Des. Codes Cryptogr.
DOI 10.1007/s10623-014-9961-5

Weighted maximum matchings and optimal equi-difference conflict-avoiding codes

Yuan-Hsun Lo · Hung-Lin Fu · Yi-Hean Lin

Received: 7 October 2013 / Revised: 17 March 2014 / Accepted: 19 March 2014

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 $x, y \in \mathcal{C}$ and $x \neq y$, 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 $\mathcal{C} \in$ CAC(n, k) is said to be equi-difference if any codeword $x \in \mathcal{C}$ has the form $\{0, i, 2i, \ldots, (k-1)i\}$. A CAC with maximum size is called optimal. In this paper we propose a graphical characterization of an equi-difference CAC, and then provide an infinite number of optimal equi-difference CACs for weight four.

Keywords Conflict-avoiding code · Equi-difference conflict-avoiding code · Weighted matching

Mathematics Subject Classification 94B25 · 94C15 · 05C70

1 Introduction

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 $\mathbb{Z}_n$. Given a k-subset $x \in \mathcal{P}(n, k)$, we define the *difference set* of x as $\Delta(x) = \{a - b : a, b \in x, a \neq b\}$. Note that $|\Delta(x)| \leq k(k-1)$. A subset $\mathcal{C} \subset \mathcal{P}(n, k)$ is

Communicated by V. D. Tonchev.

Y.-H. Lo (✉)
Department of Mathematics, National Taiwan Normal University, Taipei 116, Taiwan
e-mail: yhlo0830@gmail.com

H.-L. Fu · Y.-H. Lin
Department of Applied Mathematics, National Chiao Tung University, Hsinchu 300, Taiwan
e-mail: hlfu@math.nctu.edu.tw

Y.-H. Lin
e-mail: leona.am96g@g2.nctu.edu.tw

Published online: 03 April 2014

said to be a *conflict-avoiding code*, CAC for short, of length n and weight k if

$$\Delta(x) \cap \Delta(y) = \emptyset \text{ for any } x, y \in \mathcal{C} \text{ with } x \neq y, \tag{1}$$

and each element in $\mathcal{C}$ is called a *codeword*. Since $\Delta(x)$ is symmetric with respect to $\frac{n}{2}$, it is natural to define the *half-difference set* of x as $\Delta_2(x) = \Delta(x) \cap \Omega(n)$, where $\Omega(n) = \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\}$. Then (1) can be rewritten as

$$\Delta_2(x) \cap \Delta_2(y) = \emptyset \text{ for any } x, y \in \mathcal{C} \text{ with } x \neq y. \tag{2}$$

Without loss of generality, we assume that any codeword contains the element 0. For given n and k, let CAC(n, k) denote the class of all CACs of length n and weight k. The maximum size of some code in CAC(n, k) will be denoted by $M(n, k)$. A code $\mathcal{C} \in$ CAC(n, k) is said to be *optimal* if $|\mathcal{C}| = M(n, k)$. For instance, $x = \{0, 3, 6, 9\}$ and $y = \{0, 4, 8, 12\}$ form a CAC of length 16 and weight 4, where $\Delta_2(x) = \{3, 6, 7\}$ and $\Delta_2(y) = \{4, 8\}$. It is easy to verify that $\mathcal{C} = \{x, y\}$ is optimal in CAC(16, 4); that is, $M(16, 4) = 2$.

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 the form $\{0, i, 2i, \ldots, (k-1)i\}$. We denote by $x(i)$ the equi-difference codeword with generator i. Note here that $|\Delta_2(x(i))| \leq k-1$. A code $\mathcal{C} \in$ CAC(n, k) is called *equi-difference* if it entirely consists of equi-difference codewords. Let CAC$^e(n, k)$ denote the class of all the equi-difference codes in CAC(n, k) and $M^e(n, k)$ be the maximum size among CAC$^e(n, k)$. Notice that $M^e(n, k)$ provides a natural lower bound for $M(n, k)$.

A CAC finds its application on a *multiple-access collision channel without feedback*. By identifying each codeword in $\mathcal{C} \in$ CAC(n, k) with a binary protocol sequence of length n and Hamming weight k, the number of code size indicates the number of potential users in such channel. Please refer to [3,5] for more details.

The estimation of $M(n, k)$ or $M^e(n, k)$ has been investigated for years. In the case of weight $k = 3$, the characterization of even length was completely settled by [1,4,6,9], and some optimal (equi-difference) CACs of odd length were studied in [2,7,8,10,15]. Several optimal constructions for weight $k = 4, 5$ can be found in [11]. For general weights, please refer to [13,14].

In this paper, we characterize an equi-difference CAC in terms of a weighted matching (the definition is given later) of a weighted directed graph. By means of weighted matching, we derive an infinite family of optimal equi-difference CACs of weight 4. The main result is

$$M^e(2^c \times 3^d, 4) = \begin{cases} 2^{c-3}(3^d - 1) + M^e(2^c, 4) & \text{if } d \text{ is even, and} \\ 2^{c-3}(3^d - 3) + M^e(3 \times 2^c, 4) & \text{if } d \text{ is odd.} \end{cases}$$

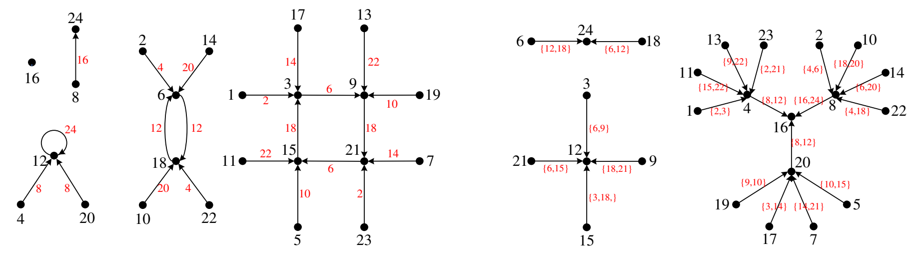
where the closed form of the values $M^e(2^c, 4)$ and $M^e(2^c \times 3, 4)$ are given as well.

The rest of this paper is organized as follows. In Sect. 2, we introduce the notion of weighted matchings. In Sect. 3, we construct an infinite family of optimal equi-difference CACs of weight four. Finally, a brief summary is given in Sect. 4.

2 Graphical representation

For any integers $n > k > 2$, define a weighted directed graph $G(n, k)$ as follows.

- The vertex set is $\Omega(n) = \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$.
- (a, b) is an edge if $b \equiv \pm(k-1)a \pmod{n}$.



(a) **(b)**

Fig. 1 **a** $G(48, 4)$ and **b** $G(48, 5)$

- Delete (if any) the edges $(\frac{n}{t}, \pm\frac{n}{t}(k-1))$ for $t = 2, 3, \ldots, k-1$ if $t|n$ so that each remaining edge represents an equi-difference codeword. Note that any edge $(\frac{n}{t}, \pm\frac{n}{t}(k-1))$ with $2 \leq t \leq k-1$ and $t|n$ has no corresponding codeword.
- Each edge $e = (a, b)$ has a *weight-set* $w(e) = \{\pm 2a, \ldots, \pm(k-1)a\} \cap \Omega(n)$.

Note that every vertex in $G(n, k)$ has at most one out-degree, and the graph $G(n, k)$ may contain loops and multi-edges. Note also that when $k = 3$, the weight-sets are empty and omitted in representation. We say the *closed weight-set* of an edge e, denoted by $w_c(e)$, is the set consists of its weights and two endpoints. Let M be a collection of edges. Denote by $w_c(M)$ the union of all closed weight-sets of edges in M. M is said to be a *weighted matching* if any two involved closed weight-sets are disjoint. Take Fig. 1b as an example, $w_c(1, 4) = \{1, 2, 3, 4\}$, $w_c(8, 16) = \{8, 16, 24\}$, $w_c(5, 20) = \{5, 10, 15, 20\}$, and $w_c(9, 12) = \{9, 12, 18, 21\}$, and these edges form a weighted matching of size 4.

Given a code $\mathcal{C} \in \text{CAC}^e(n, k)$ and a codeword $x(a)$, it is clear that $a \neq \frac{n}{t}$ for $t = 2, 3, \ldots, k-1$ and its half-difference set is the closed weight of the edge (a, b) in $G(n, k)$. On the other hand, the closed weight of an edge in $G(n, k)$ is a translation of the half-difference set of some 'reasonable' equi-difference codeword with length n and weight k. That is, $w_c(a, b) = \Delta_2(x(a))$ if and only if (a, b) is an edge in $G(n, k)$. We then have the following proposition.

Proposition 1 *The size of a maximum weighted matching in* $G(n, k)$ *is* $M^e(n, k)$.

It is worth mentioning that a few known results used this idea to obtain optimal (equi-difference) conflict-avoiding codes, especially when $k = 3$ (see [1,2,4]).

3 Optimal equi-difference CACs of weight four

In this section we only consider weight $k = 4$. For convenience, $\text{CAC}^e(n, 4)$, $M^e(n, 4)$ and $G(n, 4)$ are simply written as $\text{CAC}^e(n)$, $M^e(n)$ and $G(n)$, respectively.

Given $n \geq 2$ an integer. For $a, b \in \Omega(n)$, one can see that if $b \equiv \pm 3a \pmod{n}$, then $2b \equiv \pm 3(2a) \pmod{2n}$, and vice versa. That is, (a, b) is an edge in $G(n)$ if and only if $(2a, 2b)$ is an edge in $G(2n)$. Define $k \times G(n)$ as the graph obtained from $G(n)$ by multiplying the labels of vertices and edges by the integer $k > 0$. Then, we have the following observation.

Proposition 2 *For any positive integer* n, $2 \times G(n)$ *is a subgraph of* $G(2n)$. *Moreover, there is no edge between the subgraph and its complement in* $G(2n)$.

Proof For any odd integer $a \in \Omega(2n)$, it is obvious that $\pm 3a$ must be odd in $\mathbb{Z}_{2n}$. Then there is no edge $(a, b) \in G(2n)$ with b even. Thus the result follows. □

We then derive the following inequality:

$$M^e(n) \leq M^e(2n). \tag{3}$$

3.1 $n = 2^c$ or 3×2^c

In this subsection we provide the exact value $M^e(n)$. Given an integer a and a positive integer n, the *multiplicative suborder* of a modulo n, denoted $\mathsf{sord}_n(a)$, is the smallest positive integer k for which $a^k \equiv \pm 1 \pmod{n}$, or 0 if no such k exists. It is well-known that $\mathsf{sord}_n(a) > 0$ if $\gcd(a, n) = 1$. For example, $\mathsf{sord}_8(3) = 2$, $\mathsf{sord}_{12}(3) = 0$ and $\mathsf{sord}_{16}(3) = 4$. One can find $\mathsf{sord}_n(a)$ in [12]: A003558 for $a = 2$, A103489 for $a = 3$ and A103495 for $a = 9$, for instance. The following is an easy observation.

Proposition 3 *For $c > 1$ we have*

$$\mathsf{sord}_{2^c}(3) = 2^{c-2}.$$

Proof $\mathsf{sord}_4(3) = 1$, $\mathsf{sord}_8(3) = 2$ and $3^2 \not\equiv \pm 1 \pmod{16}$. We now claim by induction that

$$\mathsf{sord}_{2^c}(3) = 2^{c-2} \tag{4}$$

and

$$3^{2^{c-2}} \not\equiv \pm 1 (\bmod 2^{c+1}), \tag{5}$$

for $c \geq 3$.

Let $k = \mathsf{sord}_{2^{c+1}}(3)$. By Eq. (4), let $3^{2^{c-2}} = h \cdot 2^c \pm 1$ for some odd integer h. After squaring both sides we obtain

$$3^{2^{c-1}} = h^2 \cdot 2^{2c} \pm h \cdot 2^{c+1} + 1 \equiv 1 \pmod{2^{c+1}}, \tag{6}$$

which implies that $k \leq 2^{c-1}$. In addition, since $3^k \equiv \pm 1 \pmod{2^{c+1}}$, we have $3^k \equiv \pm 1 \pmod{2^c}$. Therefore, k is an integral multiple of $\mathsf{sord}_{2^c}(3) = 2^{c-2}$. By Eq. (5), we conclude that $k = 2^{c-1}$.

Since h is odd in Eq. (6), $3^{2^{c-1}} \not\equiv 1 \pmod{2^{c+2}}$. Suppose on the contrary that $3^{2^{c-1}} \equiv -1 \pmod{2^{c+2}}$. By Eq. (6), this implies that $3^{2^{c-1}} \equiv 0 \pmod{2^c}$, which is impossible. Hence we complete the proof. □

By above proposition, it is clear that in $G(2^c)$ all the odd vertices form a cycle of length 2^{c-2}. For $i \geq 1$ let C_i be the directed cycle of order i. We now characterize the structure of the graph $G(2^c)$.

Lemma 1 *Let $c \geq 1$. The underlying graph of $G(2^c)$ is composed of an isolated vertex, $C_1, C_2, C_4, \ldots$ and $C_{2^{c-2}}$. Furthermore,*

(1) the isolated vertex is 2^{c-1},
(2) the vertex set of C_{2^i} is exactly $\{t \in \Omega(2^c) : \gcd(t, 2^c) = 2^{c-i-2}\}$, and
(3) all of the vertices of $C_{2^{i-1}}$ appear twice as the edge weights in C_{2^i}, following the order that they obey in $C_{2^{i-1}}$ for $i \geq 1$.

For example, see the C_8 in Fig. 2, the vertex set is $\{t \in \Omega(32) : \gcd(t, 32) = 1\}$, and the weights on the edges are exactly the vertex set of C_4 and repeated in order.

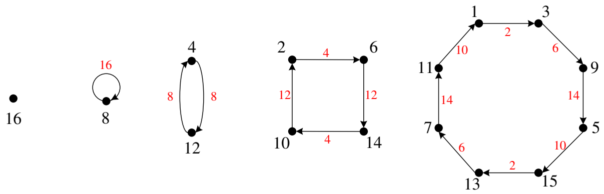


Fig. 2 $G(32)$

Lemma 2 *For $c \geq 2$, we have*

$$M^e(2^c) \leq \begin{cases} \frac{1}{6}(2^c - 3c + 7) & \text{if } c \text{ is odd, and} \\ \frac{1}{6}(2^c - 3c + 8) & \text{if } c \text{ is even.} \end{cases} \tag{7}$$

Proof It is obvious that $M^e(4) = 1$ and $M^e(8) = 1$. Let $c \geq 4$. Suppose for induction that

$$M^e(2^{c-2}) \leq \begin{cases} \frac{1}{6}(2^{c-2} - 3c + 13) & \text{if } c \text{ is odd, and} \\ \frac{1}{6}(2^{c-2} - 3c + 14) & \text{if } c \text{ is even.} \end{cases} \tag{8}$$

Consider the two largest cycles $C_{2^{c-2}}, C_{2^{c-3}}$. Let M be a maximum weighted matching associated with the subgraph $C_{2^{c-2}} \cup C_{2^{c-3}}$. We claim that $|M| \leq 2^{c-3} - 1$. Assume that out of M there are x edges in $C_{2^{c-3}}$. Consider the edges we could choose from $C_{2^{c-2}}$ to keep the weighted matching property of M. By Lemma 1(2), there are $2^{c-2} - 4x$ such edges and each of their weights appears twice. Therefore, we have

$$|M| \leq x + (2^{c-3} - 2x) = 2^{c-3} - x.$$

If $x = 0$, then taking the edges in $C_{2^{c-2}}$ alternately is the only way to attain the equality of $|M| \leq 2^{c-3} - x$, however, this is impossible due to Lemma 1(3). Therefore, we have $|M| \leq 2^{c-3} - 1$ for any $x \geq 0$, and when $x = 0$

$$\begin{aligned} M = &\{(\pm 3^{2i}, \pm 3^{2i+1}) : 0 \leq i \leq 2^{c-4}\} \\ &\cup \{(\pm 3^{2^{c-4}+2i-1}, \pm 3^{2^{c-4}+2i}) : 0 \leq i \leq 2^{c-4}\}, \end{aligned} \tag{9}$$

for example, attains the upper bound of $|M|$. In this case, $M^e(2^c) = |M| + M^e(2^{c-2})$ holds since no edge in M affects the choice of the edges in $\bigcup_{j=0}^{c-4} C_{2^j}$. □

We now derive the following result.

Theorem 1 *For $c \geq 2$, we have*

$$M^e(2^c) = \begin{cases} \frac{1}{6}(2^c - 3c + 7) & \text{if } c \text{ is odd, and} \\ \frac{1}{6}(2^c - 3c + 8) & \text{if } c \text{ is even.} \end{cases}$$

Proof By Lemma 2, it suffices to construct a weighted matching of size attaining the upper bound in Eq. (7). This can be accomplished by greedily choosing $2^{c-3} - 1$ edges from $C_{2^{c-2}}$, $2^{c-5} - 1$ edges from $C_{2^{c-4}}$, and so on. For example, Eq. (9) shows one of the choices of $2^{c-3} - 1$ edges from $C_{2^{c-2}}$. Then we complete the proof. □

We now pay our attention on length $n = 3 \times 2^c$. For $i \geq 1$ let D_i be the directed graph obtained from C_i by appending two vertices to each vertex in C_i. See Fig. 1(a) for example. In D_i, we say an edge (a, b) is a *pendant edge* if a is a leaf and is a *cycle-edge* otherwise. By Proposition 3, we have the structure of $G(3 \times 2^c)$ as follows.

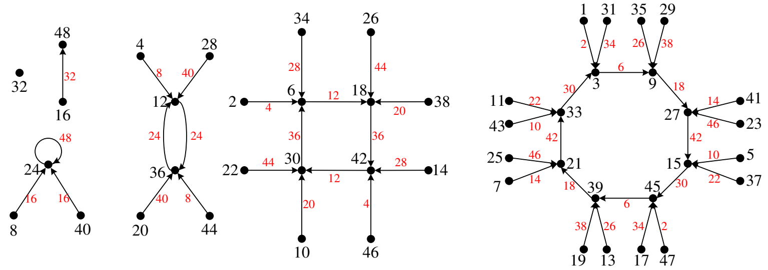


Fig. 3 $G(96)$

Lemma 3 *Let $c \geq 1$. The underlying graph of $G(3 \times 2^c)$ is composed of an isolated vertex, an edge, D_1, D_2, D_4, ... and $D_{2^{c-2}}$. Furthermore,*

(1) the isolated vertex is 2^c, and the unique edge is $(2^{c-1}, 3 \times 2^{c-1})$;
(2) the interior vertex set of D_{2^i} is $\{t \in \Omega(3 \times 2^c) : \gcd(t, 3 \times 2^c) = 3 \times 2^{c-i-2}\}$, all of them appear twice as the weights on cycle-edges of $D_{2^{i+1}}$ in order; and
(3) the set of leaves of D_{2^i} is $\{t \in \Omega(3 \times 2^c) : \gcd(t, 3 \times 2^c) = 2^{c-i-2}\}$, all of them appear twice as the weights on pendant edges of $D_{2^{i+1}}$ in order.

For example, $G(96)$ consists of an isolated vertex 32, an edge $(16, 48)$, D_1, D_2, D_4 and D_8, see Fig. 3.

Lemma 4 *For $c \geq 1$, we have*

$$M^e(3 \times 2^c) \leq \begin{cases} \frac{5}{7}(2^{c-1} - 4) + 3 \text{ if } c \equiv 0 \pmod 3, \\ \frac{5}{7}(2^{c-1} - 1) + 1 \text{ if } c \equiv 1 \pmod 3, \text{ and} \\ \frac{5}{7}(2^{c-1} - 2) + 1 \text{ if } c \equiv 2 \pmod 3. \end{cases} \tag{10}$$

Proof We proceed by induction on c. It is easy to see that $M^e(6) = 1$, $M^e(12) = 1$, $M^e(24) = 3$ and $M^e(48) = 6$. Let $c \geq 5$, and assume that the assertion is true for $c - 3$. Let M be a maximum weighted matching associated with $D_{2^{c-4}} \cup D_{2^{c-3}} \cup D_{2^{c-2}}$, the three largest components of $G(3 \times 2^c)$. We claim that $|M| \leq 5 \cdot 2^{c-4}$, then the result will follow from the fact that $M^e(3 \times 2^c) \leq |M| + M^e(3 \times 2^{c-3})$.

Firstly, among all different kinds of choices of M we claim that there exists one such that M contains 2^{c-2} pendant edges in $D_{2^{c-2}}$. That is, every interior vertex in $D_{2^{c-2}}$ and one of its appending vertices is an edge in M. Note that all such interior vertices are of the form $3u$, where u is odd. Suppose that there does not exist such weighted matching M. We then have two cases as follows.

Case 1. The vertex $3v$, v is odd, is not an endpoint of some edge in M.
Case 2. $(3u, 3v) \in M$ for some odd integers u, v.

Our strategy is to adjust M to match our assumption. For Case 1, let p_1, p_2 be the two leaves adjacent to $3v$. Denote $a_i = w(q_i, 3v)$ for $i = 1, 2$. By Lemma 3(3), one of a_1 and a_2, say a_1, is not a weight of some edge in M. Then, we put $(p_1, 3v)$ into M and remove, if any, the edge $(a_1, t) \in D_{2^{c-3}}$ from M. For Case 2, let $b = w(3u, 3v)$. It can be checked that the two leaves adjacent to the vertex b in $D_{2^{c-3}}$ are exactly the weights on the two edges incident to the vertex $3u$ in $D_{2^{c-2}}$. Let these two edges be e_1 and e_2. Since the two leaves adjacent to b are impossible to be in M, we can add e_1 or e_2 and remove the edge $(3u, 3v)$. As for the vertex $3v$, it follows by going back to Case 1.

Therefore, M contains 2^{c-2} edges in $D_{2^{c-2}}$, and all leaves in $D_{2^{c-3}}$ are used. We assume that M contains x cycle-edges in $D_{2^{c-4}}$ and y cycle-edges in $D_{2^{c-3}}$. Then there are at most $2^{c-4} - 2x - y$ pendant edges in $D_{2^{c-4}}$ contained in M. Thus, we have

$$|M| \leq 2^{c-2} + 2^{c-4} - x \leq 2^{c-2} + 2^{c-4} = 5 \cdot 2^{c-4}.$$

□

Following the proof of Lemma 4, we can choose a weighted matching as follows:

(1) choose 2^{c-2} pendant edges in $D_{2^{c-2}}$,
(2) choose $2^{c-4} - 1$ cycle-edges in $D_{2^{c-3}}$, and
(3) choose 1 pendant edge in $D_{2^{c-4}}$.

Iterating above processes will produce a weighted matching of size attaining the upper bound in Eq. (10). Note that since there are two pendant edges for each interior vertex in $D_{2^{c-5}}$, the chosen pendant edge in $D_{2^{c-4}}$ never affects the choices of edges in $D_{2^{c-5}}$ in the iteration.

Theorem 2 *For $c \geq 1$, we have*

$$M^e(3 \times 2^c) = \begin{cases} \frac{5}{7}(2^{c-1} - 4) + 3 \text{ if } c \equiv 0 \ (\text{mod } 3), \\ \frac{5}{7}(2^{c-1} - 1) + 1 \text{ if } c \equiv 1 \ (\text{mod } 3), \text{ and} \\ \frac{5}{7}(2^{c-1} - 2) + 1 \text{ if } c \equiv 2 \ (\text{mod } 3). \end{cases}$$

Take $G(96)$ as an example, see Fig. 3, we choose (1,3), (35,9), (41,27), (5,15), (17,45), (19,39), (25,21), (11,33) from D_8, choose (6,18) from D_4, choose (20, 16) from D_2, and then choose (8,24) from D_1. These form a weighted matching of size 11, attaining the bound stated in Lemma 4.

3.2 $n = 3^d$

In this subsection we consider the length $n = 3^d$, $d \geq 1$. For $0 \leq i \leq d-1$ let

$$L_i := \{j \in \Omega(3^d) : \gcd(j, 3^d) = 3^i\}.$$

It is clear that $\Omega(3^d) = L_0 \uplus L_1 \uplus \cdots \uplus L_{d-1}$ and the graph $G(3^d)$ is a full 3-ary tree with depth $d-1$ and root 3^{d-1}. More precisely, for $j \in L_i$ with $1 \leq i \leq d-1$, the vertex j has exactly three in-degrees from vertices in L_{i-1}. See Fig. 4 for an example. By viewing the underlying graph of $G(3^d)$ as a bipartite graph with partite sets X and Y, where $|X| \leq |Y|$, we have

$$M^e(3^d) \leq |X| = \begin{cases} (3^{d-2} + 3^{d-4} + \cdots + 3^1) = \frac{1}{8}(3^d - 3) & \text{if } d \text{ is odd, and} \\ (3^{d-2} + 3^{d-4} + \cdots + 3^0) = \frac{1}{8}(3^d - 1) & \text{if } d \text{ is even.} \end{cases} \quad (11)$$

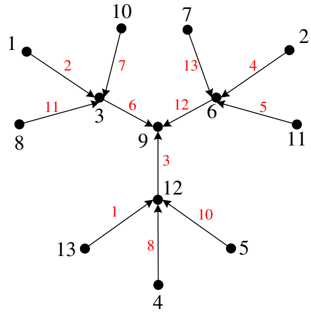
To construct a weighted matching of size reaching the bound in (11), we need more precautions. The following lemma is due to [[2], Lemma 6–7].

Lemma 5 *For $d \geq 1$ we have*

$$\mathsf{sord}_{3^d}(2) = 3^{d-1},$$

and each L_i, $i \geq 0$, forms a directed cycle C_i by defining $j \to j'$ if $j' \equiv \pm 2j$ (mod 3^d). Furthermore, by multiplying all vertices in C_i by 3, we have three copies of C_{i+1}.

Fig. 4 $G(27)$



Take Fig. 4 as an example. The three directed cycles produced from L_0, L_1 and L_2 in $G(27)$ are $\langle 1, 2, 4, 8, 11, 5, 10, 7, 13\rangle$, $\langle 3, 6, 12\rangle$ and $\langle 9\rangle$, respectively. And, $3\langle 1, 2, 4\rangle \equiv 3\langle 8, 11, 5\rangle \equiv 3\langle 10, 7, 13\rangle \equiv \langle 3, 6, 12\rangle$. Now, choose three vertices alternately from the directed cycle of L_0, say $1, 4$ and 11. Since $\gcd(2, 3) = 1$, the three numbers $\pm 3 \cdot 1$, $\pm 3 \cdot 4$ and $\pm 3 \cdot 11$ are distinct modulo 27. Therefore, the three edges $(1, 3)$, $(4, 12)$ and $(11, 6)$ will form a weighted matching in $G(27)$.

Lemma 5 also promises that the directed graph $G(3^d)$ can be obtained recursively from $3 \times G(3^{d-1})$ by appending three vertices to all its leaves. In addition, the set of weights on pendant edges is exactly the set of leaves. We are ready for the following theorem.

Theorem 3 *Let $d \geq 1$ be an integer. Then,*

$$M^e(3^d) = \begin{cases} \frac{1}{8}(3^d - 3) & \text{if } d \text{ is odd, and} \\ \frac{1}{8}(3^d - 1) & \text{if } d \text{ is even.} \end{cases}$$

Proof Because of Eq. (11) it suffices to show that in $G(3^d)$ we can find a weighted matching of size $\frac{1}{8}(3^d - 3)$ if d is odd and $\frac{1}{8}(3^d - 1)$ otherwise. We prove it by induction on d.

It is clear that $M^e(3) = 0$, $M^e(9) = 1$. Let $d \geq 3$. Consider the directed graph $G(3^d)$. Let G be the subgraph of $G(3^d)$ induced by vertex set $L_2 \cup \cdots \cup L_{d-1}$. Since G can be viewed as $9 \times G(3^{d-2})$, in G we can find a weighted matching, say M, of size $\frac{1}{8}(3^{d-2} - 3)$ if d is odd and $\frac{1}{8}(3^{d-2} - 1)$ otherwise. Since each closed weight-set of M is disjoint from $L_0 \cup L_1$, it suffices to find a weighted matching M' of size 3^{d-2} in $L_0 \cup L_1$.

Denote by $C = \langle 1, 2, \ldots\rangle$ the directed cycle produced from L_0 following the relation $i \to j$ if $j \equiv \pm 2i \pmod{3^d}$. Note that $|C| = 3^{d-1}$. Now, alternately pick 3^{d-2} vertices starting from 1 following the direction of C, and denote the set by A. Let

$$M' := \{(a, b) \in G(3^d) : a \in A\}.$$

Pick any two edges $(a_1, b_1), (a_2, b_2) \in M'$. We claim that $w_c(a_1, b_1) \cap w_c(a_2, b_2) = \emptyset$. Since the edge weights $\pm 2a_1, \pm 2a_2$ are respectively the integers on the right of a_1, a_2 in the directed cycle C, they are obviously distinct due to the choice of A. Suppose that $b_1 = b_2$. By Lemma 5, the distance of a_1, a_2 in the directed cycle C is $\frac{|L_0|}{3} = 3^{d-2}$, which is impossible because of the choice of A. Then we conclude that M' is a weighted matching of size 3^{d-2} in $L_0 \cup L_1$. □

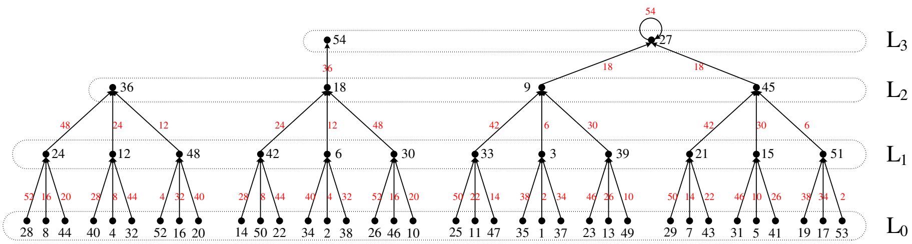


Fig. 5 $G(108)$

3.3 $n = 2^c \times 3^d$

We adopt the notation L_i for $n = 2^c \times 3^d$ by letting

$$L_i := \{j \in \Omega(2^c \times 3^d) : \gcd(j, 3^d) = 3^i\},$$

for $0 \le i \le d$. Note that $|L_d| = 2^{c-1}$ and $|L_i| = 2^c \times 3^{d-1-i}$ for $i < d$. One can see that in $G(2^c \times 3^d)$ all edges are either on L_d or lying across two adjacent layers L_i, L_{i+1} for some $i < d$. More precisely, the induced directed graph of L_d is isomorphic to $3^d \times G(2^c)$, and each of the other edges (out of L_d) is from its tail in L_i to its head in L_{i+1} for some $i < d$. See Fig. 5 for an example. In fact, $G(2^c \times 3^d)$ has a *hierarchy property*:

> The induced directed graph of L_d is isomorphic to $3^d \times G(2^c)$, of $L_{d-1} \cup L_d$ is isomorphic to $3^{d-1} \times G(3 \times 2^c)$, of $L_{d-2} \cup L_{d-1} \cup L_d$ is isomorphic to $3^{d-2} \times G(3^2 \times 2^c)$, and so on.

By considering the underlying graph of $G(2^c \times 3^d)$ as a bipartite graph, we have

$$M^e(2^c \times 3^d) \le \begin{cases} |L_1| + |L_3| + \cdots + |L_{d-1}| + M^e(2^c) & \text{if } d \text{ is even}, \\ |L_1| + |L_3| + \cdots + |L_{d-2}| + M^e(3 \times 2^c) & \text{if } d \text{ is odd}, \end{cases}$$
$$= \begin{cases} 2^{c-3}(3^d - 1) + M^e(2^c) & \text{if } d \text{ is even}, \\ 2^{c-3}(3^d - 3) + M^e(3 \times 2^c) & \text{if } d \text{ is odd}. \end{cases} \tag{12}$$

In what follows we shall construct a weighted matching of $G(2^c \times 3^d)$ to attain the bound in Eq. (12). To do this, we have to study the structure of $G(2^c \times 3^d)$ in more detail. By the hierarchy property of $G(2^c \times 3^d)$, every vertex in L_i, for $1 \le i \le d-1$, is of in-degree 3 and every vertex in L_0 is of in-degree 0. For $i = 0, 1$ and $0 \le j \le c$ let

$$L_{i(j)} := \{x \in L_i : \gcd(x, 2^c) = 2^j\}.$$

Obviously, any vertex in $L_{0(j)}$ can be expressed as $a \times 2^j$ for some a with $\gcd(a, 6) = 1$ and vertex in $L_{1(j)}$ can be expressed as $b \times 3 \times 2^j$ for some b with $\gcd(b, 6) = 1$.

Lemma 6 *Consider the induced directed graph of $L_0 \cup L_1$ in $G(2^c \times 3^d)$.*

(1) All edges are lying across $L_{0(j)}$ and $L_{1(j)}$.
(2) The set of edge weights between $L_{0(j)}$ and $L_{1(j)}$ is exactly $L_{0(c)}$ for $j = c-1, c$.
(3) The multiset of edge weights between $L_{0(j)}$ and $L_{1(j)}$ is exactly $L_{0(j+1)} \cup L_{0(j+1)}$ (i.e., each member in $L_{0(j+1)}$ appears twice) for $j = 0, 1, \ldots, c-2$.
(4) Let x, y, z be the weights of three edges incident to some vertex $v \in L_{1(j)}$. Then x, y, z appear together as vertices adjacent to the some vertex v', where $v' \in L_{1(j+1)}$ if $j < c$ and $v' \in L_{1(j)}$ if $j = c$.

Proof (1) Suppose that the two vertices $x = a \times 2^j \in L_{0(j)}$ and $y = b \times 3 \times 2^{j'} \in L_{1(j')}$ are adjacent for some $j, j' \leq c$ and a, b with $\gcd(a, 6) = \gcd(b, 6) = 1$. We assume that $j > j'$ due to symmetry. Since $\pm 3x \equiv y \pmod{2^c \times 3^d}$, one has $\pm a \times 2^{j-j'} \equiv b \pmod{2^{c-j'} \times 3^{d-1}}$, which implies that $\gcd(a \times 2^{j-j'}, 2^{c-j'} \times 3^{d-1}) = \gcd(b, 2^{c-j'} \times 3^{d-1}) = 1$. Hence we have $j = j'$.

(2)–(3) For $x \in L_{0(j)}$, it is not hard to see that $\pm 2x$ is in $L_{0(j)}$ if $j = c$ and $L_{0(j+1)}$ otherwise. Then (2) and (3) follow from (1) and the size of each $L_{0(j)}$.

(4) We only consider the case for $j < c$ as the $j = c$ case can be dealt with in the same way. Since x, y, z are edge weights, $x \equiv \pm 2x'$, $y \equiv \pm 2y'$ and $z \equiv \pm 2z' \pmod{2^c \times 3^d}$ for some $x', y', z' \in L_{0(j)}$. By the argument in (2)–(3), x, y, z are vertices in $L_{0(j+1)}$. Moreover, $x \equiv \pm 2x'$ and $\pm 3x' \equiv v$ implies that $\pm 3x \equiv 2v \pmod{2^c \times 3^d}$, that is, x is adjacent to $\pm 2v$. Similarly, y and z are adjacent to $\pm 2v$ as well. Hence we complete the proof. □

We are ready for the main result.

Theorem 4 *Let $c, d \geq 0$. There exists a weighted matching of $G(2^c \times 3^d)$ of size attaining the bound in Eq. (12). That is,*

$$M^e(2^c \times 3^d) = \begin{cases} 2^{c-3}(3^d - 1) + M^e(2^c) & \text{if } d \text{ is even, and} \\ 2^{c-3}(3^d - 3) + M^e(3 \times 2^c) & \text{if } d \text{ is odd.} \end{cases}$$

Proof By induction on d. Theorems 1 and 2 are the two cases when $d = 0$ and 1, respectively. Let $d \geq 2$. Consider $G(2^c \times 3^d)$. Denote by G the induced directed graph of $L_2 \cup \cdots \cup L_d$. Since, by the hierarchy property, G is isomorphic to $3^2 \times G(2^c \times 3^{d-2})$, assume that in G we can find a weighted matching, say M, of size

$$|M| = \begin{cases} 2^{c-3}(3^{d-2} - 1) + M^e(2^c) & \text{if } d \text{ is even, and} \\ 2^{c-3}(3^{d-2} - 3) + M^e(3 \times 2^c) & \text{if } d \text{ is odd.} \end{cases}$$

By the hierarchy property, it remains to find a weighted matching of size $2^c \times 3^{d-2}$ among the induced directed graph of $L_0 \cup L_1$.

Denote by G' the induced directed graph of $L_0 \cup L_1$. For $j \geq 0$ denote by G'_j the induced directed graph of $L_{0(j)} \cup L_{1(j)}$. By Lemma 6(1), we have

$$G' = \biguplus_{j=0}^{c} G'_j.$$

For each j we shall find a weighted matching M'_j of size $|L_{1(j)}|$ in G'_j such that $w_c(M'_{j_1}) \cap w_c(M'_{j_2}) = \emptyset$ whenever $j_1 \neq j_2$. By Lemma 6(2)–(3), for any two edges $e_1 \in G'_{j_1}$ and $e_2 \in G'_{j_2}$, if $|j_1 - j_2| > 1$, then $w_c(e_1)$ and $w_c(e_2)$ must be disjoint. Therefore, we only need to ensure that $w_c(M'_j) \cap w_c(M'_{j-1}) = \emptyset$ for $j = c, c-1, \ldots, 1$ in the process of construction.

At first, consider the case of $j = c$. Observe that G'_c is isomorphic to the outer 2-layers of $G(3^d)$ by multiplying 2^c, so we can construct M'_c by following the proof of Theorem 3. As for $j = c - 1$, pick any vertex v in $L_{1(c-1)}$ and consider the three edges with the same head v.

By Lemma 6(2) and 6(4), there exists one edge on which the weight does not appear in $w_c(M'_c)$. Therefore, we can find the desired weighted matching M'_{c-1}. Formally, let

$$M'_{c-1} = \{e \in G'_{c-1} : w(e) \in L_{0(c)} \backslash w_c(M'_c)\}.$$

Finally, we shall construct M'_{j-1} from M'_j for j from $c-1$ to 1. Let v be any vertex in $L_{1(j)}$ and (x, v), (y, v), (z, v) be the three edges in G'_j. By Lemma 6(3)–(4), there are exactly two vertices $v_1, v_2 \in L_{1(j-1)}$ such that x, y, z are their edge weights in G'_{j-1} and there is no other edge in G'_{j-1} having weight x, y or z. Since only one of x, y, z is used in M'_j, we can always find edges e_1 and e_2 incident to v_1 and v_2 respectively such that $w_c(e_1) \cap w_c(e_2) = \emptyset$. By the same fashion, we can successfully find a weighted matching M'_{j-1} of size $|L_{1(j-1)}|$ in G'_{j-1} with $w_c(M'_j) \cap w_c(M'_{j-1}) = \emptyset$.

Then the desired weighted matching of G' is

$$M' = M'_c \cup M'_{c-1} \cup \cdots \cup M'_0,$$

whose cardinality is

$$|L_{1(c)}| + |L_{1(c-1)}| + \cdots + |L_{1(0)}| = |L_1| = 2^c \times 3^{d-2}.$$

Thus we complete the proof. □

See Fig. 5 for an example to illustrate the method of finding M'. Following the proof of Theorem 3, M'_2 can be chosen as $\{(4, 12), (16, 48), (44, 24)\}$. Then $\{(14, 42), (34, 6), (26, 30)\}$ is the only choice for M'_1 to ensure the closed weight-sets of M'_2 and M'_1 are disjoint.

Finally, M'_0 can be defined as $\{(11, 33), (29, 21), (1, 3), (19, 51), (49, 39), (31, 15)\}$.

4 Concluding remarks

In this paper, we apply the newly defined weighted matching to evaluate the maximum size of an equi-difference CACs with weight 4. For $n = 2^c \times 3^d$, we have the exact value $M^e(n, 4)$. We believe that this approach can be utilized to determine more other cases.

Acknowledgments The authors would like to express their gratitude to the referees for their valuable comments and suggestions in improving the presentation of this paper. Partially supported by National Science Council, Taiwan under grants NSC 101-2115-M-390-004-MY3 (Y. H. Lo) and NSC 100-2115-M-009-005-MY3 (H. L. Fu and Y. H. Lin).

References

1. Fu H.L., Lin Y.H., Mishima M.: Optimal conflict-avoiding codes of even length and weight 3. IEEE Trans. Inf. Theory **56**(11), 5747–5756 (2010).
2. Fu H.L., Lo Y.H., Shum K.W.: Optimal conflict-avoiding codes of odd length and weight three. Des. Codes Cryptogr. 1–21 (2012). doi:10.1007/s10623-012-9764-5.
3. Györfi L., Vajda I.: Constructions of protocol sequences for multiple access collision channel without feedback. IEEE Trans. Inf. Theory **39**(5), 1762–1765 (1993).
4. 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. Inf. Theory **53**(8), 2732–2742 (2007).
5. Levenshtein V.I.: Conflict-avoiding codes and cyclic triple systems. Probl. Inf. Transm. **43**(3), 199–212 (2007).
6. Levenshtein V.I., Tonchev V.D.: Optimal conflict-avoiding codes for three active users. In: Proceedings of IEEE Internation Symposium on Information Theory, Adelaide, Australia. pp. 535–537. (2005).
7. Lin Y., Mishima M., Satoh J., Jimbo M.: Optimal equi-difference conflict-avoiding codes of odd length and weight three. Finite Fields Appl. **26**, 49–68 (2014).
8. Ma W., Zhao C., Shen D.: New optimal constructions of conflict-avoiding codes of odd length and weight 3. Des. Codes Cryptogr. 1–14 (2013). doi:10.1007/s10623-013-9827-2.
9. 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).

10. Momihara K.: Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three. Des. Codes Cryptogr. **45**(3), 379–390 (2007).
11. Momihara K., Müller M., Satoh J., Jimbo M.: Constant weight conflict-avoiding codes. SIAM J. Discret. Math. **21**(4), 959–979 (2007).
12. The OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences. http://oeis.org.
13. Shum K.W., Wong W.S., Chen C.S.: A general upper bound on the size of constant-weight conflict-avoiding codes. IEEE Trans. Inf. Theory **56**(7), 3265–3276 (2010).
14. 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).
15. Wu S.L., Fu H.L.: Optimal tight equi-difference conflict-avoiding codes of length $n = 2^k \pm 1$ and weight 3. J. Comb. Des. **21**(6), 223–231 (2013).