Optimal Tight Equi-Difference Conflict-Avoiding Codes of Length $n = 2^k \pm 1$ and Weight 3

Shung-Liang Wu[1] and Hung-Lin Fu[2]

[1]*Department of Computer Science and Information Engineering, National United University, Miaoli 36003, Taiwan, E-mail: slwu@nuu.edu.tw*

[2]*Department of Applied Mathematics, National Chaio Tung University, Hsin Chu 30010, Taiwan, E-mail: hlfu@math.nctu.edu.tw*

Received February 16, 2012; revised August 28, 2012

Published online 5 October 2012 in Wiley Online Library (wileyonlinelibrary.com).
DOI 10.1002/jcd.21332

Abstract: **For a k-subset X of $\mathbb{Z}_n$, the set of differences on X is the set $\Delta X = \{i - j \pmod n : i, j \in X, i \neq j\}$. A conflict-avoiding code CAC of length n and weight k is a collection $\mathcal{C}$ of k-subsets of $\mathbb{Z}_n$ such that $\Delta X \bigcap \Delta Y = \emptyset$ for any distinct $X, Y \in \mathcal{C}$. Let CAC(n, k) be the class of all the CACs of length n and weight k. The maximum size of codes in CAC(n, k) is denoted by $M(n, k)$. A code $\mathcal{C} \in$ CAC(n, k) is said to be optimal if $|\mathcal{C}| = M(n, k)$. An optimal code $\mathcal{C}$ is tight equi-difference if $\bigcup_{X \in \mathcal{C}} \Delta X = \mathbb{Z}_n \setminus \{0\}$ and each codeword in $\mathcal{C}$ is of the form $\{0, i, 2i, \ldots, (k-1)i\}$. In this paper, the necessary and sufficient conditions for the existence problem of optimal tight equi-difference conflict-avoiding codes of length $n = 2^k \pm 1$ and weight 3 are given.** © 2012 Wiley Periodicals, Inc. J. Combin. Designs 21: 223–231, 2013

Keywords: *conflict-avoiding codes; equi-difference; optimal codes*

1. INTRODUCTION

A protocol sequence set for a multiple-access collision channel without feedback has been investigated by many researchers [3, 5–7, 12, 15]. A set $\mathbf{X} = \{X_1, X_2, \ldots, X_N\}$ of N binary sequences is called an (N, k, n, σ) *protocol sequence set* if any $X_i = (x_{i,0}, x_{i,1}, \ldots, x_{i,n-1}) \in \mathbf{X}$ is of length n and weight k and has the property that at least σ successful packet transmissions in a frame are guaranteed for each active user, provided that at most k out of N users are active. This (N, k, n, σ) protocol sequence set with $\sigma = 1$ is said to be a *conflict-avoiding code* CAC of length n and weight k, and can be reformulated as a set $\mathbf{X}$ of binary sequences of length n and weight k with the

following property:

$$\sum_{0\le r\le n-1} x_{i,r}x_{j,r+q} \le 1,$$

for any distinct X_i, X_j in $\mathbf{X}$ and every integer q, where the subscripts are taken modulo n.

In mathematical terms, a conflict-avoiding code CAC of length n and weight k is a set $\mathcal{C} \subseteq \{0, 1\}^n$ of binary vectors, or *codewords*, all of Hamming weight k, such that the Hamming distance between arbitrary cyclic shifts of distinct codewords is at least $2k - 2$. By identifying each codeword in $\mathcal{C}$ with a k-subset of $\mathbb{Z}_n$ representing the indices of its nonzero positions, where $\mathbb{Z}_n$ is the group of residues modulo n, we can restate the definition of CAC the following.

For a k-subset X of $\mathbb{Z}_n$, the set of differences on X is defined to be the set

$$\Delta X = \{i - j \pmod n : \ i, j \in X, i \ne j\}.$$

A conflict-avoiding code CAC of length n and weight k is a set $\mathcal{C}$ of k-subsets, called *codewords*, of $\mathbb{Z}_n$ such that $\Delta X \bigcap \Delta Y = \emptyset$ for any distinct $X, Y \in \mathcal{C}$. Codewords X, Y in $\mathcal{C}$ are said to be *equivalent* if $\Delta X = \Delta Y$. Let CAC(n, k) denote the class of all the CACs of length n and weight k. The maximum size of codes in CAC(n, k) is denoted by $M(n, k)$. A code $\mathcal{C} \in$ CAC(n, k) is *optimal* if $|\mathcal{C}| = M(n, k)$. Since for any codeword X in $\mathcal{C}$, there is an integer r in $\mathbb{Z}_n$ such that the translation $\widetilde{X} = \{i + r \in \mathbb{Z}_n : i \in X\}$ contains the element 0 of $\mathbb{Z}_n$ and their set of differences is invariant under translation, i.e., $\Delta X = \Delta\widetilde{X}$, we can assume without loss of generality that each codeword in $\mathcal{C}$ includes the element 0.

Suppose X is a codeword in CAC of length n and weight k. This codeword X is said to be *equi-difference* if it is of the form

$$X = \{0, i, 2i, \ldots, (k - 1)i\} \pmod n.$$

Evidently, in this case, $\Delta X = \{\pm ri : 1 \le r \le k - 1\}$ and $|\Delta X| \le 2(k - 1)$. A codeword with $|\Delta X| < 2(k - 1)$ is called *exceptional*. If all codewords in $\mathcal{C}$ are equi-difference, then $\mathcal{C}$ is called an *equi-difference* code. The maximum size of equi-difference codes in CAC$^e(n, k)$ is defined in an analogous manner to $M(n, k)$, i.e., $M^e(n, k) = \max\{|\mathcal{C}| : \mathcal{C} \in \text{CAC}^e(n, k)\}$, where CAC$^e(n, k)$ is the class of all the equi-difference codes in CAC(n, k).

For convenience sake, CAC$(n, 3)$, CAC$^e(n, 3)$, $M(n, 3)$, and $M^e(n, 3)$ are simply written as CAC(n), CAC$^e(n)$, $M(n)$, and $M^e(n)$, respectively. By $\Delta\mathcal{C}$, we mean the union of sets of differences of codewords in $\mathcal{C}$, that is, $\Delta\mathcal{C} = \bigcup_{X\in\mathcal{C}} \Delta X$. A code $\mathcal{C}$ of length n is *tight* if $\Delta\mathcal{C} = \mathbb{Z}_n \setminus \{0\}$.

Several works have been done for $M(n)$. Levenshtein and Tonchev [5, 6] show that $M(n) \le \frac{n+1}{4}$ and $M(n) = M^e(n) = \frac{n-2}{4}$ if $n \equiv 2 \pmod 4$.

When n is a multiple of 4, Jimbo et al. [4] give a better upper bound on $M(n)$ with $n = 4t$ as follows.

$$M(n) \leq \begin{cases} 7n/32, & \text{if } t \equiv 0 \pmod 8, \\ (7n+4)/32, & \text{if } t \equiv 1 \pmod 8, \\ (7n-24)/32, & \text{if } t \equiv 2, 10 \pmod{24}, \\ (7n+12)/32, & \text{if } t \equiv 3 \pmod{24}, \\ (7n-16)/32, & \text{if } t \equiv 4, 20 \pmod{24}, \\ (7n-12)/32, & \text{if } t \equiv 5, 13 \pmod{24}, \\ (7n-8)/32, & \text{if } t \equiv 6 \pmod 8, \\ (7n-4)/32, & \text{if } t \equiv 7 \pmod 8, \\ (7n-20)/32, & \text{if } t \equiv 11, 19 \pmod{24}, \\ (7n+16)/32, & \text{if } t \equiv 12 \pmod{24}, \\ (7n+8)/32, & \text{if } t \equiv 18 \pmod{24}, \\ (7n+20)/32, & \text{if } t \equiv 21 \pmod{24}. \end{cases}$$

They also prove this upper bound is sharp if $n \equiv 8 \pmod{16}$. The remaining cases for the problem of optimal conflict-avoiding code of even length n and weight 3 are determined by [1, 8]. The exact values of $M(n)$ for n even now are completely given. However, known results for $M(n)$ with n odd is far from being solved. Levenshtein [5] presented some $M(n)$ where $n \leq 100$ and $n \neq 31, 33, 43, 57, 73, 89, 93$, and 99. Recently, [2] has completely found out $M(n)$ with n odd and $n < 500$ and for certain class of prime powers n, $M(n)$ is established. Some constructions of tight CAC^e of length n with n prime are obtained in [9, 10], and studies of $\mathrm{CAC}(n, k)$ with $k > 3$ can be found in [11, 13, 14].

In this paper, we focus on the constructions of optimal tight equi-difference conflict-avoiding codes of length $n = 2^k \pm 1$ and weight 3 and we obtain the following consequences.

Theorem 1.1.

(1) *Let $n = 2^k + 1$ for $k \geq 2$. Then there exists an optimal tight equi-difference code $\mathcal{C}$ in $CAC^e(n)$ with $|\mathcal{C}| = M^e(n) = M(n)$ if and only if $k \equiv 0$ (mod 2).*
(2) *Let $n = 2^k - 1$ for $k \geq 3$. Then there exists an optimal tight equi-difference code $\mathcal{C}$ in $CAC^e(n)$ with $|\mathcal{C}| = M^e(n) = M(n)$ if and only if $k = 2^t$ for $t \geq 2$.*

2. CONSTRUCTING OPTIMAL TIGHT EQUI-DIFFERENCE CODES

Throughout this paper, assume n to be an odd integer and $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$. Given a positive integer m with $1 \leq m \leq \frac{n-1}{2}$, a *cycle* C of length m, denoted m-cycle, is an m-tuple $(c_1, c_2, \ldots, c_m)$ of pairwise distinct elements $c_1, c_2, \ldots, c_m$ in $\mathbb{Z}_n^*$ and whose edges are those connecting c_1 with c_m and c_i with c_{i+1} for $1 \leq i \leq m-1$. An m-cycle is *even* if $m \equiv 0 \pmod 2$ or $m = 1$. That is, whenever we say that a cycle is odd, it always means that its length is greater than or equal to 3. Giving an m-cycle $C = (c_1, c_2, \ldots, c_m)$, we will use ∂C for the set of distinct elements $c_i (1 \leq i \leq m)$ in C and this cycle C is called *doubling* if for each i with $1 \leq i \leq m$, $c_{i+1} = \min\{2c_i, n - 2c_i\}$.

Given any odd integer n, let $\Omega_n = \{1, 2, \ldots, \frac{n-1}{2}\}$ be a set of integers i with $1 \leq i \leq \frac{n-1}{2}$. By $G(\Omega_n)$, we mean a *graph* G with vertex set $V(G) = \Omega_n$ and edge set

$E(G) = \{(x, y) : x, y \in \Omega_n, x \neq y, y = \min\{2x, n-2x\}\}$. Since for each element x with $x \equiv 0$ (resp. $x \equiv 1$) (mod 2) in Ω_n, the edges $(x, \min\{2x, n-2x\})$, $(x, \frac{x}{2})$ (resp. $(x, \frac{n-x}{2})$) are contained in $G(\Omega_n)$, this implies that the degree of each vertex in $G(\Omega_n)$ is two, and we have the following consequence. It should be mentioned that the graph $G(\Omega_n)$ has been used to find the set of equi-difference codewords in [2, 4–6].

Lemma 2.1. *For any odd integer n, the graph $G(\Omega_n)$ is a union of vertex-disjoint m_i-cycles $(1 \leq i \leq k)$ satisfying that $\sum_{i=1}^{k} m_i = \frac{n-1}{2}$.*

Note that each m_i-cycle in $G(\Omega_n)$ is doubling. And if $n = 3r$ for some integer r, then the graph $G(\Omega_n)$ would contain just a 1-cycle (r), which corresponds to the exceptional codeword $\{0, r, 2r\}$. It is obvious that an exceptional codeword itself is also an equi-difference codeword. A doubling cycle C of $G(\Omega_n)$ with $1 \in C$ is said to be *base*. In fact, it will be shown that the base cycle in $G(\Omega_n)$ has the largest length in all cycles of $G(\Omega_n)$. For any codeword X in $\mathcal{C}$, it is easy to see that $|\Delta X| = 2$, 4, or 6. Since an optimal code of length n and weight 3 contains at most $n-1$ differences and each codeword in it will provide at least four differences except possibly for the exceptional codeword, we may modify the inequality $M(n) \leq \frac{n+1}{4}$ the following.

Lemma 2.2.

(1) $M^e(n) \leq M(n) \leq \frac{n-1}{4}$, *if* $n \not\equiv 0$ (*mod* 3).
(2) $M^e(n) \leq M(n) \leq \frac{n+1}{4}$, *if* $n \equiv 0$ (*mod* 3).

A *matching* M in a graph is a set of pairwise nonadjacent edges, i.e., no two edges share a common vertex. A *perfect matching* is a matching such that every vertex of the graph is incident to exactly one edge of the matching. A *path* in a graph is a sequence of edges $(v_1, v_2), (v_2, v_3), \ldots, (v_{m-1}, v_m)$. This path is from vertex v_1 to vertex v_m and has length $m-1$, denoted by $P = [v_1, v_2, \ldots, v_m]$.

Proposition 2.3. *If C is an even m-cycle with $m > 1$ in $G(\Omega_n)$, then there is an equi-difference code $\mathcal{C}$ in $CAC^e(n)$ with $|\mathcal{C}| = \frac{m}{2}$ and $\Delta\mathcal{C} = \pm\partial C$.*

Proof. Since C is even, there are two perfect matchings in C, and choose one perfect matching $M = \{(a_1, b_1), (a_2, b_2), \ldots, (a_{m/2}, b_{m/2})\}$ arbitrarily. Since C is also doubling, we may assume that $b_i = 2a_i$ or $n - 2a_i$ for $1 \leq i \leq m/2$. For each edge (a_i, b_i) in M with $1 \leq i \leq m/2$, define a codeword X_i as $X_i = \{0, a_i, 2a_i\}$ and set $\mathcal{C} = \{X_i : 1 \leq i \leq m/2\}$, where $\Delta X_i = \pm\{a_i, b_i\}$.

The proof then follows since each codeword X_i in $\mathcal{C}$ is equi-difference and $\Delta\mathcal{C} = \bigcup_{i=1}^{m/2} \Delta X_i = \pm\partial C$. □

Proposition 2.4. *If $C = (c_1, c_2, \ldots, c_m)$ is an odd m-cycle in $G(\Omega_n)$, then there is an equi-difference code $\mathcal{C}$ in $CAC^e(n)$ with $|\mathcal{C}| = \frac{m-1}{2}$ and $\Delta\mathcal{C} = \pm(\partial C \setminus \{c_i\})$ for some i with $1 \leq i \leq m$.*

Proof. Removing any vertex c_i and edges incident with it from C, we have an odd path $P = [c_{i+1}, c_{i+2}, \ldots, c_{i-1}]$ of length $m-2$, and so there exists a perfect matching M in P. The rest of the proof is analogous to that in Proposition 2.3 and we leave it to the reader. □

Note that in Propositions 2.3 and 2.4, if $G(\Omega_n)$ is just an m-cycle, then there exists an optimal equi-difference code $\mathcal{C}$ in $\mathrm{CAC}^e(n)$ with $|\mathcal{C}| = M^e(n) = M(n) = \lfloor \frac{m}{2} \rfloor$.

Theorem 2.5. *There exists an optimal tight equi-difference code $\mathcal{C}$ in $CAC^e(n)$ with $|\mathcal{C}| = M^e(n) = M(n)$ if and only if the graph $G(n)$ contains no odd cycles.*

By Lemma 2.1, $G(\Omega_n)$ is a union of vertex-disjoint even m_i-cycles $C_i (1 \le i \le r)$, i.e., $G(\Omega_n) = \bigcup_{i=1}^{r} C_i$. Since any cycles C_i, C_j $(i \ne j)$ in $G(\Omega_n)$ are pairwise disjoint, it follows that $\bigcup_{i=1}^{r} \partial C_i = \Omega_n$. Let $\mathcal{C}$ be the code obtained from the union of codes $\mathcal{C}_i$ for $1 \le i \le r$. The proof of Theorem 2.5 then follows by Propositions 2.3 and 2.4 and Lemma 2.2. In fact, $|\mathcal{C}| = \frac{n-1}{4}$ if $n \not\equiv 0 \pmod 3$, and $|\mathcal{C}| = \frac{n+1}{4}$ if $n \equiv 0 \pmod 3$.

3. THE CONSTRUCTIONS OF DOUBLING CYCLES IN $G(\Omega_n)$

Let n be an odd integer (≥ 5). The *order* of 2 modulo n, denoted by $o(n)$, is the least positive integer r for which $2^r \equiv 1 \pmod n$. It is well known that $o(n)$ divides $\phi(n)$ where $\phi(n)$ is the Euler phi-function. Unless otherwise specified, throughout we shall assume $C = (2, 2^2, \ldots, 2^{o(n)}) \pmod n$ to be the base cycle on $\mathbb{Z}_n^*$ and $tC = (2t, 2^2t, \ldots, 2^{o(n)}t) \pmod n$ to be the cycle obtained from C by multiplying each vertex in C by the element $t \in \mathbb{Z}_n^*$. Recall that in Lemma 2.1, the graph $G(\Omega_n)$ is a union of disjoint m_i-cycles with $\sum m_i = \frac{n-1}{2}$. Hence, it is very important to confirm the odd/even length of each doubling cycle in $G(\Omega_n)$. Moreover, despite the fact that Levenshtein and Tonchev [6] has mentioned that the graph $G(\Omega_n)$ is a union of disjoint doubling cycles t_iC for some elements $t_i \in \mathbb{Z}_n^*$, for the sake of the completeness and self-containedness of this paper, we shall entirely characterize the structure of cycles in $G(\Omega_n)$. In fact, these consequences can be utilized further to set up an optimal code CAC of length n with n any odd integer.

The base cycle C plays a vital role for the constructions of doubling cycles in $G(\Omega_n)$. Because we can use the base cycle C to establish all doubling cycles in $G(\Omega_n)$, we shall refer to the base cycle C as a member of $G(\Omega_n)$. Similarly, the cycle tC is also viewed as a member of $G(\Omega_n)$. To avoid the complicated notations, we will use $(c_1, c_2, \ldots, c_{o(n)})$ to denote a cycle where $c_i \in \mathbb{Z}_n^*$ and $<c_1, c_2, \ldots, c_{o(n)}>$ to denote a doubling cycle in $G(\Omega_n)$; it is always clear from the context.

Proposition 3.1. *If C is a base doubling m-cycle of $G(\Omega_n)$, then $m = \frac{o(n)}{2}$ or $o(n)$.*

Proof. Since C is base and doubling, it means that $1 \in C$ and $2 \in C$ and so we may assume

$$C = (2, 2^2, \ldots, 2^{o(n)}) \pmod n, \text{ where } 2^{o(n)} \equiv 1 \pmod n.$$

By virtue of the fact that $2^{o(n)} \equiv 1 \pmod n$, it follows that if $o(n) \equiv 0 \pmod 2$, then $2^{o(n)/2} \not\equiv -1 \pmod n$ or $2^{o(n)/2} \equiv -1 \pmod n$.

If $o(n) \equiv 1 \pmod 2$ or $2^{o(n)/2} \not\equiv -1 \pmod n$, then

$$\begin{aligned} &C = (c_1 = 2, c_2, \ldots, c_{o(n)} = 1), \text{ where } 2^i \equiv c_i \pmod n; \\ &C = <d_1 = 2, d_2, \ldots, d_{o(n)} = 1>, \text{ where } d_i = c_i, \text{ if } c_i \le \tfrac{n-1}{2}, \\ &\qquad \text{and } d_i = n - c_i, \text{ if } c_i > \tfrac{n-1}{2}. \end{aligned}$$

If $2^{o(n)/2} \equiv -1 \pmod{n}$, then

$$C = (c_1 = 2, c_2, \ldots, c_{o(n)/2} = -1, c_{o(n)/2+1} = -2, \ldots, c_{o(n)} = 1),$$
$$\text{where } 2^i \equiv c_i (\text{mod } n);$$
$$C = <d_1 = 2, d_2, \ldots, d_{o(n)/2} = 1>, \text{ where } d_i = c_i, \text{ if } c_i \leq \tfrac{n-1}{2},$$
$$\text{and } d_i = n - c_i, \text{ if } c_i > \tfrac{n-1}{2}.$$

It is clear that the base doubling cycle C in $G(\Omega_n)$ has length $\frac{o(n)}{2}$ or $o(n)$, as desired. □

Suppose $\overline{C} = (c_1, c_2, \ldots, c_m)$ is an m-cycle where $c_i \in \mathbb{Z}_n^*$. The λ-fold of $\overline{C}$ is the *multicycle* $\overline{C}^{\lambda}$ that is a union of λ copies of $\overline{C}$, i.e., $\overline{C}^{\lambda} = (d_1, d_2, \ldots, d_{\lambda m})$ with $d_{jm+i} = c_i$ for $0 \leq j \leq \lambda - 1$ and $1 \leq i \leq m$. We usually say that λ is the *edge multiplicity* of $\overline{C}^{\lambda}$.

Given $t \in \mathbb{Z}_n^*$, by $tC = (2t, 2^2t, \ldots, 2^{o(n)}t) \pmod{n}$, we mean a multicycle $\overline{C}^{\lambda}$ with edge multiplicity λ ($\geq$1). It is obvious that if $\lambda = 1$, then tC itself is a cycle, and if $\lambda \geq 2$, then this multicycle $\overline{C}^{\lambda} = (c_1, c_2, \ldots, c_{o(n)})$ where $2^i t \equiv c_i \pmod{n}$ for $1 \leq i \leq o(n)$ corresponds to the cycle $tC = (c_1, c_2, \ldots, c_{o(n)/\lambda})$. The cycle $tC = (c_1, c_2, \ldots, c_{o(n)/\lambda})$ is said to be *full* if there does not exist c_i, c_j $(i \neq j)$ in tC such that $c_i + c_j = n$, that is, c_j is the additive inverse of c_i, and *short*, otherwise. For example, the cycle C in Proposition 3.1 with length $o(n)$ (resp. $o(n)/2$) is *full* (resp. *short*). Note that whether the cycle tC is full or short, by using the same method mentioned in Proposition 3.1, tC can be transformed into a doubling cycle in $G(\Omega_n)$.

Lemma 3.2. *Let s, t be distinct elements in $\mathbb{Z}_n^*$.*

(1) *$sC = C$ if and only if $s \in C$.*
(2) *$sC = tC$ if and only if there exists an element $2^j s$ in sC such that $2^j s \equiv t \pmod{n}$.*
(3) *If $s \in tC$, then $sC = tC$.*
(4) *Either $sC = tC$ or $sC \bigcap tC = \emptyset$.*

Proof. We just give the proofs of (1) and (4), and leave the rest to the reader.

(1) If $sC = C$, then there is an element $2^j s$ with $1 \leq j \leq o(n)$ in sC satisfying that $2^j s = 2^{o(n)} \equiv 1 \pmod{n}$, so $s = 2^{o(n)-j} \in C$ since $\gcd(2^j, n) = 1$. Conversely, if $s \in C$, we may assume that $s = 2^i$ with $1 \leq i \leq o(n)$, and

$$\begin{aligned} sC &= (2 \cdot 2^i, 2^2 \cdot 2^i, \ldots, 2^{o(n)} \cdot 2^i) \pmod{n} \\ &= (2^{i+1}, 2^{i+2}, \ldots, 2^{o(n)}, 2, \ldots, 2^i) \pmod{n} \\ &= C. \end{aligned}$$

(4) If $sC \bigcap tC \neq \emptyset$, we show that $sC = tC$. If $x \in sC \bigcap tC$, let $x \equiv 2^j s \equiv 2^k t \pmod{n}$, where $2^j s \in sC$ and $2^k t \in tC$. We may assume $k < j$. Since $\gcd(2^k, n) = 1$, $2^{j-k} s \equiv t \pmod{n}$ and it follows from (2) that $sC = tC$. □

Remark that each doubling cycle of $G(\Omega_n)$ can be obtained from the base cycle C, which indicates that the length of the base doubling cycle is the largest in all doubling cycles of $G(\Omega_n)$. And if $sC \neq tC$, then sC and tC are disjoint by Lemma 3.2(3). In other words, distinct cycles in $G(\Omega_n)$ are pairwise disjoint, and these distinct cycles are the

cells of a partition of Ω_n. If $w \in sC$ and for any $t \in sC$, $w \leq t$, we can use wC as the representative of the cycle sC. Then for each element $t \in \Omega_n$, there is exactly one cycle, say wC, in $G(\Omega_n)$ such that $t \in wC$. Note that if C is full, then wC may be full or short, but if C is short, then wC must be short.

Lemma 3.3. *If the base cycle C is short, then for any $t \in \mathbb{Z}_n^*$, the cycle tC is also short.*

Proof. For any $t \in \Omega_n$, $tC = (2t, 2^2t, \ldots, 2^{o(n)}t) \pmod n$, where $2^{o(n)/2}t \equiv -t \pmod n$ and $2^{o(n)}t \equiv t \pmod n$ is a multicycle $\overline{C}^{\lambda}$ since C is short. It is enough to consider only the case where $t \in \Omega_n$ since we can use $(n-t)C$ instead of tC, if $t > \frac{n-1}{2}$.

If $\lambda = 1$, then tC is a short $o(n)$-cycle.

If $\lambda \geq 2$, let $\overline{C}^{\lambda} = (c_1, c_2, \ldots, c_{o(n)})$ where $2^i t \equiv c_i \pmod n$ for $1 \leq i \leq o(n)$ and $c_{j \cdot o(n)/\lambda + k} = c_k$ for $0 \leq j \leq \lambda - 1$ and $1 \leq k \leq o(n)/\lambda$. There exists an integer r such that $r \cdot o(n)/\lambda + 1 \leq o(n)/2 < (r+1) \cdot o(n)/\lambda$, and so we may assume $tC = (c_{r \cdot o(n)/\lambda + 1}, c_{r \cdot o(n)/\lambda + 2}, \ldots, c_{(r+1) \cdot o(n)/\lambda})$. Since $c_{r \cdot o(n)/\lambda + 1} = 2t$, $c_{o(n)/2} \equiv -t \pmod n$, and $c_{(r+1) \cdot o(n)/\lambda} \equiv t \pmod n$, it would force that $c_{o(n)/2} = c_w \equiv -t \pmod n$, where w is the middle number between the integer interval $[r \cdot o(n)/\lambda + 1, (r+1) \cdot o(n)/\lambda]$. Therefore, we have tC is a short $o(n)/\lambda$-cycle. □

Proposition 3.4. *Let tC be any doubling m-cycle of $G(\Omega_n)$ for some $t \in \mathbb{Z}_n^*$. Then m divides $o(n)$.*

Suppose the length of the base cycle C is $o(n)$. The proof of Proposition 3.4 follows by virtue of Lemma 3.2.

Based on the above results, we further characterize the structure of the graph $G(\Omega_n)$ in Lemma 2.1 as follows.

Theorem 3.5. *Suppose $s_i C$ for $1 \leq i \leq r$ are pairwise distinct doubling cycles with $\bigcup_{i=1}^{r} \partial s_i C = \Omega_n$. Then $G(\Omega_n)$ is the union of $s_i C$ $(1 \leq i \leq r)$.*

4. OPTIMAL TIGHT EQUI-DIFFERENCE CACS OF LENGTH $n = 2^k \pm 1$ AND WEIGHT 3

In this section, we concentrate ourselves on the constructions of optimal tight equi-difference codes $\mathcal{C}$ in $CAC^e(n)$ with $n = 2^k \pm 1$.

Lemma 4.1.

(1) *Suppose $n = 2^k + 1$ for $k \geq 1$. Then $2^k \equiv -1 \pmod n$ and $o(n) = 2k$.*
(2) *Suppose $n = 2^{2q+1} + 1$ for $q \geq 0$. Then $n \equiv 0 \pmod 3$.*
(3) *Suppose $n = 2^{2q} + 1$ for $q \geq 1$. Then $n \not\equiv 0 \pmod 3$.*

By Lemma 4.1 and Proposition 3.1, we have the following consequence.

Proposition 4.2. *Suppose $n = 2^k + 1$, where $k \geq 3$ and $k \equiv 1 \pmod 2$. Then the graph $G(\Omega_n)$ contains an odd k-cycle. In particular, it also contains a 1-cycle.*

Theorem 4.3. *Let $n = 2^k + 1$ for $k \geq 3$. Then there exists an optimal tight equi-difference code $\mathcal{C}$ in $CAC^e(n)$ with $|\mathcal{C}| = M^e(n) = M(n)$ if and only if $k \equiv 0 \pmod 2$.*

Proof. By Proposition 4.2, it is enough to show the sufficient condition. Suppose tC for $t \in \mathbb{Z}_n^*$ is any m-cycle obtained from the base cycle C. By Lemma 4.1, C is short, and by Lemma 3.3, tC is also short. Moreover, we have that $m \mid o(n) = 2k$ by Proposition 3.4.

Claim: $m \nmid k$ and $m \equiv 0 \pmod 4$.

Suppose, on the contrary, that $m \mid k$, say $k = am$ for some positive integer a. Then $2^k \equiv 1^a = 1 \pmod n$, contradicting the fact that $2^k \equiv -1 \pmod n$. Now, since k is even, if m is not a multiple of 4, then $m \mid k$, a contradiction.

By utilizing the fact that $m \equiv 0 \pmod 4$, if tC is full (resp. short), then tC is an even doubling m-cycle (resp. $m/2$-cycle) of $G(\Omega_n)$. This means that all doubling cycles in $G(\Omega_n)$ are even. Note that in this case, $G(\Omega_n)$ contains no 1-cycle since $n \not\equiv 0 \pmod 3$ by Lemma 4.1.

Now, by virtue of Theorem 2.5, there exists an optimal tight equi-difference code $\mathcal{C}$ in $CAC^e(n)$ with $|\mathcal{C}| = M^e(n) = M(n) = \frac{n-1}{4} = 2^{k-2}$. □

Next, we investigate the second case where $n = 2^k - 1$, and get the analogous results like Lemma 4.1.

Lemma 4.4.

(1) *Suppose* $n = 2^k - 1$ *for* $k \geq 3$. *Then* $o(n) = k$ *and* $2^{o(n)/2} \not\equiv -1 \pmod n$ *if* $k \equiv 0 \pmod 2$.
(2) *Suppose* $n = 2^{2q+1} - 1$ *for* $q \geq 1$. *Then* $n \not\equiv 0 \pmod 3$.
(3) *Suppose* $n = 2^{2q} - 1$ *for* $q \geq 1$. *Then* $n \equiv 0 \pmod 3$.

Proposition 4.5. *Suppose* $n = 2^k - 1$ $(k \geq 3)$, *where* $k \equiv 1 \pmod 2$ *or* $k \equiv 0 \pmod 2$ *and* $k \neq 2^p$ *for* $p \geq 2$. *Then the graph* $G(\Omega_n)$ *contains an odd cycle. In particular, if* $k \equiv 0 \pmod 2$, *it also contains a* 1*-cycle.*

Proof. If $k \equiv 1 \pmod 2$, by Lemma 4.4 and Proposition 3.1, we have that the base doubling cycle in $G(\Omega_n)$ is full with odd length k. If $k \equiv 0 \pmod 2$ and $k \neq 2^p$ for $p \geq 2$, we may assume that $k = 2^t q$, where $t \geq 1$ and q is odd with $q \geq 3$, and so $n = 2^k - 1 = 2^{2^t q} - 1 = (2^q - 1)w$ for some integer w.

Consider the multicycle $wC^{k/q}$ given as

$$\begin{aligned} wC^{k/q} &= (2w, 2^2w, \ldots, 2^q w, 2^{q+1}w, \ldots, 2^k w) \pmod n \\ &= (2w, 2^2w, \ldots, w, 2w, \ldots, w) \pmod n \\ &= (c_1, c_2, \ldots, c_k) \pmod n, \end{aligned}$$

where $c_{iq+j} = 2^j w$ and $c_{iq+q} = w$ for $1 \leq j \leq q-1$ and $0 \leq i \leq 2^t - 1$.

Note that $2^q w = (2^q - 1 + 1)w \equiv w \pmod n$. Corresponding to the multicycle $wC^{k/q}$, we have that there is an odd doubling q-cycle wC in $G(\Omega_n)$. □

Theorem 4.6. *Let* $n = 2^k - 1$ *for* $k \geq 3$. *Then there exists an optimal tight equi-difference code* $\mathcal{C}$ *in* $CAC^e(n)$ *with* $|\mathcal{C}| = M^e(n) = M(n)$ *if and only if* $k = 2^p$ *for* $p \geq 2$.

Proof. It suffices to prove the sufficient condition by Proposition 4.5. According to Lemma 4.4, $o(n) = k = 2^p$ for $p \geq 2$. It is clear that the length of each doubling m-cycle in $G(\Omega_n)$ must be even, i.e., exactly one of 1, 2, and a multiple of 4 by Proposition 3.4, and in view of Theorem 2.5, the proof follows. □

Remark. The construction of CAC of length $n = 2^{2^{2p}} - 1$ using a recursive method can be found in [9, 11].

Now, combining Theorem 4.3 with Theorem 4.6, we have the main consequences of this paper, i.e., Theorem 1.1.

ACKNOWLEDGMENTS

The authors would like to appreciate the referees for their useful comments, especially, one of the referees provides some techniques which simplify the proof of Theorem 4.3.

REFERENCES

[1] H. L. Fu, Y. H. Lin, and M. Mishima, Optimal conflict-avoiding codes of even length and weight 3, IEEE Trans Inform Theory 56(11) (2010), 5747–5756.

[2] H. L. Fu, Y. H. Lo, and K. W. Shum, Optimal conflict-avoiding codes of odd length and weight 3, Des Codes Cryptogr (2012), preprint.

[3] L. Györfi and I. Vajda, Constructions of protocol sequences for multiple access collision channel without feedback, IEEE Trans Inform Theory 39(5) (1993), 1762–1765.

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

[5] V. I. Levenshtein, Conflict-avoiding codes for three active users and cyclic triple systems, Probl Inf Transm 43(3) (2007), 199–212.

[6] V. I. Levenshtein and V. D. Tonchev, Optimal conflict-avoiding codes for three active users, Proceedings of the IEEE International Symposium on Information Theory, Adelaide, Australia, 4–9 September 2005, pp. 535–537.

[7] P. Mathys, A class of codes for a T active users out of N multiple-access communication system, IEEE Trans Inform Theory 36(6) (1990), 1206–1219.

[8] M. Mishima, H. L. Fu, and S. Uruno, Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3, Des Codes Cryptogr 52(3) (2009), 275–291.

[9] K. Momihara, Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three, Des Codes Cryptogr 45(3) (2007), 379–390.

[10] K. Momihara, On cyclic $2(k-1)$-support $(n, k)_{k-1}$ difference families, Finite Fields Appl 15 (2009), 415–427.

[11] K. Momihara, M. Müller, J. Satoh, and M. Jimbo, Constant weight conflict-avoiding codes, SIAM J Discrete Math 21(4) (2007), 959–979.

[12] Q. A. Nguyen, L. Györfi, and J. L. Massey, Constructions of binary constant-weight cyclic codes and cyclically permutable codes, IEEE Trans Inform Theory 38(3) (1992), 940–949.

[13] K. W. Shum and W. S. Wong, A tight asymptotic bound on the size of constant-weight conflict-avoiding codes, Des Codes Cryptogr 57(1) (2010), 1–14.

[14] K. W. Shum, W. S. Wong, and C. S. Chen, A general upper bound on the size of constant-weight conflict avoiding codes, IEEE Trans Inform Theory 56(7) (2010), 3265–3276.

[15] B. S. Tsybakov and A. R. Rubinov, Some constructions of conflict-avoiding codes, Probl Inform Transm 38(4) (2002), 268–279.