Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9764-5

Optimal conflict-avoiding codes of odd length and weight three

Hung-Lin Fu · Yuan-Hsun Lo · Kenneth W. Shum

Received: 12 February 2012 / Revised: 16 October 2012 / Accepted: 20 October 2012

Abstract A conflict-avoiding code (CAC) $\mathcal{C}$ of length n and weight k is a collection of k-subsets of $\mathbb{Z}_n$ such that $\Delta(x) \cap \Delta(y) = \emptyset$ for any $x, y \in \mathcal{C}, x \neq y$, where $\Delta(x) = \{a - b : a, b \in x, a \neq b\}$. Let CAC$(n, k)$ denote the class of all CACs of length n and weight k. A CAC with maximum size is called optimal. In this paper, we study the constructions of optimal CACs for the case when n is odd and $k = 3$.

Keywords Conflict-avoiding code · Tight equi-difference conflict-avoiding code · Optimal code with weight 3

Mathematics Subject Classification (2000) 94B25 · 94C15 · 11A15

1 Introduction

Protocol sequences for a multiple-access channel without feedback have been investigated in [3,8,9,12,13,19]. In such model, the time axis is partitioned into intervals (slots) whose duration corresponds to the transmission time for one packet. All users are supposed to have slot synchronization and no other synchronization is assumed. If exactly one user is sending a packet in a particular slot, then the packet is transmitted successfully. If more than one users

Communicated by V. D. Tonchev.

H.-L. Fu · Y.-H. Lo (✉)
Department of Applied Mathematics, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu 30010, Taiwan
e-mail: yhlo0830@gmail.com

H.-L. Fu
e-mail: hlfu@math.nctu.edu.tw

K. W. Shum
Institute of Network Coding, The Chinese University of Hong Kong, Shatin, Hong Kong
e-mail: wkshum@inc.cuhk.edu.hk

Published online: 07 November 2012

are sending packets in a particular slot simultaneously, then there is a *conflict* in this slot and none of the packets has successful transmission.

Let $x_i = (x_{i,0}, x_{i,1}, \ldots, x_{i,n-1})$ be a *binary protocol sequence* with length n over the set $\{0, 1\}$ and W is a set of this kind of binary protocol sequences. There is a one-to-one correspondence between all M users (potential users) and W, and each user is provided by an infinite binary sequence which periodically repeats the corresponding protocol sequence. Suppose that one user receives the sequence x_i and becomes active at time T after a duration of being inactive. The user sends or does not send a data packet in slot $T + j - 1$ if $x_{i,j} = 1$ or $x_{i,j} = 0$, respectively. Packets are transmitted continuously by repeating x_i until the user becomes inactive. We assume that the user will stay in the inactive state for at least n time slots before he becomes active again. The set $W = \{x_1, x_2, \ldots, x_M\}$ of M binary sequences is said to be an $(M, k, \omega, n, \sigma)$ *protocol sequence set* if any sequence is of length n, Hamming weight k, and has the property that at least σ packets are transmitted successfully in a frame of n slots for each active user, if at most ω users out of M potential users are active. On the assumption that the number of conflicts of any two distinct sequences is at most λ, the weight k of the $(M, k, \omega, n, \sigma)$ protocol sequence set satisfies $k \geq \lambda(\omega - 1) + \sigma$ in order to guarantee that at least σ packets survive for each user in a frame. Such an $(M, k, \omega, n, \sigma)$ protocol sequence set is also called a *conflict-avoiding code* (CAC) of length n with weight k. In this paper, we consider the case when $\lambda = \sigma = 1$, $\omega = 3$, and $k = 3$.

Let $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ denote the ring of residues modulo n and $\mathcal{P}(n, k)$ denote the set of all k-subsets of $\mathbb{Z}_n$. Each element $x \in \mathcal{P}(n, k)$ can be identified with a binary sequence of length n and weight k representing the indices of the nonzero positions. Given a k-subset $x \in \mathcal{P}(n, k)$, we define the *difference set* of x by $\Delta(x) = \{a - b \pmod n : a, b \in x, a \neq b\}$. Note that $|\Delta(x)| \leq k(k - 1)$; furthermore, $i \in \Delta(x)$ implies $(n - i) \in \Delta(x)$, i.e., $\Delta(x)$ is symmetric with respect to $n/2$. On the assumption that $\lambda = 1$, a CAC of length n with weight k is a subset $\mathcal{C} \subset \mathcal{P}(n, k)$ satisfying the condition that $\Delta(x) \cap \Delta(y) = \phi$ for any $x, y \in \mathcal{C}$ with $x \neq y$. Each element $x \in \mathcal{C}$ is called a *codeword* of length n with weight k. Without loss of generality, we can assume that all codewords contain 0. For instance, $\mathcal{C} = \{\{0, 1, 2\}, \{0, 4, 8\}\}$ is a CAC of length 11 and weight 3, and the two codewords are correspondent to the two binary protocol sequences $(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$ and $(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$, respectively. For given n and k, let $\mathrm{CAC}(n, k)$ denote the class of all CACs of length n with weight k. The maximum size of some code in $\mathrm{CAC}(n, k)$ will be denoted by $M(n, k)$. A code $\mathcal{C} \in \mathrm{CAC}(n, k)$ is said to be *optimal* if $|\mathcal{C}| = M(n, k)$. The above example is optimal in $\mathrm{CAC}(11,3)$, i.e., $M(11, 3) = 2$.

A codeword $x \in \mathcal{P}(n, k)$ is said to be *equi-difference* with *generator* $i \in \mathbb{Z}_n \setminus \{0\}$, if x is of form $\{0, i, 2i, \ldots, (k - 1)i\}$. Note here that $|\Delta(x)| \leq 2(k - 1)$ if x is an equi-difference codeword. A code $\mathcal{C} \in \mathrm{CAC}(n, k)$ is called *equi-difference* if it entirely consists of equi-difference codewords. Let $\mathrm{CAC}^e(n, k)$ denote the class of all the equi-difference codes in $\mathrm{CAC}(n, k)$ and $M^e(n, k)$ be the maximum size among $\mathrm{CAC}^e(n, k)$. Furthermore, an optimal code $\mathcal{C} \in \mathrm{CAC}(n, k)$ is said to be *tight* if $\bigcup_{x \in \mathcal{C}} \Delta(x) = \mathbb{Z}_n \setminus \{0\}$.

In the case of general weight k, Shum et al. [16] showed that for fixed k, the number $M(n, k)$ increases approximately with slope $(2k - 2)^{-1}$ as a function of length n. Moreover, Shum and Wong [17] presented an asymptotic version of upper bound $M(n, k)$ for all fixed k, with length n approaching infinity. Some optimal constructions for $k = 4, 5$ can be found in [11]. In the case of weight $k = 3$, Levenshtein and Tonchev [9] proposed a construction of optimal CACs for each length $n \equiv 2 \pmod 4$. Later, Jimbo et al. [5] and Mishima et al. [10] extended the result to each length $n \equiv 8 \pmod{16}$ and $n \equiv 0 \pmod{16}$, respectively. Recently, Fu et al. [2] completely settled the spectrum of the size of optimal CACs of even length and

weight 3. For odd length, Levenshtein and Tonchev [9] showed some optimal CACs for some particular prime length, and Levenshtein [8] extended the result to some particular odd length. However, the number $M(n, 3)$ for general odd integer n is still unknown except when n is small or $n = 2^m \pm 1$ [20]. If only equi-difference codewords are considered, Momihara [14] presented a necessary and sufficient conditions for the existence of tight equi-difference CACs. In addition, it is worthy pointing out that an equi-difference code $\mathcal{C} \in \mathrm{CAC}^e(n, 3)$ is related to an n-ary code that can correct errors with limited magnitude, see [6,7].

In what follows, we consider the case where n is odd and $k = 3$. Given a code $\mathcal{C} \in \mathrm{CAC}(n, 3)$ and a codeword $x \in \mathcal{C}$. It is easily checked that $2 \leq |\Delta(x)| \leq 6$. Furthermore, we have the following property

$$|\Delta(x)| = \begin{cases} 2 & \text{if } x \text{ is equi-difference with generator } \frac{n}{3}, \\ 4 & \text{if } x \text{ is equi-difference with generator } i \neq \frac{n}{3}, \\ 6 & \text{otherwise.} \end{cases} \tag{1}$$

For convenience, CAC(n,3) and $M(n, 3)$ are simply written as CAC(n) and $M(n)$, respectively. Similarly, we use $\mathrm{CAC}^e(n)$ and $M^e(n)$ to denote $\mathrm{CAC}^e(n, 3)$ and $M^e(n, 3)$, respectively. The maximal sizes of conflict-avoiding code of odd length n and weight 3 is the sequence A135304 in [15].

Let $n \geq 3$ be an odd integer and $G(n)$ be a graph with vertex set $V(G(n)) = \{1, 2, \ldots, \frac{n-1}{2}\}$ and edge set $E(G(n))$, where $(a, b) \in E(G)$ if $b \equiv \pm 2a \pmod{n}$. Then the graph $G(n)$ is a union of disjoint cycles. Let $O(n)$ be the number of odd cycles in $G(n)$. A loop in $G(n)$ is considered as a cycle of length 1. For example, (7), (3, 6, 9), (1, 2, 4, 8, 5, 10) are the three cycles in $G(21)$, and $O(21) = 2$. The concept $G(n)$ can be seen in [5,8,9,14]. For convenience, we let $O(1) = 0$.

$G(n)$ is useful in finding the number $M^e(n)$. For each vertex $i \in V(G(n))$, it can be identified as the representation of the differences i and $n - i$. Therefore, an edge (a, b) represents the equi-difference codeword $\{0, a, 2a\}$ and a loop in G corresponds to the equi-difference codeword $\{0, n/3, 2n/3\}$, which occurs only when $3|n$. Moreover, if three vertices a, b, c satisfying the equation $a + b \equiv \pm c \pmod{n}$, then the set $\{a, b, c\}$ corresponds to a codeword $\{0, a, a + b\}$. Recall that the restriction $\Delta(x) \cap \Delta(y) = \phi$ for any two codewords $x \neq y$. In order to find as many codewords as possible, we shall optimize the number of disjoint vertex subsets such that each subset, say S, is one of the following three cases: (1) $|S| = 1$ and the induced subgraph is a loop, (2) $|S| = 2$ and the induced subgraph is an edge, or (3) $S = \{a, b, c\}$ and $a + b \equiv \pm c \pmod{n}$. Note here that there is at most one loop in $G(n)$, for all odd n. Our strategy is first to find the maximum matching (besides loop) and then for the unused differences we construct as many triples $\{a, b, c\}$ satisfying $a + b \equiv \pm c \pmod{n}$ as possible. Now we are going to find as many equi-difference codewords as possible, and it is not hard to observe the following result.

Proposition 1 *Given an odd integer $n \geq 3$, there exists a tight equi-difference code $\mathcal{C} \in \mathrm{CAC}^e(n)$ if and only if $O(n) = 0$ and $3 \nmid n$, or $O(n) = 1$ and $3|n$.*

2 Tight equi-difference codes

In 2007, Momihara [14] gave necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight 3. In this section, we rewrite the necessary and sufficient conditions by using a different approach. We first introduce several number-theoretic functions.

For positive integer n, let $\Phi(n)$ be the collection of elements in $\mathbb{Z}_n$ that are relatively prime to n, and let the size of it be $\varphi(n)$. For an odd integer $n \geq 3$, let e_n be the smallest exponent $e \geq 1$ so that $2^e \equiv 1 \pmod{n}$, and let c_n be the smallest exponent $c \geq 1$ so that $2^c \equiv \pm 1 \pmod{n}$. The exponent e_n is called the *multiplicative order* of 2 mod n, and the exponent c_n the *multiplicative suborder* of 2 mod n. If $e_n = \varphi(n)$, then 2 is said to be a *primitive root* mod n. By convention, we define $e_1 = 0$ and $c_1 = 0$.

By Euler's Theorem, which states that $a^{\varphi(n)} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$, we have e_n divides $\varphi(n)$. We will show later that c_n divides $\varphi(n)/2$ for all odd $n \geq 3$. The integer sequences (e_n) and (c_n), with the index n running over all odd integers are, respectively, the sequences A002326 and A003558 in [15].

The relation between c_n and e_n is as follows. First of all, it is obvious that $c_n \leq e_n$. If c_n is strictly less than e_n, then we must have $c_n = e_n/2$. Indeed, if $c_n < e_n/2$, we have $2^{2c_n} \equiv 1 \pmod{n}$, contradicting the minimality of e_n; if $e_n/2 < c_n < e_n$, then $2^{2c_n} \equiv 2^{2c_n - e_n} \equiv 1 \pmod{n}$, contradicting the minimality of e_n again. Hence, if e_n is odd, then $c_n = e_n$ is also odd. If e_n is even, then c_n is equal to either e_n or $e_n/2$. Furthermore, if e_n is even and n is prime, then $n|(2^{e_n/2} - 1)(2^{e_n/2} + 1)$, and this implies $n|(2^{e_n/2} + 1)$ and thus $c_n = e_n/2$ (See e.g. [8, Corollary 6]).

In $G(n)$, the *standard cycle*, denoted as $\langle 2 \rangle_n$, is the cycle which contains 1. For instance, $(1, 2, 4, 8, 3, 6, 7, 5, 9)$ is the standard cycle in $G(19)$. For any n, $|\langle 2 \rangle_n| = c_n$.

Given a cycle $C = (s_1, s_2, \ldots, s_t)$ in $G(n)$ and an integer a, the *modulo product* of C by a, written aC, is the cycle $(a \cdot s_1, a \cdot s_2, \ldots, a \cdot s_t) \pmod{n}$ in $G(n)$ where each item takes symmetry with respect to $n/2$. The *normal product* of C by an odd integer a, written $a \times C$, is the cycle $(a \cdot s_1, a \cdot s_2, \ldots, a \cdot s_t)$ in $G(an)$. Two cycles are said to be *congruent*, denoted as $\cong$, if they have the same length and one of them is a modulo or normal product of the other one. It is easy to see that $C \cong a \times C$. Besides, it is not difficult to see that every cycle in $G(n)$ can be written as $a\langle 2 \rangle_n$ for some integer $1 \leq a < n$.

Example 1 $\langle 2 \rangle_{31} = (1, 2, 4, 8, 15)$, $3\langle 2 \rangle_{31} = (3, 6, 12, 7, 14)$, $5\langle 2 \rangle_{31} = (5, 10, 11, 9, 13)$ and the three cycles are congruent to each other. However, $\langle 2 \rangle_{21} = (1, 2, 4, 8, 5, 10) \ncong (3, 6, 9) = 3\langle 2 \rangle_{21}$.

Example 2 $5 \times \langle 2 \rangle_{21} = (5, 10, 20, 40, 25, 50)$ is a cycle in $G(105)$. Actually, each cycle in $G(n)$ is congruent to exactly one cycle in $G(an)$ by the normal product by a, $\forall$ odd $a \in \mathbb{N}$. Therefore, $O(an) \geq O(n)$ for all odd integers a and n.

Lemma 1 *Let $C = a\langle 2 \rangle_n$ be a cycle in $G(n)$ where a is an integer in C. If $gcd(a, n) = d$, then $C \cong \langle 2 \rangle_{\frac{n}{d}}$. In particular, we have $|a\langle 2 \rangle_n| = |\langle 2 \rangle_{\frac{n}{d}}| = c_{\frac{n}{d}}$.*

Proof Let $a = a'd$ and $n = n'd$, then $C = a\langle 2 \rangle_n \cong a'\langle 2 \rangle_{n'}$ by the definition of normal product. Let $s = |a'\langle 2 \rangle_{n'}|$, then s is the minimum positive integer such that $a' \cdot 2^s \equiv \pm a' \pmod{n'}$, i.e., $2^s \equiv \pm 1 \pmod{n'}$ since $\gcd(a', n') = 1$. Hence,

$$|a'\langle 2 \rangle_{n'}| = s = |\langle 2 \rangle_{n'}| = c_{n'},$$

and thus $C \cong a'\langle 2 \rangle_{n'} \cong \langle 2 \rangle_{n'}$. □

From Lemma 1, we can deduce immediately the following.

Lemma 2 *Let $n \geq 3$ be an odd integer.*

(i) The length of any cycle in $G(n)$ divides that of the standard cycle.
(ii) For any divisor d of n, $c_d | \frac{\varphi(d)}{2}$ holds.

(iii) The number of cycles in $G(n)$ including a loop is $\sum_{d|n,d\neq 1}\varphi(d)/(2c_d)$.

Proof (i) Is obvious. (ii) For a proper divisor d of n, let

$$A = \{a \in V(G(n)) : \gcd(a, n) = n/d\}.$$

Then the induced subgraph by A are partitioned into cycles of length c_d, i.e., $|A|$ is divisible by c_d. Note that the set A can be written as $\{a : \gcd(a \cdot \frac{d}{n}, d) = 1, 1 \leq a \leq \frac{n-1}{2}\}$. By a change of variable $a' = a \cdot \frac{d}{n}$, we see that the size of A is equal to the size of $\{a' : \gcd(a', d) = 1, 1 \leq a' \leq \frac{d-1}{2}\}$. Hence $|A| = \varphi(d)/2$. This proves (ii). (iii) can be proved directly from (ii). □

There is a strong correlation between the size $M(n)$ of the optimal CAC of length n and weight 3 and the number $O(n)$ of odd cycles in $G(n)$. We provide a formula of $O(n)$ in the following theorem. For odd integer d, we define

$$\delta_d = \begin{cases} 0 & \text{if } d = 1 \text{ or if } d > 1 \text{ and } c_d \text{ is even;} \\ \frac{\varphi(d)}{2c_d} & \text{if } d > 1 \text{ and } c_d \text{ is odd.} \end{cases}$$

Theorem 1 *For odd $n \geq 3$, we have*

$$O(n) = \sum_{d|n} \delta_d,$$

and δ_d can be expressed in terms of e_d and $\varphi(d)$ by

$$\delta_d = \begin{cases} \dfrac{\varphi(d)}{2e_d} & \text{if } e_d \text{ is odd;} \\ \dfrac{\varphi(d)}{e_d} & \text{if } e_d \equiv 2 \pmod 4 \text{ and } c_d = \frac{e_d}{2}; \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Proof Let $A = \{a \in V(G(n)) : \gcd(a, n) = 1\}$ and $B = V(G(n)) \setminus A$. Then, as in the proof of Lemma 2, $|A| = \frac{\varphi(n)}{2}$. Moreover, the induced subgraph by A in $G(n)$ is a union of $\varphi(n)/(2c_n)$ disjoint cycles of length c_n. These cycles are all odd cycles if c_n is odd, and are all even cycles if c_n is even. The number of odd cycles in the subgraph induced by A is thus equal to δ_n.

Note here that c_n is either e_n or $\frac{e_n}{2}$. If e_n is odd, then $c_n = e_n$ and the number of odd cycles in the induced subgraph by A is $\frac{\varphi(n)}{2e_n}$. If $e_n \equiv 2 \pmod 4$ and $c_n = \frac{e_n}{2}$, then c_n is odd and there are $\frac{\varphi(n)}{e_n}$ odd cycles induced by A. If $e_n \equiv 2 \pmod 4$ and $c_n = e_n$ or $4|e_n$, then c_n is always even and hence the lengths of the cycles in the subgraph induced by A are all even.

Next, let us focus on the cycles in the induced subgraph by B. Each cycle in the induced subgraph by B is of the form $d\langle 2\rangle_n$ for some proper divisor d of n. By Lemma 1, $d\langle 2\rangle_n \cong \langle 2\rangle_{\frac{n}{d}}$. Then $d\langle 2\rangle_n$ is counted in $\delta_{\frac{n}{d}}$ exactly once if it is an odd cycle. This concludes the proof. □

We can compute $O(n)$ from e_d and c_d, where d runs over all factors of n. However, there is no effective method to determine the number e_n so far.

In what follows, we consider the case when n is an odd prime p. In number theory, the law of quadratic reciprocity is a theorem about modular arithmetic which gives conditions for the solvability of quadratic equations modulo prime numbers. Here we use the second supplement to quadratic reciprocity and Euler's Criterion, see [18], to obtain the following theorem.

Theorem 2 [18] *Let p be an odd prime. Then*

$$2^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv 1 \text{ or } 7 \pmod 8; \text{ and} \\ -1 \pmod{p} & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases} \tag{3}$$

For odd prime p, Theorem 1 can be formulated as

Theorem 3 *If p is an odd prime, then*

$$O(p) = \begin{cases} \frac{p-1}{2e_p} & \text{if } p \equiv 7 \pmod 8, \text{ or } p \equiv 1 \pmod 8 \text{ and } e_p \text{ is odd;} \\ \frac{p-1}{e_p} & \text{if } p \equiv 3 \pmod 8, \text{ or } p \equiv 1 \pmod 8 \text{ and } e_p \equiv 2 \pmod 4; \\ 0 & \text{if } p \equiv 5 \pmod 8, \text{ or } p \equiv 1 \pmod 8 \text{ and } 4|e_p. \end{cases} \tag{4}$$

Proof By definition, $O(p) = \delta_p$ for any odd prime p, and $\delta_p = 0$ (respectively, $\delta_p = \frac{p-1}{2c_d}$) if c_p is even (respectively, c_p is odd). Recall that for prime p, c_p is equal to either e_p if e_p is odd, or $e_p/2$ if e_p is even. We divide the proof into the following four cases.

Case 1: $p \equiv 1 \pmod 8$. c_p is even if and only if $e_p/2$ is even, i.e., $4|e_p$. In this case, we have $\delta_p = 0$.

Case 2: $p \equiv 3 \pmod 8$. We have $c_p = e_p/2$, because if $c_p = e_p$, then for all integer a, 2^a cannot be congruent to -1 mod p, but this contradicts Theorem 2. Moreover, $c_p = e_p/2$ must be odd in this case, because e_p is a divisor of $p-1$, which is divisible by 2 but not by 4.

Case 3: $p \equiv 5 \pmod 8$. We have $p - 1 = 8t + 4$ for some integer t in this case, and want to show that e_p is divisible by 4. If 2 is a primitive root mod p, then $e_p = p - 1$ is an integral multiple of 4. If 2 is not a primitive root mod p, then e_p is a proper divisor of $8t + 4$. Suppose on the contrary that e_p is not divisible by 4. Then e_p is a divisor of $4t + 2 = (p-1)/2$, and we can write $(p-1)/2 = ae_p$ for some integer a. This implies that $2^{(p-1)/2} \equiv (2^{e_p})^a \equiv 1 \pmod p$, contradicting Theorem 2. Therefore, we get $4|e_p$, and thus $\delta_p = 0$ by Theorem 1.

Case 4: $p \equiv 7 \pmod 8$. By Theorem 2, we see that e_p is a divisor of $(p-1)/2$, which is an odd integer. Therefore $c_p = e_p$ is odd in this case. □

We are ready to rewrite the result in [14].

Theorem 4 *Let $n = \prod_{i=1}^{m} p_i^{r_i}$ be an odd integer, where $p_1 < p_2 < \ldots < p_m$ are distinct prime factors and $r_i \in \mathbb{N}$. There exists a tight code $\mathcal{C} \in \mathrm{CAC}^e(n)$ if and only if one of the following holds:*

(a) *$p_1 > 3$ and each p_i satisfies the third condition in Theorem 3; or*

(b) *$p_1 = 3, r_1 = 1$, and for $i \geq 2$, p_i satisfies the third condition in Theorem 3.*

Proof By Proposition 1, there exists a tight code if and only if (i) $O(n) = 0$ and $3 \nmid n$ or (ii) $O(n) = 1$ and $3|n$. In the following we claim that condition (i) and (ii) are equivalent to (a) and (b), respectively.

By Lemma 1, the cycle $\langle 2 \rangle_{p_i}$ is congruent to $\frac{n}{p_i}\langle 2 \rangle_n$ for every prime factor p_i. If $O(n) = 0$, then the length of $\frac{n}{p_i}\langle 2 \rangle_n$ is even. Hence $O(p_i) = 0$. If $O(n) = 1$ and $3|n$, then the length of $\frac{n}{p_i}\langle 2 \rangle_n$ is even except when $p_i = 3$ (since $(\frac{n}{3})$ is a cycle in $G(n)$). Therefore, p_1 must be 3

and $O(p_i) = 0$ for all other prime factors. It remains to prove $r_1 = 1$. Suppose $r_1 \geq 2$. Since $\frac{n}{3}\langle 2\rangle_n$ and $\frac{n}{9}\langle 2\rangle_n$ are congruent to $\langle 2\rangle_3$ and $\langle 2\rangle_9$, respectively, this contradicts the assumption $O(n) = 1$.

Conversely, $O(p_i) = 0$ implies that c_{p_i} is even. Consider the case when $O(p_i) = 0$ for all $1 \leq i \leq m$. Let k be a factor of n. Assume k is a multiple of some prime factor p_t of n. Since $2^{e_k} \equiv 1 \pmod{k}$ implies $2^{e_k} \equiv 1 \pmod{p_t}$, we have $e_{p_t} | e_k$. Suppose c_k is odd. By Lemma 1, $\frac{k}{p_t}\langle 2\rangle_k \cong \langle 2\rangle_{p_t}$. This implies c_{p_t} is odd, which contradicts to $O(p_t) = 0$. Thus we have c_k is even for any proper factor k of n. In addition, each cycle in $G(n)$ can be written as the form $a\langle 2\rangle_n$, where a is an integer in its cycle. Because $a\langle 2\rangle_n$ is congruent to $\langle 2\rangle_{\frac{n}{d}}$ where $d = \gcd(a, n)$, the length of $a\langle 2\rangle_n$ is even. Hence, $O(n) = 0$. Now, consider the case when $p_1 = 3, r_1 = 1$, and $O(p_i) = 0$ for all $i \geq 2$. Similar to above argument, the length of $a\langle 2\rangle_n$ is even except when $a = \frac{n}{3}$. Thus, $O(n) = 1$ □

3 Optimal conflict-avoiding codes

In this section we consider optimal CAC which may include non-equi-difference codewords. To this end, we extend the graph $G(n)$ to a hypergraph $H(n)$. Recall that $\mathcal{P}(n, k)$ is the set of all k-subsets of $\mathbb{Z}_n$. For odd integer n, we define $H(n)$ as the hypergraph with vertex set $V(H(n)) = \{1, 2, \ldots, (n-1)/2\}$, and edge set

$$E(H(n)) := \{\Delta(x) \cap V(H(n)) : x \in \mathcal{P}(n, 3)\}.$$

Since the size of $\Delta(x)$ is restricted to 2, 4 or 6, the hyperedges in $H(n)$ has size 1, 2 or 3. An equi-difference codeword $\{0, a, 2a\}$ corresponds to hyperedge of size 1 or 2, which are precisely the loop or edges in the graph $G(n)$. For non-equi-difference codeword $\{0, a, b\}$, the corresponding hyperedge in $H(n)$ has size 3. Note that the graph $G(n)$ is a subgraph of hypergraph $H(n)$. In graph-theoretic terminology, a CAC of length n and weight 3 is precisely a collection of mutually disjoint hyperedges in $H(n)$, namely a *hypergraph matching*. A matching in $H(n)$ containing the largest possible number of hyperedges is called optimal. The number of hyperedges in an optimal matching in $H(n)$ is called the *matching number* of $H(n)$, and is equal to $M(n)$.

In order to find an optimal conflict-avoiding code, it is better off finding as many equi-difference codewords as possible. This is due to the fact that an equi-difference codeword costs the least differences in $G(n)$. The following bound of $M(n)$ is true for any odd integer $n \geq 3$.

Lemma 3 *Let $n \geq 3$ be an odd integer. Then*

$$\frac{1}{2}\left(\frac{n-1}{2} - O(n)\right) + \xi_n \leq M(n) \leq \frac{1}{2}\left(\frac{n-1}{2} - O(n)\right) + \xi_n + \left\lfloor \frac{O(n) - \xi_n}{3} \right\rfloor,$$

where $\xi_n = 1$ or 0 depending on if $3|n$ or not.

Proof In $G(n)$, the size of maximum matching is $\frac{1}{2}\left(\frac{n-1}{2} - O(n)\right) + \xi_n$. Since $G(n)$ is a subgraph of $H(n)$, then the lower bound is derived. This lower bound is the maximal number of equi-difference codewords of length n.

For the upper bound, we let $\mathcal{C}$ be an optimal CAC of length n. Let x_1, x_2 and x_3 be the number of hyperedges of 1, 2, and 3 in the corresponding hypergraph matching in $H(n)$ respectively. The value of x_1 is equal to 0 when n is not a multiple of 3.

Suppose that n is a multiple of 3. Let $j = n/3$. We want to show that there is an optimal matching of $H(n)$ which contains the hyperedge $\{j\}$ of size 1. Let $\mathcal{M}$ be a maximal

matching of $H(n)$. If the vertex j is not covered by any hyperedge in $\mathcal{M}$, then we can add the hyperedge $\{j\}$ to $\mathcal{M}$ and increase the number of hyperedges in the matching by one, contradicting the assumption that $\mathcal{M}$ is optimal. If the vertex j is covered by some other hyperedge in $\mathcal{M}$ already, we can remove this hyperedge from $\mathcal{M}$ and replace it by $\{j\}$. The resulting collection of hyperedges is a matching with the same number of hyperedges as in $\mathcal{M}$, and is hence optimal. Hence, we assume without loss of generality that $x_1 = 1$ if $3|n$, and $x_1 = 0$ otherwise.

Since the hyperedges in a matching must be disjoint, we have $x_1 + 2x_2 + 3x_3 \leq (n-1)/2$. As there are $O(n)$ odd cycles, we get

$$x_2 \leq \left(\frac{n-1}{2} - O(n)\right)/2. \tag{5}$$

We consider two cases. Firstly, suppose that n is not divisible by 3. Then $x_1 = 0$, and by adding (5) to $2x_2 + 3x_3 \leq (n-1)/2$, we get

$$3x_2 + 3x_3 \leq \frac{3}{2} \cdot \frac{n-1}{2} - \frac{O(n)}{2} \leq \frac{3}{2}\left(\frac{n-1}{2} - O(n)\right) + O(n).$$

Using the fact that $\frac{n-1}{2} - O(n)$ is even, we get

$$|\mathcal{C}| \leq x_2 + x_3 \leq \frac{1}{2}\left(\frac{n-1}{2} - O(n)\right) + \lfloor O(n)/3 \rfloor.$$

The second case $3|n$ can be treated similarly, and is omitted. □

Example 3 For length $n = 31$, the hyperedges corresponding to the following seven codewords

$$\{0, 2, 5\}, \{0, 4, 8\}, \{0, 6, 12\}, \{0, 7, 14\}, \{0, 9, 18\}, \{0, 10, 20\}, \{0, 15, 30\}$$

are illustrated in Fig. 1. The codeword $\{0, 2, 5\}$ is not equi-difference. It corresponds to the hyperedge $\{2, 3, 5\}$ of size 3. There are many other hyperedges of size 3 in $H(31)$, but they are not shown in Fig. 1. The remaining six codewords are equi-difference. This CAC is optimal, because it attains the upper bound

$$\frac{1}{2}\left(\frac{n-1}{2} - O(n)\right) + \xi_n + \left\lfloor \frac{O(n) - \xi_n}{3} \right\rfloor = \frac{1}{2}\left(\frac{31-1}{2} - 3\right) + \left\lfloor \frac{3}{3} \right\rfloor = 7$$

in Lemma 3.

Let $\mathbb{Z}_{odd}$ be the set of odd integers larger than or equal to 1. In order to state the second result in this section, we identify two special subsets of $\mathbb{Z}_{odd}$.

$$A = \{n \in \mathbb{Z}_{odd} : c_n \text{ is odd and } 2^{c_n} \equiv 1 \bmod n\},$$
$$B = \{n \in \mathbb{Z}_{odd} : c_n \text{ is odd and } 2^{c_n} \equiv -1 \bmod n\}.$$

The set $\mathbb{Z}_{odd} \setminus (A \cup B)$ consists of all odd integers n with c_n even. In particular, Theorem 3 expresses that a prime is in A if it satisfies the first condition in Theorem 3, in B if it satisfies the second condition, and in $\mathbb{Z}_{odd} \setminus (A \cup B)$ if it satisfies the third condition.

Example 4 Running over all odd integers from 3 to 99, we have

$$\{7, 23, 31, 47, 49, 71, 73, 79, 89\} \subset A, \text{ and}$$
$$\{3, 9, 11, 19, 27, 33, 43, 57, 59, 67, 81, 83, 99\} \subset B.$$

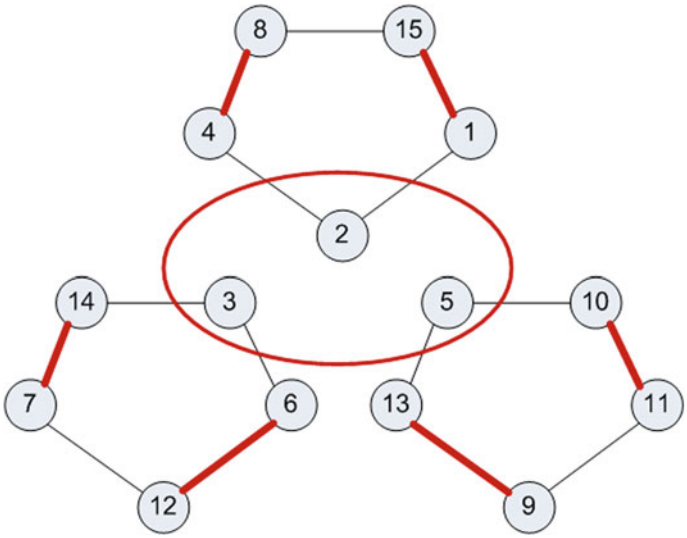

Fig. 1 An optimal matching of hypergraph $H(31)$

Theorem 5 *Let $n \geq 3$ be an odd integer, factorized as*

$$n = p_1 p_2 \cdots p_{m_1} \cdot q_1 q_2 \cdots q_{m_2} \cdot r_1 r_2 \cdots r_{m_3},$$

where p_i, q_j, and r_ℓ are primes (not necessary distinct) with $p_i \in A$, $q_j \in B$, and $r_\ell \notin A \cup B$. Let $n' = p_1 p_2 \cdots p_{m_1}$ and $n'' = q_1 q_2 \cdots q_{m_2}$. Then

$$O(n) = O(n'n'') = O(n') + O(n''), \tag{6}$$

and

$$M(n) = \frac{1}{4}(n - n'n'') + M(n'n''). \tag{7}$$

In order to prove Theorem 5, we need the following two lemmas. The first one can be derived from the definition of A and B.

Lemma 4 *Let $n \geq 3$ be odd integers.*

(i) $2^b \equiv \pm 1 \pmod n$ *if and only if b is a multiple of c_n.*
(ii) *If* $2^x \equiv 1 \pmod n$ *for some odd integer x, then $n \in A$.*
(iii) *If* $2^y \equiv -1 \pmod n$ *for some odd integer y, then $n \in B$.*

The next lemma shows that if $a \in A$ and $b \in B$, then $\gcd(a, b) = 1$.

Lemma 5 *Let $n, m \geq 3$ be odd integers.*

(i) *If all prime factors of n are in A, then $n \in A$.*
(ii) *If all prime factors of n are in B, then $n \in B$.*
(iii) *If $m \notin A \cup B$, then $mn \notin A \cup B$ for all odd $n \geq 3$.*
(iv) *If $m \in A$ and $n \in B$, then $mn \notin A \cup B$.*

Proof We first prove by induction that if a prime p is in A, then p^a is also in A for all $a \geq 1$. This is clearly true for $a = 1$. Suppose that $p^a \in A$. By definition we have $2^{c_{p^a}} = 1 + kp^a$

for some integer k. Raising both sides to the power p, we get

$$2^{pc_{p^a}} = 1 + \sum_{i=1}^{p} \binom{p}{i} k^i p^{ia}.$$

The summation on the right-hand side is divisible by p^{a+1}. Thus $2^{pc_{p^a}} \equiv 1 \pmod{p^{a+1}}$. This implies that $p^{a+1} \in A$ by Lemma 4(ii).

Next we show that if n, m are relatively prime and are both in A, then their product mn is in A. Indeed, from $2^{c_n} \equiv 1 \pmod{n}$ and $2^{c_m} \equiv 1 \pmod{m}$, we can see that $2^{c_n c_m}$ is congruent to 1 mod n and mod m. Since $\gcd(n, m) = 1$, we get $2^{c_n c_m} \equiv 1 \pmod{mn}$. By Lemma 4(ii), we conclude that mn is in A. This proves part (i)

Part (ii) of the lemma can be proved similarly.

For part (iii), we have $2^x \equiv 1 \pmod{m}$ only if x is even. However, from $2^{c_{mn}} \equiv 1 \pmod{mn}$, we get $2^{c_{mn}} \equiv 1 \pmod{m}$. Hence, c_{mn} is even.

To prove part (iv) of the lemma, we note that $2^{c_{mn}}$ cannot be congruent to $-1 \pmod{mn}$; otherwise, it would imply that $2^{c_m} \equiv -1 \pmod{m}$, contradicting the assumption that $m \in A$. Therefore, we have $2^{c_{mn}} \equiv 1 \pmod{mn}$, and thus $2^{c_{mn}} \equiv 1 \pmod{n}$. Since $n \in B$, this is possible only if c_{mn} is even. □

Proof of Theorem 5 To prove (6), we recall that we can compute $O(n)$ by summing δ_d over all divisors d of n. If d is divisible by a prime r_ℓ for some ℓ, then it follows from Lemma 5(iii) that $\delta_d = 0$. If d is divisible by $p_i q_j$ for some i and j, then from Lemma 5(iv) δ_d is also equal to 0. Therefore,

$$\begin{aligned} O(n) &= \sum_{\substack{d|n \\ d\in A}} \delta_d + \sum_{\substack{d|n \\ d\in B}} \delta_d \\ &= O(p_1 p_2 \cdots p_{m_1}) + O(q_1 q_2 \cdots q_{m_2}). \end{aligned}$$

Each odd cycle in $G(p_1 \cdots p_{m_1} q_1 \cdots q_{m_2})$ are congruent to an odd cycle in $G(n)$. The odd cycles in $G(p_1 \cdots p_{m_1} q_1 \cdots q_{m_2})$ are in one-to-one correspondence to the odd cycles in $G(n)$. Any CAC of length $p_1 \cdots p_{m_1} q_1 \cdots q_{m_2}$ can be "lifted" to a CAC of length n. This proves (6).

Let $m(n)$ be the largest number of hyperedges which lies across three distinct vertices. Then we have $m(n) = m(n'n'')$. The largest number of codewords in a CAC(n) is

$$\begin{aligned} M(n) &= \frac{1}{2}\left(\frac{n-1}{2} - O(n)\right) + m(n) \\ &= \frac{1}{2}\left(\frac{n-1}{2} - O(n'n'')\right) + m(n'n'') \\ &= \frac{1}{2}\left(\frac{n-1}{2} - O(n'n'')\right) + M(n'n'') - \frac{1}{2}\left(\frac{n'n''-1}{2} - O(n'n'')\right) \\ &= \frac{1}{4}(n - n'n'') + M(n'n''). \end{aligned}$$

This completes the proof of Theorem 5. □

For example, when $n = 11 \cdot 31 = 341$, $G(341)$ contains four odd cycles of length 5, namely,

$$(11, 22, 44, 88, 165), (31, 62, 124, 93, 155),$$
$$(33, 66, 132, 77, 154), (55, 110, 121, 99, 143).$$

We can find an optimal CAC of length 341 consisting of 83 equi-difference codewords and one non-equi-difference codeword $\{0, 11, 66\}$. Thus, $M(341) = 84$. For $n = 5 \cdot 11 \cdot 31 = 1705$, $G(1705)$ also contains four odd cycles of length 5, namely,

$$5 \times (11, 22, 44, 88, 165), 5 \times (31, 62, 124, 93, 155),$$
$$5 \times (33, 66, 132, 77, 154), 5 \times (55, 110, 121, 99, 143).$$

We can find an optimal CAC of length 1705 containing the non-equi-difference codeword $\{0, 55, 330\}$. We have $M(1705) = (1705 - 341)/4 + 84 = 425$.

We note that the right-hand side of (7) only depends on the prime factors which belongs to A and B. Theorem 5 reveals some structure in the computation of $M(n)$. The set of odd integers, $\mathbb{Z}_{odd}$, can be regarded as a semi-group, with integer multiplication as the semi-group operation. The subset of odd integers

$$\mathcal{E} = \{n \in \mathbb{Z}_{odd} : O(n) = 0\}$$

is a semi-subgroup. By (6) in Theorem 5, $\mathcal{E}$ consists of all odd integers whose divisors are all in $\mathbb{Z}_{odd} \setminus (A \cup B)$. The smallest elements in $\mathcal{E}$ are

$$\mathcal{E} = \{5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 85, 91, 97, \ldots\}.$$

For any integer a, we define $a\mathcal{E}$ as the set $\{ae : e \in \mathcal{E}\}$. Using this notation, the integers satisfying the condition of Theorem 4 in Sect. 2 (i.e., there exists a tight code in $\mathrm{CAC}^e(n)$) are precisely the elements in $\mathcal{E} \cup 3\mathcal{E}$.

The set of all odd integers can be partitioned as a disjoint union as

$$\mathbb{Z}_{odd} = \bigcup_a a\mathcal{E},$$

with the index a running over all integers in $A \cup B$. If $M(a)$ is obtained by some means, then the value of $M(n)$ is known for all n in $a\mathcal{E}$. In the computation of $M(n)$ for general odd n, it is sufficient to consider odd integer whose prime factors are in $A \cup B$.

4 Conflict-avoiding codes of prime power length

In this section, we pay our attention on the special case when n is a prime power. We first introduce a class of particular primes. A prime p which satisfies $2^{p-1} \equiv 1 \pmod{p^2}$ is called a *Wieferich prime* (see for example Sect. 6.10 in [4]). There have been only two Wieferich primes, namely 1093 and 3511, discovered so far. In addition, it is expected that the third smallest Wieferich prime must be larger than 6.7×10^{15} if it exists [1].

Remark 1 For the two known Wieferich primes 1093 and 3511, it can be shown by computer that $O(1093) = 0$ and $O(3511) = 1$ but $O(3511^2) = 3512$, see Appendix A.

Lemma 6 *If p is a non-Wieferich odd prime, then for $r \geq 2$, we have $e_{p^r} = p^{r-1} \cdot e_p$ and $c_{p^r} = p^{r-1} \cdot c_p$.*

Proof (1) We first show $e_{p^2} = p \cdot e_p$. Since, by definition, $2^{e_{p^2}} \equiv 1 \pmod{p^2}$, we have $2^{e_{p^2}} \equiv 1 \pmod{p}$. Therefore, e_{p^2} is an integral multiple of e_p. Since p is not a Wieferich prime, we have $2^{p-1} \not\equiv 1 \pmod{p^2}$, and this implies $2^{e_p} \not\equiv 1 \pmod{p^2}$. Let h be an

integer between 1 and $p-1$ defined by the relation $2^{e_p} \equiv ph+1 \pmod{p^2}$. By raising both sides to the power t, we obtain

$$(2^{e_p})^t \equiv (ph+1)^t \equiv tph + 1 \pmod{p^2}.$$

The right-hand side is congruent to 1 mod p^2 if and only if t is a multiple of p. We thus conclude that $e_{p^2} = p \cdot e_p$. Furthermore, $2^{e_{p^2}} \not\equiv 1 \pmod{p^3}$ can be obtained from the fact $\gcd(p, h) = 1$. This argument can be extended to any p^r, $r \geq 3$. This completes the proof of this part.

(2) By definition, c_p equals e_p or $\frac{e_p}{2}$ depending on if e_p is odd or even. The case when e_p is odd has just been proven in (1). The case when e_p is even, it follows from (1) that $e_{p^r} = p^{r-1}e_p$ is even. Since $\Phi(p^r) = \{a : a \in \mathbb{Z}_{p^r}, \gcd(a, p^r) = 1\}$ forms a cyclic group under multiplication, $2^{\frac{e_{p^r}}{2}} \equiv 1$ or $-1 \pmod{p^r}$. Again, by $e_{p^r} = p^{r-1}e_p$, we have

$$c_{p^r} = \frac{e_{p^r}}{2} = \frac{p^{r-1}e_p}{2} = p^{r-1}c_p.$$

This concludes the proof. □

Lemma 2(ii) states that the vertex set $\{a \in V(G(n)) : \gcd(a, n) = d\}$ in $G(n)$ can be partitioned into cycles of length $c_{n/d}$. Consider $n = p^r$, where p is non-Wieferich prime and $r \in \mathbb{N}$. We say the vertices in the set

$$\{a \in V(G(p^r)) : \gcd(a, p^r) = p^t\}$$

are on the tth level, and can be partitioned into cycles of length $c_{p^{r-t}}$. Note that the 0th level is also called the *base level*. By Lemma 6, the cycle structure in $G(p^r)$ can be completely characterized.

Theorem 6 *For p is a non-Wieferich odd prime and $r \in \mathbb{N}$, each level in $G(p^r)$ contains $O(p)$ odd cycles. That is, there are $r \cdot O(p)$ odd cycles in $G(p^r)$.*

Proof For $0 \leq t \leq r-1$,

$$|\{a \in V(G(p^r)) : \gcd(a, p^r) = p^t\}| = \frac{p^{r-t-1}(p-1)}{2},$$

and each cycle in the tth level is of the same length $c_{p^{r-t}}$. Then, by Lemma 6, the tth level contains

$$\left(\frac{p^{r-t-1}(p-1)}{2}\right) \Big/ c_{p^{r-t}} = \frac{p^{r-t-1}(p-1)}{2p^{r-t-1}c_p} = O(p)$$

cycles. This completes the proof. □

Example 5 $G(3) = (1)$, $G(9) = (1, 2, 4) \cup (3)$, $G(27) = (1, 2, 4, 8, 11, 5, 10, 7, 13) \cup (3, 6, 12) \cup (9)$, and $G(81) = (1, 2, 4, 8, 16, 32, 17, 34, 13, 26, 29, 23, 35, 11, 22, 37, 7, 14, 28, 25, 31, 19, 38, 5, 10, 20, 40) \cup (3, 6, 12, 24, 33, 15, 30, 21, 39) \cup (9, 18, 36) \cup (27)$. Then $O(27) = 3 \cdot O(3)$ and $O(81) = 4 \cdot O(3)$.

In $G(81)$, by multiplying all the vertices in the standard cycle by 3, we have three copies of the first level cycle: $3(1, 2, 4, 8, 16, 32, 17, 34, 13) \equiv 3(26, 29, 23, 35, 11, 22, 37, 7, 14) \equiv 3(28, 25, 31, 19, 38, 5, 10, 20, 40) \equiv (3, 6, 12, 24, 33, 15, 30, 21, 39)$. In the same way, by multiplying the vertices in the standard cycle by 9, we will have nine copies of the second

level cycle. This is because for any b on the first (or second) level, there are exactly 3 (or 9) vertices v on the standard level so that $3v \equiv b$ (or $9v \equiv b$) under modulo 81. The following lemma presents a more precise description of this phenomenon.

Lemma 7 *Let p be a non-Wieferich prime and r be a positive integer.*

(i) In $G(p^r)$, for any $b \in V(G(p^r))$ on the tth level cycle, there are exactly p^{t-s} vertices x satisfying the congruent formula

$$xp^{t-s} \equiv \pm b \ (mod\ p^r), \tag{8}$$

where $r > t > s \geq 0$. Furthermore, these p^{t-s} vertices are on the same cycle in the sth level. Note that $s = 0$ refers to the base level in the statement.

(ii) If $ap^t \equiv \pm a' p^t \ (mod\ p^r)$ in $G(p^r)$, then a and a' lie on the same cycle where $r > t \geq 1$.

Proof (i) Assume a is a solution, then $ap^{t-s} \equiv \pm b \pmod{p^r}$ implies $ap^{t-s} = i \cdot p^r \pm b$. Since the candidates of a are integers from 1 to $\frac{p^r-1}{2}$, $ap^{t-s} \leq \frac{p^{t-s}}{2}(p^r - 1)$. Then ap^{t-s} is either $i \cdot p^r + b$ for $0 \leq i \leq \frac{p^{t-s}-1}{2}$, or $i \cdot p^r - b$ for $1 \leq i \leq \frac{p^{t-s}-1}{2}$. Hence there are at most p^{t-s} vertices in $G(p^r)$ satisfying the congruent formula.
Now, if $b = b' p^t$, where $\gcd(b', p) = 1$, then $b' p^s$ is a solution to $xp^{t-s} \equiv \pm b \pmod{p^r}$. Let $\tilde{c}$ be the length of cycle C where b lies on, i.e., $\tilde{c} = c_{p^{r-t}}$. For $0 \leq j \leq p^{t-s}-1$, we have

$$(b' p^s) 2^{j\tilde{c}} \cdot p^{t-s} = b' p^t \cdot 2^{j\tilde{c}} = b \cdot (2^{\tilde{c}})^j \equiv \pm b \pmod{p^r}.$$

It is obvious that $b' p^s \cdot 2^{j\tilde{c}}$, $0 \leq j \leq p^{t-s} - 1$, are on the same cycle in the sth level. Moreover, since the length of sth level cycle is $c_{p^{r-s}} = p^{t-s} \times \tilde{c}$ by Lemma 6, these p^{t-s} vertices are all distinct.

(ii) Since a and a' are solutions of $xp^{t-s} \equiv \pm b \pmod{p^r}$ for some b, trivially they are on the same cycle by (i).

To obtain an optimal CAC, we could first pack equi-difference codewords in cycles of even length tightly. Then for odd cycles of length greater than or equal to 3, we try to find disjoint hyperedges $E_1, E_2, \ldots, E_\mu$ of size 3, such that (i) all vertices in the union $E_1 \cup, E_2 \cup, \ldots, \cup E_\mu$ are contained in the odd cycles, and (ii) no two vertices in $E_1 \cup, E_2 \cup, \ldots, \cup E_\mu$ are contained in the same odd cycle. We say that hyperedges satisfying (i) and (ii) *lie across distinct odd cycles*. Obviously such hyperedges exists only if there are at least three odd cycles in $G(n)$.

Back to Example 5, let a, $3b$, $9c$ be arbitrary vertices in the three non-loop cycles in $G(81)$, where a, b, c are relatively prime to 3. Since the sum of any two integers from a, $3b$, $9c$ is not congruent to the remaining one or its negative modulo 81, $\{a, 3b, 9c\}$ will not be a hyperedge in $H(81)$. Then, $M(81) = M^e(81) = 19$. This findings lead us to conclude the following result. □

Theorem 7 *Let p be a non-Wieferich odd prime and r be a positive integer. If $O(p) \leq 2$, then*

$$M(p^r) = M^e(p^r) = \frac{1}{2}\left(\frac{p^r - 1}{2} - r \cdot O(p)\right) + \xi_p,$$

where $\xi_p = 1$ or 0 depending on if $p = 3$ or not.

Proof Firstly, it is obvious that $\xi_p = 1$ only when $p = 3$, and $\xi_{3^r} = \xi_3 = 1$. By Lemma 3 and Theorem 6, it suffices to show that there is no hyperedge lying across distinct odd cycles.

In what follows, we show a further result that such a hyperedge exists only when its three vertices lie on the same level in $G(p^r)$.

We first consider the case when all the three vertices lie on distinct levels, say level x, y and z where $0 \le x < y < z < r$. Let ap^x, bp^y, cp^z be the three vertices where a, b, c are relatively prime to p. Without loss of generality, assume $ap^x + bp^y \pm cp^z \equiv 0 \pmod{p^r}$. This implies $a + bp^{y-x} \pm cp^{z-x} \equiv 0 \pmod{p^{r-x}}$ and then $a \equiv 0 \pmod{p^{y-x}}$, a contradiction to $\gcd(a, p) = 1$.

Now, consider the case when the three vertices lie on two different levels, say level x and y. Let ap^x, bp^x, cp^y be the three vertices where a, b, c are relatively prime to p. Without loss of generality, assume $ap^x + bp^x \pm cp^y \equiv 0 \pmod{p^r}$. If $x > y$, then $ap^{x-y} + bp^{x-y} \pm c \equiv 0 \pmod{p^{r-y}}$ implies $c \equiv 0 \pmod{p^{r-y}}$, a contradiction to $\gcd(c, p) = 1$. If $x < y$, observe that ap^x and bp^x lie on the different cycles on level x in $G(p^r)$. This means a and b lie on different base level cycles in $G(p^{r-x})$. By the hypothesis that $ap^x + bp^x \pm cp^y \equiv 0 \pmod{p^r}$, we have

$$\begin{aligned} &a + b \pm cp^{y-x} \equiv 0 (\mathrm{mod}\ p^{r-x}) \Rightarrow a + b \equiv 0 \pmod{p^{y-x}} \\ &\Rightarrow ap^{r-y} + bp^{r-y} \equiv 0 \pmod{p^{r-x}}. \end{aligned}$$

By Lemma 7, a and b should be on the same cycle in $G(p^{r-x})$, which contradicts to the assumption we made. This concludes the proof. □

Remark 2 Levenshtein and Tonchev [9] stated $M(n) \sim \frac{n}{4}$ as odd $n \to \infty$. Theorem 7 shows, however, that $\frac{n-1}{4} - M(n) \ge \log_p n$ or $\frac{1}{2}\log_p n$ if $O(p) = 2$ or $O(p) = 1$, where $n = p^r$ for some r.

Theorem 8 *Let $p > 3$ be a non-Wieferich prime. Then, for $r \ge 1$,*

$$M(p^r) = \frac{1}{4}\left(p^r - rp + r - 1\right) + rM(p).$$

Proof For $O(p) \le 2$, by Theorem 7, $M(p^r) = \frac{1}{2}\left(\frac{p^r-1}{2} - r \cdot O(p)\right)$ and $O(p) = 2\left(\frac{p-1}{4} - M(p)\right)$. On these two equations we immediately deduce the objective formula.

For $O(p) \ge 3$, we assume that in $H(p)$ the maximum number of mutually disjoint hyperedges of size 3 lying across distinct odd cycles is $m(p)$. That is, assume

$$M(p) = \frac{1}{2}\left(\frac{p-1}{2} - O(p)\right) + m(p).$$

In the proof of Theorem 7, those hyperedges of size 3 can not lie across different levels in $H(p^r)$. We claim that there are exactly $m(p)$ such mutually disjoint hyperedges on each level in $H(p^r)$. Assume that $E_i = \{a_i, b_i, c_i\}, i = 1, 2, \ldots, m(p)$, are those hyperedges in $H(p)$. For each E_i, let $t \times E_i$ denote the set $\{ta_i, tb_i, tc_i\}$. We first consider the $(r-1)$-th level. Since any cycle C in $H(p)$ is congruent to $p^{r-1} \times C$ on the $(r-1)$-th level in $H(p^r)$, $p^{r-1} \times E_1$, $p^{r-1} \times E_2, \ldots, p^{r-1} \times E_{m(p)}$ are mutually disjoint hyperedges of size 3 lying across different cycles, and there is no more extra such hyperedges. Then, there is a bijective mapping between cycles on any two levels. This implies that exactly $m(p)$ mutually disjoint hyperedges lying across different cycles can be found on each level. By Theorem 6, we hence have

$$M(p^r) = \frac{1}{2}\left(\frac{p^r - 1}{2} - rO(p)\right) + rm(p).$$

By replacing $m(p)$ by $M(p) - \frac{1}{2}(\frac{p-1}{2} - O(p))$, the equation in the theorem is derived. □

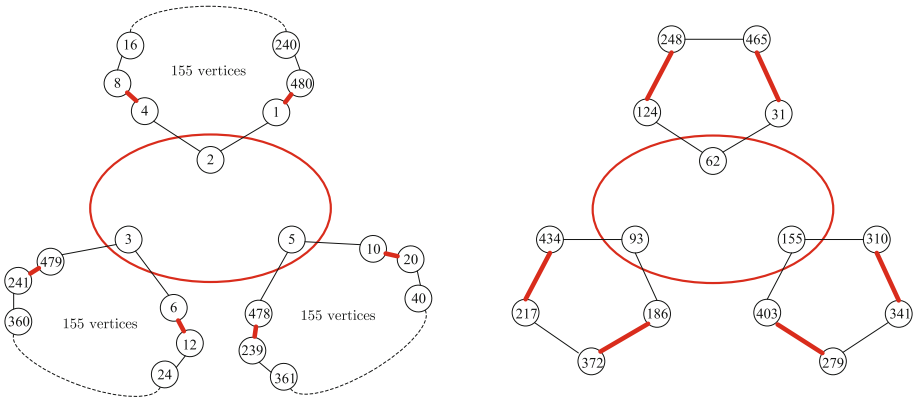

Fig. 2 An optimal matching of hypergraph $H(31^2)$

Remark 3 For $p = 3$, the only case when $\xi_p = 1$, we have the following formula by a similar argument:

$$M(3^r) = \frac{1}{4}(3^r - 2r + 3).$$

Example 6 Example 3 expresses $M(31) = 7$. For $n = 31^r$, by Theorem 8, $M(31^r) = \frac{1}{4}(31^r - 2r - 1)$. Fig. 2 shows the case $r = 2$. The hyperedges of size 3 on the base and 1st level are $\{2, 3, 5\}$ and $\{62, 93, 155\}$, respectively. Both of their corresponding codewords are not of equi-difference. The remaining vertices can be partitioned into 237 pairs, each of them corresponds to an equi-difference codeword. This CAC is optimal because it attains the upper bound of Lemma 3, and the formula

$$M(31^2) = \frac{1}{4}\Big(961 - 4 - 1\Big) = 239$$

holds.

5 An algorithm for constructing non-equi-difference CAC

In this section, we consider optimal CAC for general positive integer n by giving a systematic method for constructing non-equi-difference CAC. We first, in $H(n)$, construct as many mutually disjoint hyperedges lying across distinct odd cycles as possible. Then remove the involved vertices. Finally, we find the maximum matching in the induced subgraph of $G(n)$ by the remaining vertices. We use an example to illustrate the idea of this procedure.

Example 7 In Fig. 3 there are seven cycles in $G(99)$ and all of them are odd cycles. There are two cycles of length 15, three cycles of length 5, one cycle of length 3 and one loop. The hyperedges $\{1, 10, 11\}$ and $\{6, 9, 15\}$ lie across distinct odd cycles. These two hyperedges correspond to the non-equi-difference codewords $\{0, 1, 11\}$ and $\{0, 6, 15\}$.

We initialize $\mathcal{C}$ as the empty set. Firstly we put the non-equi-difference codewords $\{0, 1, 11\}$ and $\{0, 6, 15\}$ into $\mathcal{C}$. We then pack the odd cycles with edges of size two, and put the corresponding equi-difference codewords into $\mathcal{C}$. The resulting matching is shown by the thick lines in Fig. 3. We have thus constructed a CAC with 24 codewords, which is optimal by Lemma 3.

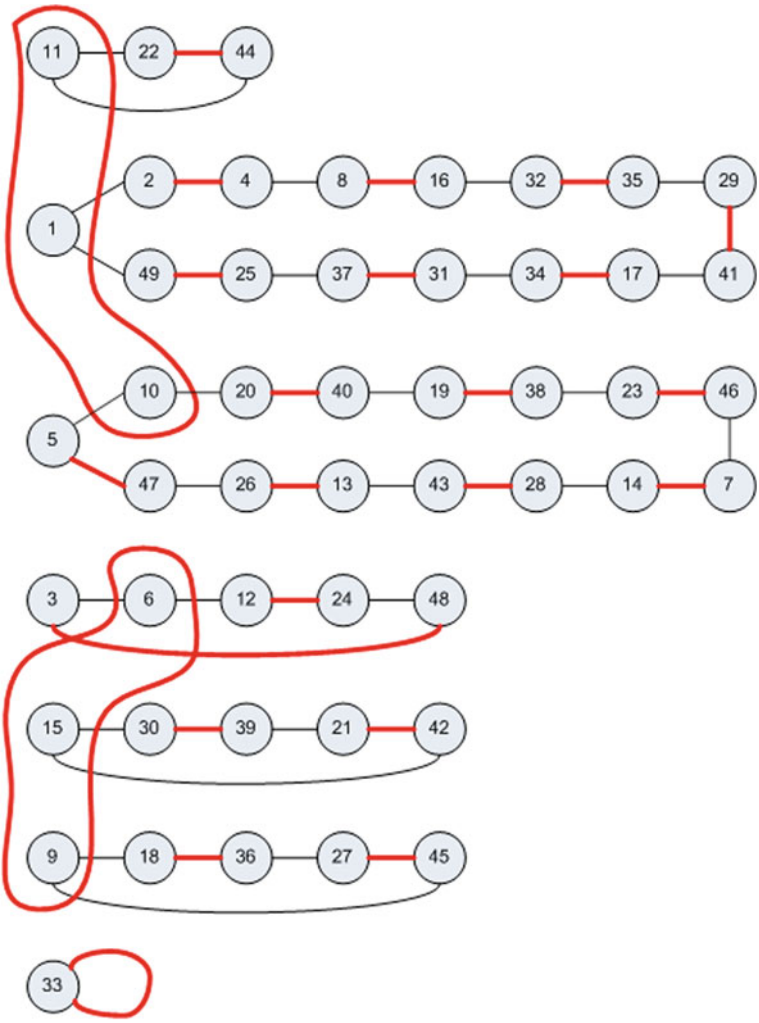

Fig. 3 An optimal matching of hypergraph $H(99)$

In order to find such mutually disjoint hyperedges effectively, we construct an auxiliary hypergraph $H'(n)$ with $O(n)-\xi_n$ vertices, where $\xi_n = 1$ or 0 depending on if $3|n$ or otherwise. Each vertex is associated with an odd cycle of length at least 3 in $G(n)$. For each hyperedge of size 3 lying across three distinct odd cycles, we put a hyperedge of size 3 covering the three corresponding vertices in $H'(n)$. We then apply any hypergraph matching algorithm on the auxiliary graph $H'(n)$. If a hypergraph matching consisting of $\lfloor \frac{O(n)-\xi_n}{3} \rfloor$ hyperedges is found, then we have an optimal CAC attaining the upper bound in Lemma 3. However, if the hyperedges in the resulting hypergraph matching is strictly less than $\lfloor \frac{O(n)-\xi_n}{3} \rfloor$, then the CAC constructed in this way may or may not be optimal. According to our experiences on finding hyperedges in $H(p)$, we conjecture that $H'(p)$ has a hypergraph matching of size $\left\lfloor \frac{O(p)}{3} \right\rfloor$ for any prime p with $O(p) \geq 3$.

Conjecture 1 For any non-Wieferich prime p, $H'(p)$ contains a hypergraph matching of size $\left\lfloor \frac{O(p)}{3} \right\rfloor$. That is,

$$M(p^r) = \frac{1}{2}\left(\frac{p^r - 1}{2} - r \cdot O(p)\right) + r\left\lfloor \frac{O(p)}{3} \right\rfloor$$

By computer search, the above conjecture is verified for all odd primes less than 1000.

For odd length less than 100, a table of optimal CAC of weight 3 is given in Appendix B. We observe for length 31, 33, 43, 57, 73, 89, 93 and 99, the optimal CAC contains non-equi-difference codeword(s). For the rest of the cases, an optimal CAC can be constructed entirely by equi-difference codewords.

In Appendix C, the values of $M(n)$ for odd n, $100 \leq n \leq 520$ are tabulated.

Acknowledgments The authors would like to express their gratitude to the referees for their helpful comments in improving the presentation of this paper, especially for the carefully reading in the revised version. The work of H. L. Fu and Y. H. Lo was supported in part by the NSC under Grant 100-2115-M-009-005-MY3, and the work of K. W. Shum was partially supported by a grant from the University Grants Committee (Project No. AoE/E-02/08) of the Hong Kong Special Administrative Region, China

Appendices

A Standard cycles in $G(p)$ for Wieferich primes $p = 1093, 3511$

The following table shows the standard cycles in $G(1093)$ and $G(3511)$. In $G(1093)$, the other two cycles are $5\langle 2\rangle_{1093}$ and $7\langle 2\rangle_{1093}$, which are both of even length 182. This implies that $O(1093^r) = 0$ for all $r \geq 1$. In $G(3511)$, $\langle 2\rangle_{3511}$ is the only one cycle and of odd length 1755. In $G(3511^2)$, however, the standard cycle $\langle 2\rangle_{3511^2}$ is of length 1755 and all other cycles are congruent to it. That is, there are 3,512 odd cycles in $G(3511^2)$. Moreover, it is easy to find triples from different cycles to produce more codewords. $\{2140703\ (\in \langle 2\rangle_{3511^2}), 821830\ (\in 5\ \langle 2\rangle_{3511^2}), 2962533\ (\in 145\langle 2\rangle_{3511^2})\}$ and $\{3126190\ (\in 125\langle 2\rangle_{3511^2}), 4067727\ (\in 2841\langle 2\rangle_{3511^2}),\ 5133204\ (\in 12821\langle 2\rangle_{3511^2})\}$, for instance (Table 1).

Table 1 The standard cycles in $G(1093)$ and $G(3511)$

n	$\langle 2\rangle_n$	Length	$O(n)$
1093	(1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 69, 138, 276, 541, 11, 22, 44, 88, 176, 352, 389, 315, 463, 167, 334, 425, 243, 486, 121, 242, 484, 125, 250, 500, 93, 186, 372, 349, 395, 303, 487, 119, 238, 476, 141, 282, 529, 35, 70, 140, 280, 533, 27, 54, 108, 216, 432, 229, 458, 177, 354, 385, 323, 447, 199, 398, 297, 499, 95, 190, 380, 333, 427, 239, 478, 137, 274, 545, 3, 6, 12, 24, 48, 96, 192, 384, 325, 443, 207, 414, 265, 530, 33, 66, 132, 264, 528, 37, 74, 148, 296, 501, 91, 182, 364, 365, 363, 367, 359, 375, 343, 407, 279, 535, 23, 46, 92, 184, 368, 357, 379, 335, 423, 247, 494, 105, 210, 420, 253, 506, 81, 162, 324, 445, 203, 406, 281, 531, 31, 62, 124, 248, 496, 101, 202, 404, 285, 523, 47, 94, 188, 376, 341, 411, 271, 542, 9, 18, 36, 72, 144, 288, 517, 59, 118, 236, 472, 149, 298, 497, 99, 198, 396, 301, 491, 111, 222, 444, 205, 410, 273, 546)	182	0

Table 1 continued

n	$\langle 2 \rangle_n$	Length	$O(n)$
3511	(1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 1463, 585, 1170, 1171, 1169, 1173, 1165, 1181, 1149, 1213, 1085, 1341, 829, 1658, 195, 390, 780, 1560, 391, 782, 1564, 383, 766, 1532, 447, 894, 1723, 65, 130, 260, 520, 1040, 1431, 649, 1298, 915, 1681, 149, 298, 596, 1192, 1127, 1257, 997, 1517, 477, 954, 1603, 305, 610, 1220, 1071, 1369, 773, 1546, 419, 838, 1676, 159, 318, 636, 1272, 967, 1577, 357, 714, 1428, 655, 1310, 891, 1729, 53, 106, 212, 424, 848, 1696, 119, 238, 476, 952, 1607, 297, 594, 1188, 1135, 1241, 1029, 1453, 605, 1210, 1091, 1329, 853, 1706, 99, 198, 396, 792, 1584, 343, 686, 1372, 767, 1534, 443, 886, 1739, 33, 66, 132, 264, 528, 1056, 1399, 713, 1426, 659, 1318, 875, 1750, 11, 22, 44, 88, 176, 352, 704, 1408, 695, 1390, 731, 1462, 587, 1174, 1163, 1185, 1141, 1229, 1053, 1405, 701, 1402, 707, 1414, 683, 1366, 779, 1558, 395, 790, 1580, 351, 702, 1404, 703, 1406, 699, 1398, 715, 1430, 651, 1302, 907, 1697, 117, 234, 468, 936, 1639, 233, 466, 932, 1647, 217, 434, 868, 1736, ... ⋮ ..., 795, 1590, 331, 662, 1324, 863, 1726, 59, 118, 236, 472, 944, 1623, 265, 530, 1060, 1391, 729, 1458, 595, 1190, 1131, 1249, 1013, 1485, 541, 1082, 1347, 817, 1634, 243, 486, 972, 1567, 377, 754, 1508, 495, 990, 1531, 449, 898, 1715, 81, 162, 324, 648, 1296, 919, 1673, 165, 330, 660, 1320, 871, 1742, 27, 54, 108, 216, 432, 864, 1728, 55, 110, 220, 440, 880, 1751, 9, 18, 36, 72, 144, 288, 576, 1152, 1207, 1097, 1317, 877, 1754, 3, 6, 12, 24, 48, 96, 192, 384, 768, 1536, 439, 878, 1755)	1755	1

B Optimal CAC of odd length ≤ 100 and weight 3

Table 2 Codewords of optimal CAC(n) for odd n, $5 \leq n \leq 100$

n	$M(n)$	Generators of equi-difference codewords	Non-equi-difference codewords
5,7	1	1	
9	2	1,3	
11	2	1,4	
13	3	1,3,4	
15	4	1,3,4,5	
17	4	1,3,4,7	
19	4	1,3,4,7	
21	5	1,3,4,5,7	
23	5	1,3,4,5,7	
25	6	1,4,5,6,9,11	
27	6	1,3,4,9,10,11	
29	7	1,4,5,6,7,9,13	
31	7	4,6,7,9,10,15	{0,2,5}
33	8	4,6,7,9,10,11,16	{0,2,5}

Table 2 continued

n	$M(n)$	Generators of equi-difference codewords	Non-equi-difference codewords
35	8	1,4,5,6,7,9,11,16	
37	9	1,3,4,7,9,10,11,12,16	
39	10	1,3,4,9,10,12,13,14,16,17	
41	10	1,3,4,7,10,11,12,13,16,18	
43	10	2,5,8,9,11,12,13,14,20	{0,1,7}
45	11	1,3,4,5,9,11,12,14,15,16,19	
47	11	1,4,6,7,10,16,17,18,19,21,22	
49	11	1,4,5,6,7,11,15,16,18,20,23	
51	13	1,3,4,5,9,12,13,14,15,16,17,20,22	
53	13	1,4,6,7,9,10,11,13,15,16,17,24,25	
55	13	1,4,5,6,9,11,14,16,19,20,21,24,26	
57	14	4,6,7,10,11,13,15,16,17,18,19,24,28	{0,2,5}
59	14	1,4,5,6,7,13,16,18,20,21,22,24,25,28	
61	15	1,3,4,5,9,12,13,14,15,16,19,20,22,25,27	
63	15	1,3,4,5,7,9,11,12,13,15,16,17,19,20,21	
65	16	1,3,4,5,7,11,12,13,15,16,17,18,19,20,21,28	
67	16	1,3,4,9,10,11,12,14,16,19,23,25,26,27,30,31	
69	17	1,3,4,5,9,11,12,13,14,15,16,17,20,21,23,25,31	
71	17	1,3,4,5,7,9,12,13,16,17,19,20,21,22,23,28,30	
73	17	4,6,9,10,11,14,16,17,19,23,24,26,29,30,33,36	{0,2,5}
75	19	1,3,4,5,11,12,13,14,15,16,18,19,20,25,26,27,29,31,33,34	
77	18	1,4,6,7,9,10,11,13,15,16,17,19,23,24,25,28,36,37	
79	19	1,3,4,9,10,12,13,14,15,16,19,22,23,27,29,31,34,36,37	
81	19	1,3,4,7,9,10,12,13,16,17,22,27,28,29,30,31,33,35,38	
83	20	1,4,6,7,10,11,13,16,18,19,24,28,29,30,31,33,34,37,39,40	
85	21	1,3,4,5,7,9,12,15,16,17,19,20,21,22,23,25,26,27,28,36,37	
87	22	1,3,4,5,7,12,13,15,16,18,20,21,22,23,25,27,28,29,34,35,38,39	
89	21	4,6,7,10,11,13,16,17,18,21,23,24,25,28,30,31,35,37,40,44	{0,2,5}
91	22	1,3,4,7,9,10,12,13,16,17,21,22,23,25,27,28,29,30,36,38,40,43	
93	23	1,4,5,7,12,13,16,17,18,19,20,21,22,23,25,27,28,29,30,31,41,45	{0,6,15}
95	23	1,4,5,6,9,11,14,15,16,19,20,21,24,26,29,31,34,35,36,39,41,46	
97	24	1,4,5,6,9,13,14,16,17,19,20,21,22,23,	
		24,29,30,33,35,36,41,43,45,47	
99	24	2,7,8,12,13,17,18,19,20,21,22,23,	{0,1,11}
		25,27,28,29,30,31,32,33,47,48	{0,6,15}

C The size of optimal CAC for odd n, $100 \leq n \leq 520$

In this appendix we tabulate the value $M(n)$, for odd n between 100 and 520. The entries marked by * indicate that non-equi-difference codewords are required to construct optimal CAC. Otherwise, we can find an equi-difference CAC which is optimal. Except $n =$

189, 243, 405, 343, 441, which are marked by † in the following table, the number of codewords matches the upper bound in Lemma 3, and is thus optimal. For $n = 243, 343$, which are powers of 3 and 7 respectively, the value of $M(n)$ is given by Theorem 7. For $n = 189, 405, 441$, the optimality follows from arguments similar to the proof of Theorem 7 (Tables 3 and 4).

Table 3 List of $M(n)$ for odd n, $101 \leq n \leq 300$

n	101	103	105	107	109	111	113	115	117	119
$M(n)$	25	25	26	26	27	28	28	28	29	29
n	121	123	125	127	129	131	133	135	137	139
$M(n)$	29	31	31	30*	31*	32	32	33	34	34
n	141	143	145	147	149	151	153	155	157	159
$M(n)$	35	35	36	36	37	36*	38	38*	39	40
n	161	163	165	167	169	171	173	175	177	179
$M(n)$	39*	40	41*	41	42	41*	43	43	44*	44
n	181	183	185	187	189	191	193	195	197	199
$M(n)$	45	46	46	46	47†	47	48	49	49	49
n	201	203	205	207	209	211	213	215	217	219
$M(n)$	50*	50	51	51	51*	52	53	53*	52*	54*
n	221	223	225	227	229	231	233	235	237	239
$M(n)$	55	55*	56	56	57	57*	57*	58	59	59
n	241	243	245	247	249	251	253	255	257	259
$M(n)$	60	60†	60	61	62*	60*	62	64	64	64
n	261	263	265	267	269	271	273	275	277	279
$M(n)$	65	65	66	65*	67	67	68	68	69	69*
n	281	283	285	287	289	291	293	295	297	299
$M(n)$	69*	70*	71*	71	72	73	73	73	73*	74

Table 4 List of $M(n)$ for odd n, $301 \leq n \leq 520$

n	301	303	305	307	309	311	313	315	317	319
$M(n)$	74*	76	76	76*	77	77	78	78	79	79
n	321	323	325	327	329	331	333	335	337	339
$M(n)$	80*	80	81	82	81*	80*	83	83	82*	85
n	341	343	345	347	349	351	353	355	357	359
$M(n)$	84*	85†	86	86	87	87	88	88	89	89
n	361	363	365	367	369	371	373	375	377	379
$M(n)$	89	88*	89*	91	92	92	93	94	94	94
n	381	383	385	387	389	391	393	395	397	399
$M(n)$	94*	95	95	94*	97	97	98*	98	99	99*
n	401	403	405	407	409	411	413	415	417	419
$M(n)$	100	100*	101†	101	102	103	102	103	104*	104
n	421	423	425	427	429	431	433	435	437	439

Table 4 continued

$M(n)$	105	105	106	106	107*	106*	108	109	108	109*
n	441	443	445	447	449	451	453	455	457	459
$M(n)$	110†	110	110*	112	112	112	112*	113	114	114
n	461	463	465	467	469	471	473	475	477	479
$M(n)$	115	115	116*	116	116	118	116*	118	119	119
n	481	483	485	487	489	491	493	495	497	499
$M(n)$	120	120*	121	121	122*	122	123	123*	123*	124
n	501	503	505	507	509	511	513	515	517	519
$M(n)$	125	125	126	127	127	122*	123*	128	128	130

References

1. Dorais F.G., Klyve D.W.: A Wieferich prime search up to 6.7×10^{15}. J. Integer Seq. **14**, (2011).
2. Fu H.-L., Lin Y.-H., Mishima M.: Optimal conflict-avoiding codes of even length and weight 3. IEEE Trans. Inform. Theory **56**(11), 5747–5756 (2010).
3. Györfi L., Vajda I.: Constructions of protocol sequences for multiple access collision channel without feedback. IEEE Trans. Inform. Theory **39**(5), 1762–1765 (1993).
4. Hardy G.H., Wright E.M.: An Introduction to the Theory of Numbers, pp. 72–73. Oxford University Press, New York (1938).
5. 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 **53**(8), 2732–2742 (2007).
6. Kløve T., Elarief N., Bose B.: Systematic, single limited magnitude error correcting codes for flash memories. IEEE Trans. Inform. Theory **57**(7), 4477–4487 (2011).
7. Kløve T., Luo J., Naydenova I., Yari S.: Some codes correcting asymmetric errors of limited magnitude. IEEE Trans. Inform. Theory **57**(11), 7459–7472 (2011).
8. Levenshtein V.I.: Conflict-avoiding codes and cyclic triple systems. Probl. Inform. Transm. **43**(3), 199–212 (2007).
9. Levenshtein V.I., Tonchev V.D.: Optimal conflict-avoiding codes for three active users. In: Proceedings of IEEE International Symposium on Information Theory, Adelaide, pp. 535–537 (2005).
10. Mishima M., Fu H.-L., Uruno S.: Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3. Des. Codes Cryptogr. **52**(3), 275–291 (2009).
11. Momihara K., Müller M., Satoh J., Jimbo M.: Constant weight conflict-avoiding codes. SIAM J. Discrete Math. **21**(4), 959–979 (2007).
12. Massey J.L., Mathys P.: The collision channel without feedback. IEEE Trans. Inform. Theory **31**(2), 192–204 (1985).
13. Mathys P.: A class of codes for T active users out of N multiple-access communication system. IEEE Trans. Inform. Theory **36**(6), 1206–1219 (1990).
14. Momihara K.: Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three. Des. Codes Cryptogr. **45**(3), 379–390 (2007).
15. OEIS Foundation Inc. The on-line encyclopedia of integer sequences. http://oeis.org
16. Shum K.W., Wong W.S., Chen C.S.: A general upper bound on the size of constant-weight conflict-avoiding codes. IEEE Trans. Inform. Theory **56**(7), 3265–3276 (2010).
17. Shum K.W., Wong W.S.: A tight asymptotic bound on the size of constant-weight conflict-avoiding codes. Des. Codes Cryptogr. **57**(1), 1–14 (2010).
18. Silverman J.H.: A Friendly Introduction to Number Theory, pp. 150–160. Pearson Education Taiwan Ltd, Taiwan (2004).
19. Tsybakov B.S., Rubinov A.R.: Some constructions of conflict-avoiding codes. Probl. Inf. Transm. **38**(4), 268–279 (2002).
20. Wu S.-L., Fu H.-L.: Optimal tight equi-difference conflict-avoiding codes of length $n = 2^k \pm 1$ and weight 3. J. Combin. Des. (2012). doi:10.1002/jcd.21332.