m_1 m_2 + m_1 + m_2) + 1$ with $6m_1 m_2 + m_1 + m_2$ codewords, which also attains the upper limit of Lemma 2.1. By continuing this process, we have the desired optimal code $C \in \mathrm{CAC}^{\mathrm{e}}(n = \prod_{i \in [1:r]} p_i, 4)$ with $|C| = \frac{n-1}{6}$. □

In the following corollaries, it is enough to check the case of $r = 2$ since the similar process can be applied recursively.

Corollary 6.5. *Let $p_1, p_2, \ldots, p_r$ be primes such that $p_i \equiv 7 \pmod 8$ and let C_i be an optimal code in $\mathrm{CAC}^{\mathrm{e}}(3p_i, 4)$ constructed in Corollary 3.8 for each $i \in [1 : r]$. Then there exists an optimal equi-difference code $C \in \mathrm{CAC}^{\mathrm{e}}(n = 3\prod_{i \in [1:r]} p_i, 4)$ with $|C| = \frac{n-3}{6}$.*

Proof. Each code C_i has $m_i = \frac{3p_i - 3}{6}$ codewords, which attains the upper limit of Lemma 2.1. The composed code of C_1 and C_2 is an equi-difference code of length

$3p_1p_2 = 3(2(2m_1m_2 + m_1 + m_2) + 1)$ with $2m_1m_2 + m_1 + m_2$ codewords, which also attains the upper limit of Lemma 2.1. □

COROLLARY 6.6. *Let $p_1, p_2, \ldots, p_r$ be primes such that $p_i \equiv 13 \pmod{24}$ and let C_i be an optimal code in $\mathrm{CAC^e}(4p_i, 4)$ constructed in Corollary 5.3 for each $i \in [1:r]$. Then there exists an optimal equi-difference code $C \in \mathrm{CAC^e}(n = 4\prod_{i\in[1:r]} p_i, 4)$ with $|C| = \frac{n+2}{6}$.*

Proof. Each code C_i has $m_i = \frac{4p_i+2}{6}$ codewords, which attains the upper limit of Lemma 2.1. Here, we can assume $m_i = 2\ell_i + 1$ for some $\ell \in \mathbb{N}$ since $p_i \equiv 1 \pmod 3$. Let C_1' be a code derived by deleting an exceptional codeword with generator p_1 from C_1. By composing C_1' and C_2, we have an equi-difference code of length $4p_1p_2 = 4(3(3\ell_1\ell_2 + \ell_1 + \ell_2) + 1)$ with $2(3\ell_1\ell_2 + \ell_1 + \ell_2) + 1$ codewords, which also attains the upper limit of Lemma 2.1. □

COROLLARY 6.7. *Let $p_1, p_2, \ldots, p_r$ be primes such that $p_i \equiv 5 \pmod{24}$ and let C_i be an optimal code in $\mathrm{CAC^e}(2p_i, 5)$ constructed in Corollary 3.10 for each $i \in [1:r]$. Then there exists an optimal equi-difference code $C \in \mathrm{CAC^e}(n = 2\prod_{i\in[1:r]} p_i, 5)$ with $|C| = \frac{n-2}{8}$.*

Proof. Each code C_i has $m_i = \frac{2p_i-2}{8}$ codewords, which attains the upper limit of Lemma 2.3. By composing C_1 and C_2, we have an equi-difference code of length $2p_1p_2 = 2(4(4m_1m_2 + m_1 + m_2) + 1)$ with $4m_1m_2 + m_1 + m_2$ codewords, which also attains the upper limit of Lemma 2.3. □

COROLLARY 6.8. *Let $p_1, p_2, \ldots, p_r$ be primes such that $p_i \equiv 11 \pmod{12}$ and let C_i be an optimal code in $\mathrm{CAC^e}(4p_i, 5)$ constructed in Corollary 3.11 for each $i \in [1:r]$. Then there exists an optimal equi-difference code $C \in \mathrm{CAC^e}(n = 4\prod_{i\in[1:r]} p_i, 5)$ with $|C| = \frac{n-4}{8}$.*

Proof. Each code C_i has $m_i = \frac{4p_i-4}{8}$ codewords, which attains the upper limit of Lemma 2.3. By composing C_1 and C_2, we have an equi-difference code of length $4p_1p_2 = 4(2(2m_1m_2 + m_1 + m_2) + 1)$ with $2m_1m_2 + m_1 + m_2$ codewords, which also attains the upper limit of Lemma 2.3. □

7. Tables. In this section, we give some tables for the existence of equi-difference CACs of small code length. Table 7.1 shows the first 110 primes satisfying the conditions of Corollary 3.3. Table 7.2 shows the maximal size $\mathrm{M^e}(n, 4)$ of an equi-difference CAC for each $n \in [4:100]$ and their corresponding generators.

REFERENCES

[1] Q, A. N., Györfi. L., Massey, J. L., *Constructions of binary constant weight cyclic codes and cyclically permutable codes*, IEEE Trans. Inform. Theory, 38 (1992), no. 3, pp. 940–949.

[2] Beth, T., Jungnickel, D., Lenz, H., *Design Theory*, Cambridge University Press, 1999.

[3] Buratti, M., *On simple radical difference families*, J. Combin. Designs, 3 (1995), pp. 161–168.

[4] ———, *Cyclic designs with block size 4 and related optimal optical orthogonal codes*, Des. Codes Cryptogr., 26 (2002), pp. 111–125.

[5] Colbourn, C. J., Dinitz, J. H.: Chen, K., Zhu, L., *The CRC Handbook of Combinatorial Designs*, CRC Press, 1996.

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

[7] Ireland, K., Rosen, M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1980.

[8] Jimbo, M., Mishima, M., Janiszewski, S., Teymorian, A. Y., Tonchev, V., *On conflict-avoiding codes of length $n = 4m$ for three active users*, IEEE Trans. Inform. Theory, submmited.

[9] Lam, C., Miao, Y., *$(C_k \oplus G, k, \lambda)$ difference families*, Des. Codes Cryptogr., 24 (2001), pp. 291–304.

[10] Levenshtein, V. I., Vinck, A. J. H., *Perfect (d,k)-codes capable of correcting single peak shifts*, IEEE Trans. Inform. Theory, 39 (1993), pp. 656–662.

[11] Levenshtein, V. I., *Conflict-avoiding codes for three active users and cyclic triple systems*, J. Combin. Theory, submitted.

[12] ———, *Conflict-avoiding codes for many active users*, Problems of Theoretic Cybernetics, Abstracts of 14th International Conference, Penza, Publishing House of Mech. Math. Department of Moscow State University, (2005), p. 86. (in Russian).

[13] Leopoldt, H. W., Roqutte, P., *Mathmatische Abhandlungen Band* 1, Walter de Gruyter, 1975.

[14] Massey, J. L., Mathys, P., *The collision channel without feedback*, IEEE Trans. Inform. Theory, 31 (1985), no. 2, pp. 192–204.

[15] Mathys, P., *A class of codes for a T active useres out of N multiple-access*, IEEE Trans. Inform. Theory, 36 (1990), no. 6, pp. 1206–1219.

[16] Ribenboim, P., *Classical theory of algebraic numbers*, Springer-Verlag, New York, 2001.

[17] Tsybakov, B. S., Rubinov, A. R., *Some constructions of conflict-avoiding codes*, Prob. Inf. Trans., 38 (2002), no. 4, pp. 268–279.

[18] Wilson, R. M., *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory, 4 (1972), pp. 17–47.

Fig. 4.1. *The connected component of $G(p) = (V, E)$ containing a vertex $a \in V$ is either $G_a^1(p) = (V_a^1, E_a^1)$ or $G_a^2(p) = (V_a^2, E_a^2)$.*

p	m	α	γ	c_1	c_2
7	1	3	6	-	28
37	6	2	8	-	-
139	23	2	8	-	556
163	27	2	8	-	652
181	30	2	8	724	-
241	40	7	102	-	-
313	52	10	61	-	-
337	56	10	326	-	-
349	58	2	8	-	-
379	63	2	8	-	1516
409	68	21	263	-	-
421	70	2	8	1684	-
541	90	2	8	2164	-
571	95	3	27	-	2284
607	101	3	27	-	2428
631	105	3	27	-	2524
751	125	3	27	-	3004
859	143	2	8	-	3436
877	146	2	8	-	-
937	156	5	125	-	-
1033	172	5	125	-	-
1087	181	3	27	-	4348
1123	187	2	8	-	4492
1171	195	2	8	-	-
1291	215	2	8	-	5164
1297	216	10	1000	-	-
1447	241	3	27	-	5788
1453	242	2	8	5812	-
1483	247	2	8	-	5932
1693	282	2	8	-	-
1741	290	2	8	-	-
1747	291	2	8	-	6988
2011	335	3	27	-	8044
2161	360	23	1362	-	-
2239	373	3	27	-	8956
2311	385	3	27	-	9244
2371	395	2	8	-	9484
2473	412	5	125	-	-
2539	423	2	8	-	10156
2647	441	3	27	-	10588
2677	446	2	8	10708	-
2707	451	2	8	-	10828
2719	453	3	27	-	10876
2857	476	11	1331	-	-
3169	528	7	343	-	-
3361	560	22	565	-	-
3433	572	5	125	-	-
3511	585	7	343	-	-
3547	591	2	8	-	14188
3559	593	3	27	-	14236
3571	595	2	8	-	14284
3613	602	2	8	-	-
3637	606	2	8	14548	-
3727	621	3	27	-	14908
3877	646	2	8	-	-
3919	653	3	27	-	15676
3931	655	2	8	-	15724
4003	667	2	8	-	16012
4021	670	2	8	16084	-
4111	685	12	1728	-	-
4201	700	11	1331	-	-
4219	703	2	8	-	16876
4261	710	2	8	-	-
4297	716	5	125	-	-
4357	726	2	8	-	-
4363	727	2	8	-	17452
4441	740	21	379	-	-
4507	751	2	8	-	18028
4561	760	11	1331	-	-
4603	767	2	8	-	18412
4801	800	7	343	-	-
4831	805	3	27	-	19324
4861	810	11	1331	19444	-
4903	817	3	27	-	19612
4987	831	2	8	-	19948
4999	833	3	27	-	19996
5023	837	3	27	-	20092
5107	851	2	8	-	-
5119	853	3	27	-	20476
5431	905	3	27	-	21724
5479	913	3	27	-	21916
5563	927	2	8	-	22252
5683	947	2	8	-	22732
5689	948	11	1331	-	-
5743	957	10	1000	-	-
5749	958	2	8	22996	-
5827	971	2	8	-	23308
5857	976	7	343	-	-
5869	978	2	8	23476	-
5881	980	316	386	-	-
5923	987	2	8	-	23692
6073	1012	10	1000	-	-
6343	1057	3	27	-	25372
6379	1063	2	8	-	25516
6397	1066	2	8	-	-
6469	1078	2	8	25876	-
6571	1095	3	27	-	26284
6577	1096	5	125	-	-
6733	1122	2	8	26932	-
6781	1130	2	8	27124	-
6823	1137	3	27	-	27292
6907	1151	2	8	-	27628
6949	1158	2	8	27796	-
7129	1188	7	343	-	-
7159	1193	3	27	-	28636
7237	1206	2	8	28948	-
7243	1207	2	8	-	28972
7759	1293	3	27	-	31036
7789	1298	2	8	-	-
7879	1313	3	27	-	31516

Table 7.1

The first 110 *primes* $p = 6m + 1$ *satisfying the conditions of Corollary 3.3.* $\alpha \in \mathrm{GF}(p)^\times$ *denotes a primitive element and* $\gamma = \alpha^3$. *The code* $C \in \mathrm{CAC}(n = p, 4)$ *defined by the list of generators* $(1, \gamma, \ldots, \gamma^{m-1})$ *is optimal. The column* c_1 *(or* c_2*) indicates the length* $n = 4p$ *if* p *satisfies the conditions of Corollary 5.3 (or Corollary 5.5, respectively).*

n	m	c	t	$\Gamma(C)$	n	m	c	t	$\Gamma(C)$
4	0	4	**1**	1	53	8	5	**7**	1, 6, 7, 8, 10, 19, 22
5	0	5	**1**	1	54	9	0	**7**	1, 4, 7, 9, 10, 13, 16
6	1	0	**1**	1	55	9	1	**7**	1, 4, 5, 7, 9, 11, 13
7	1	1	**1**	1	56	9	2	**8**	1, 4, 5, 7, 9, 11, 13, 25
8	1	2	**1**	1	57	9	3	**8**	1, 4, 5, 7, 11, 13, 16, 17
9	1	3	**1**	1	58	9	4	**8**	1, 4, 5, 9, 11, 13, 14, 17
10	1	4	**1**	1	59	9	5	**8**	1, 4, 10, 14, 18, 22, 24, 25
11	1	5	**1**	1	60	10	0	**7**	1, 4, 5, 7, 11, 17, 18
12	2	0	**1**	1	61	10	1	**8**	1, 5, 6, 7, 8, 11, 19, 26
13	2	1	**1**	1	62	10	2	**8**	1, 4, 7, 9, 10, 11, 13, 19
14	2	2	**1**	1	63	10	3	**8**	1, 4, 5, 7, 9, 11, 13, 19
15	2	3	**1**	1	64	10	4	**9**	1, 4, 5, 7, 9, 11, 13, 16, 29
16	2	4	**2**	1, 4	65	10	5	**8**	1, 4, 5, 7, 13, 16, 18, 28
17	2	5	**2**	1, 4	66	11	0	**9**	1, 4, 5, 7, 11, 13, 16, 19, 30
18	3	0	**2**	1, 4	67	11	1	**9**	1, 4, 5, 11, 14, 16, 18, 29, 30
19	3	1	**2**	1, 4	68	11	2	**10**	1, 4, 5, 7, 9, 11, 13, 16, 17, 31
20	3	2	**3**	1, 4, 5	69	11	3	**11**	1, 4, 5, 11, 13, 14, 16, 17, 20, 25, 31
21	3	3	**3**	1, 4, 5	70	11	4	**8**	1, 4, 5, 7, 9, 11, 13, 17
22	3	4	**2**	1, 4	71	11	5	**10**	1, 5, 6, 8, 13, 14, 17, 25, 30, 31
23	3	5	**2**	1, 4	72	12	0	**9**	1, 4, 5, 9, 11, 14, 16, 17, 26
24	4	0	**3**	1, 4, 5	73	12	1	**8**	1, 4, 5, 7, 9, 11, 13, 16
25	4	1	**3**	1, 4, 5	74	12	2	**9**	1, 4, 5, 7, 9, 11, 13, 19, 34
26	4	2	**3**	1, 4, 5	75	12	3	**10**	1, 4, 5, 7, 11, 13, 16, 17, 19, 23
27	4	3	**3**	1, 4, 7	76	12	4	**11**	1, 4, 5, 7, 9, 11, 13, 16, 17, 19, 35
28	4	4	**4**	1, 4, 5, 7	77	12	5	**12**	1, 6, 7, 8, 11, 13, 15, 20, 27, 29, 34, 36
29	4	5	**3**	1, 4, 5	78	13	0	**10**	1, 4, 5, 7, 11, 13, 16, 17, 18, 29
30	5	0	**4**	1, 4, 5, 7	79	13	1	**10**	1, 4, 5, 7, 11, 16, 17, 18, 20, 35
31	5	1	**3**	1, 4, 5	80	13	2	**12**	1, 4, 5, 7, 9, 11, 13, 16, 17, 19, 20, 37
32	5	2	**4**	1, 4, 5, 7	81	13	3	**10**	1, 4, 5, 7, 9, 11, 13, 17, 19, 25
33	5	3	**4**	1, 4, 5, 13	82	13	4	**10**	1, 4, 7, 9, 10, 11, 13, 16, 19, 29
34	5	4	**4**	1, 4, 5, 7	83	13	5	**11**	1, 4, 7, 15, 18, 20, 22, 24, 26, 32, 37
35	5	5	**6**	1, 5, 6, 7, 8, 13	84	14	0	**10**	1, 4, 5, 7, 11, 13, 16, 19, 20, 25
36	6	0	**5**	1, 4, 7, 9, 10	85	14	1	**13**	1, 4, 5, 14, 17, 18, 20, 22, 23, 24, 26, 32, 38
37	6	1	**6**	1, 6, 8, 10, 11, 14	86	14	2	**11**	1, 4, 7, 9, 13, 15, 22, 23, 25, 35, 38
38	6	2	**5**	1, 4, 5, 7, 9	87	14	3	**13**	1, 4, 5, 7, 11, 16, 17, 19, 20, 23, 26, 31, 37
39	6	3	**5**	1, 4, 5, 7, 11	88	14	4	**13**	1, 4, 7, 9, 11, 15, 16, 17, 23, 25, 31, 39, 41
40	6	4	**6**	1, 4, 5, 7, 9, 17	89	14	5	**12**	1, 4, 5, 9, 14, 20, 22, 24, 26, 32, 34, 35
41	6	5	**5**	1, 4, 10, 16, 18	90	15	0	**11**	1, 4, 5, 7, 9, 13, 16, 19, 20, 22, 28
42	7	0	**5**	1, 4, 5, 7, 11	91	15	1	**14**	1, 6, 7, 8, 13, 15, 20, 22, 27, 29, 34, 36, 41, 43
43	7	1	**6**	1, 5, 6, 7, 8, 13	92	15	2	**14**	1, 4, 7, 9, 11, 13, 15, 16, 19, 23, 25, 29, 41, 43
44	7	2	**7**	1, 4, 5, 7, 9, 11, 19	93	15	3	**15**	1, 4, 5, 7, 13, 16, 17, 19, 20, 22, 23, 25, 28, 29, 41
45	7	3	**6**	1, 4, 5, 7, 9, 13	94	15	4	**12**	1, 4, 5, 9, 13, 16, 17, 19, 21, 22, 29, 35
46	7	4	**6**	1, 4, 5, 7, 9, 11	95	15	5	**13**	1, 5, 6, 7, 8, 19, 20, 23, 33, 39, 41, 42, 43
47	7	5	**6**	1, 4, 11, 19, 20, 21	96	16	0	**11**	1, 4, 5, 7, 11, 13, 16, 17, 18, 23, 29
48	8	0	**6**	1, 5, 6, 7, 8, 13	97	16	1	**12**	1, 4, 5, 7, 9, 16, 17, 20, 22, 26, 28, 36
49	8	1	**8**	1, 6, 7, 8, 13, 15, 20, 22	98	16	2	**13**	1, 4, 7, 9, 15, 17, 19, 22, 25, 26, 29, 31, 37
50	8	2	**7**	1, 4, 5, 7, 9, 13, 22	99	16	3	**12**	1, 4, 5, 7, 9, 11, 13, 16, 19, 23, 25, 31
51	8	3	**6**	1, 4, 5, 7, 9, 19	100	16	4	**14**	1, 4, 5, 7, 9, 11, 13, 16, 17, 19, 20, 23, 25, 47
52	8	4	**8**	1, 4, 5, 7, 9, 11, 13, 23					

Table 7.2

This table shows for each $n \in [4:100]$ with $n = 6m + c$, $m = \lfloor n/6 \rfloor$, $c \in [0:5]$, the maximal size $t = \mathrm{M}^{\mathrm{e}}(n,4)$ of an equi-difference CAC. $\Gamma(C)$ is the set of generators of such a maximal equi-difference code C (the lexicographical smallest with respect to the generators).