Science in China Series A: Mathematics
Mar., 2008, Vol. 51, No. 3, 416–426
www.scichina.com math.scichina.com
www.springerlink.com

A new combinatorial approach to the construction of constant composition codes

YIN JianXing[†] & TANG Yu

Department of Mathematics, Suzhou University, Suzhou 215006, China
(email: jxyin@suda.edu.cn, ytang@suda.edu.cn)

Abstract Constant composition codes (CCCs) are a new generalization of binary constant weight codes and have attracted recent interest due to their numerous applications. In this paper, a new combinatorial approach to the construction of CCCs is proposed, and used to establish new optimal CCCs.

Keywords: constant composition code, optimal, combinatorial approach, construction

MSC(2000): 05B05, 94B25

1 Introduction

Let $Q = \{a_t : 0 \leqslant t \leqslant q-1\}$ be an alphabet of q elements. Most of the time Q are taken to be the finite field GF(q) of order q or the ring of integers modulo q. By an $(n, M, d; q)$-code we mean a q-ary code $C \subseteq Q^n$ with length n, size M and Hamming distance d. If C consists of the codewords of a given constant weight w, it is termed an $(n, M, d, w; q)$-CWC. An $(n, M, d; q)$-code is called a constant composition code (CCC), or an $(n, M, d, [w_0, w_1, \dots, w_{q-1}]; q)$-CCC, if for any i $(0 \leqslant i \leqslant q-1)$, the symbol a_i appears exactly w_i times in every codeword. CCCs are a new generalization of binary constant weight codes, which include the important permutation codes. Here, the constant composition $[w_0, \dots, w_{q-1}]$ is essentially an unordered multiset. We will write it in an "exponential" form for more convenience. The notation $[1^i 2^j 3^k \cdots]$ denotes i occurrences of 1, j occurrences of 2, etc. in the constant composition.

The maximum size of an $(n, M, d, [w_0, w_1, \dots, w_{q-1}]; q)$-CCC is denoted by $A(n, d, [w_0, w_1, \dots, w_{q-1}]; q)$. A CCC achieving this size is often called optimal. To measure the optimality, the following two known bounds serve as our benchmarks.

Lemma 1[1]. *If* $nd - n^2 + (w_0^2 + w_1^2 + \cdots + w_{q-1}^2) > 0$, *then*

$$A(n, d, [w_0, \dots, w_{q-1}]; q) \leqslant \frac{nd}{nd - n^2 + (w_0^2 + \cdots + w_{q-1}^2)}. \tag{1}$$

Lemma 2[2]. *For any integer* r *satisfying* $0 \leqslant r \leqslant q-1$,

$$A(n, d, [w_0, \dots, w_{q-1}]; q) \leqslant \frac{n}{w_r} A(n-1, d, [\widehat{w_0}, \dots, \widehat{w_{q-1}}]; q), \tag{2}$$

Received August 20, 2007; accepted October 22, 2007
DOI: 10.1007/s11425-008-0036-9

[†] Corresponding author

This work was supported by the National Natural Foundation of China (Grant Nos. 10671140, 10626038)

where

$$\widehat{w_i} = \begin{cases} w_i - 1, & \textit{if } i = r \\ w_i, & \textit{if } i \neq r. \end{cases}$$

CCCs have been used since the early 1980's to bound error and erasure probabilities in decision feedback channels[3], their systematic study only began in late 1990's with Svanström[4]. Today, the constructions of optimal CCCs have attracted extensive attention due to their numerous applications (see, for example [1, 2, 5–11]). In this paper, a new combinatorial approach to the construction of CCCs is proposed and used to establish new optimal CCCs.

2 The combinatorial approach

We use [12] and [13] as our standard design-theoretic references.

Suppose that there is a set X of v points and that from these a collection $\mathcal{A}$ of subsets (called blocks) is drawn. The ordered pair $(X, \mathcal{A})$ is then referred to as a design of order v. In design theory there are normally a number of additional rules imposed when the blocks are selected.

A design $(X, \mathcal{A})$ is termed a packing, or a $\mathrm{P}(k, 1; v)$, if all of its blocks have size k and every pair of distinct points occurs in at most one block of $\mathcal{A}$. Furthermore, if $v = gn$ and there exists a partition $\mathcal{H}$ of X into n subsets (called holes) of cardinality g such that no block contains two distinct points of any hole, that is, $|H \cap B| \leqslant 1$ for any block $B \in \mathcal{A}$ and any hole $H \in \mathcal{H}$, then the $\mathrm{P}(k, 1; v)$ is known as a holey packing (HP) or an $\mathrm{HP}(k, 1; g^n)$[14]. In this case, we write $(X, \mathcal{H}, \mathcal{A})$ instead of $(X, \mathcal{A})$. In literature, if every pair of distinct points from distinct holes occurs in exactly one block, then $(X, \mathcal{H}, \mathcal{A})$ is called a group divisible design (GDD), or a k-GDD of type g^n in short. A k-GDD of type g^n can exist only if $n \geqslant k$, $(n-1)g \equiv 0 \pmod{k-1}$ and $n(n-1)g^2 \equiv 0 \pmod{k(k-1)}$. For the sake of uniformity, the term "holey packing" is understood to include the GDD case.

There exists an ultimate relationship between combinatorial designs and codes. It is well known (see, for example, [15]) that the row vectors of the "blocks-by-points" incidence matrix of a $\mathrm{P}(k, 1; v)$ with b blocks form a binary CWC with the parameters $(n = v, M = b, d = 2(k-1), w = k)$. Conversely, the support design of an $(n, M, d, w; 2)$-CWC is a $\mathrm{P}(k, 1; v)$. It was also shown that an $\mathrm{HP}(k, 1; g^n)$ gives an $(n, M = b, d, w = k; q = g + 1)$-CWC over Z_{g+1} for a certain d with $k - 1 \leqslant d \leqslant 2k$, and vice versa (see [16] for GDD case and [17, 18] for general holey packings). Recently, various constructions of CCCs were established by using combinatorial designs such as generalized doubly resolvable designs, PBDs, difference families and so on (see, for example, [5, 8–10, 19] and the references therein).

Since the codewords of the derived $(g + 1)$-ary code from an $\mathrm{HP}(k, 1; g^n)$ are of constant weight k, each of its codewords contains the symbol $0 \in Z_{g+1}$ exactly $n - k$ times. This obvious fact motivates us to propose a new combinatorial approach to constructing optimal CCCs by employing grid holey packings (GHPs) defined below.

Let k, g, n and w_i $(1 \leqslant i \leqslant g)$ be positive integers such that $k = \sum_{i=1}^{g} w_i$. Let X be a set of ng points which admits two partitions $\mathcal{R}$ and $\mathcal{H}$ where

- $\mathcal{R} = \{R_1, R_2, \dots, R_g\}$ is a partition of X into g subsets (called restricted groups) of cardinality n; and

- $\mathcal{H} = \{H_1, H_2, \ldots, H_n\}$ is a partition of X into n subsets (called holes) of cardinality g such that

$$|H_i \cap R_j| = 1, H_i \in \mathcal{H}, R_j \in \mathcal{R}.$$

A grid holey packing, or a $\mathrm{GHP}([w_1, \ldots, w_g], 1; n \times g)$ is defined to be a quadruple $(X, \mathcal{H}, \mathcal{R}, \mathcal{A})$, where $\mathcal{A}$ is a collection of k-subsets (called blocks) of X such that

- every pair of distinct points of X occurs in at most one block; and
- for any block $B \in \mathcal{A}$, i $(1 \leqslant i \leqslant n)$ and j $(1 \leqslant j \leqslant g)$,

$$|H_i \cap B| \leqslant 1 \text{ and } |R_j \cap B| = w_j.$$

By definition, one can see that a $\mathrm{GHP}([w_1, \ldots, w_g], 1; n \times g)$ is an $\mathrm{HP}(k, 1; g^n)$ with $k = \sum_{i=1}^{g} w_i$ which satisfies certain additional rules. The "grid" nomenclature arises from that one can lay out the ng points in $n \times g$ grid, the points on the j-th vertical line being the points of the j-th restricted group R_j, the points on the ith horizontal line being the points of the ith hole H_i.

We are now ready to describe our approach to obtaining CCCs via GHPs.

Theorem 1. *If a* $\mathrm{GHP}([w_1, \ldots, w_g], 1; n \times g)$ *with* b *blocks exists, then so does an* $(n, M, d, [w_0, w_1, \ldots, w_g]; g+1)$*-CCC for a certain* $d \in [k-1, 2k]$ *where* $M = b$ *and* $w_0 = n - \sum_{i=1}^{g} w_i$.

Proof. Let $(X, \mathcal{H}, \mathcal{R}, \mathcal{A})$ be the given $\mathrm{GHP}([w_1, \ldots, w_g], 1; n \times g)$. Since X is a finite set, we may assume that $X = I_n \times I_g$ (if necessary, we may relabel the ng points), where $I_m = \{1, 2, \ldots, m\}$, $\mathcal{H} = \{H_i = \{i\} \times I_g : i \in I_n\}$ and $\mathcal{R} = \{R_j = I_n \times \{j\} : j \in I_g\}$. By definition, the size of the blocks in the GHP is equal to $k = \sum_{i=1}^{g} w_i$. Write $w_0 = n - \sum_{i=1}^{g} w_i = n - k$. Now for any block

$$B = \{(i_1, j_1), (i_2, j_2), \ldots, (i_k, j_k)\},$$

we form a codeword $c(B)$ having value j_t in its i_t-th position $(1 \leqslant t \leqslant k)$ and value zero in any other position. Since the j-th restrict group intersects every block at exactly w_j points for any $j \in I_g$, the derived code $C = \{c(B) : B \in \mathcal{A}\}$ is an $(n, M = b, d, [w_0, w_1, \ldots, w_g]; q = g+1)$-CCC over the alphabet Z_{g+1}. Obviously, the distance d of the derived CCC lies in the interval $[k-1, 2k]$.

It is remarkable that the distance d of the derived CCC from a GHP cannot be determined uniquely by the parameters of the GHP. It might be any value between $k-1$ and $2k$, depending on heavily how the blocks cut across the holes in the given GHP. We use the subscript d in the notation to indicate this. So, the notation $\mathrm{GHP}_d([w_1, \ldots, w_g], 1; n \times g)$ stands for a GHP whose corresponding CCC has distance $d \in [k-1, 2k]$. In this case, the GHP must satisfy one more property than a normal GHP so that its derived CCC has distance d. We refer to this extra property as "distance property" of the GHP.

From Theorem 1, we see that a maximum $\mathrm{GHP}_d([w_1, \ldots, w_g], 1; n \times g)$ gives us an optimal $(n, M, d, [w_0, w_1, \ldots, w_g]; g+1)$-CCC with $M = b$ and $w_0 = n - \sum_{i=1}^{g} w_i$. The process in the proof of Theorem 1 can be reversed. For convenience, we call a maximum $\mathrm{GHP}_d([w_1, \ldots, w_g], 1; n \times g)$ optimal for any fixed $d \in [k-1, 2k]$ and use prefix "O" to denote it. It follows that we may restate Theorem 1 as follows.

Theorem 2. *For any $d \in [k-1, 2k]$, the existence of an* $\mathrm{OGHP}_d([w_1, \dots, w_g], 1; n \times g)$ *is equivalent to that of an optimal* $(n, M, d, [w_0, w_1, \dots, w_g]; g+1)$-CCC *with* $M = b$ *and* $w_0 = n - \sum_{i=1}^{g} w_i$.

To illustrate the idea in Theorem 2, we give a simple example.

Example 1. Take $V = I_5 \times I_2$, $\mathcal{H} = \{H_i = \{i\} \times I_2 : i \in I_5\}$ and $\mathcal{R} = \{R_j = I_5 \times \{j\} : j \in I_2\}$. Let $\mathcal{A}$ consist of the following 5 blocks over V:

$$\begin{aligned}&\{(1,1),(2,1),(4,2)\},\\&\{(2,1),(3,1),(5,2)\},\\&\{(3,1),(4,1),(1,2)\},\\&\{(4,1),(5,1),(2,2)\},\\&\{(5,1),(1,1),(3,2)\}.\end{aligned}$$

Then $(V, \mathcal{H}, \mathcal{R}, \mathcal{A})$ is an $\mathrm{OGHP}_4([2,1], 1; 5 \times 2)$. Applying Theorem 2, this OGHP gives an optimal $(5, 5, 4, [2,2,1]; 3)$-CCC over alphabet Z_3 shown in Table 1.

Table 1

Blocks	Corresponding Codewords
$\{(1,1),(2,1),(4,2)\}$	1 1 0 2 0
$\{(2,1),(3,1),(5,2)\}$	0 1 1 0 2
$\{(3,1),(4,1),(1,2)\}$	2 0 1 1 0
$\{(4,1),(5,1),(2,2)\}$	0 2 0 1 1
$\{(5,1),(1,1),(3,2)\}$	1 0 2 0 1

3 The application

The equivalence in Theorem 2 translates the construction of optimal CCCs into a combinatorial problem. As a consequence, design-theoretic techniques can be utilized. Combinatorial design theory is mature and widely applied today. It is beyond doubt that new classes of optimal CCCs can be produced through the use of Theorem 2. This section serves to provide new optimal CCCs by applying Theorem 2.

3.1 New optimal ternary CCCs

Svanström[11] made an investigation into optimal ternary CCCs with weight 3. He proved that

$$A(n, 4, [n-3, 2, 1]; 3) \leqslant \begin{cases} \dfrac{n(n-2)}{4}, & \text{if } n \text{ is even;} \\ \dfrac{n(n-1)}{4}, & \text{if } n \equiv 1 \pmod 4; \\ \dfrac{(n-1)^2}{4} + \left\lfloor \dfrac{n-3}{12} \right\rfloor, & \text{if } n \equiv 3 \pmod 4; \end{cases} \tag{3}$$

and

$$A(n, 4, [n-3, 2, 1]; 3) = \begin{cases} \dfrac{n(n-2)}{4}, & \text{if } n \text{ is even;} \\ \dfrac{(n-1)^2}{4}, & \text{if } n = 7 \text{ or } 11. \end{cases}$$

The determination of $A(n, 4, [n-3, 2, 1]; 3)$ remains unsettled for all odd $n \notin \{7, 11\}$. Recently, Chee et al.[19] gave a nice PBD-closure result for the set of lengths of certain types of CCCs and proved that the above upper bound (3) is attainable for all $n \equiv 1 \pmod 4$. Applying Theorem 2, we may state their result in the following

Lemma 3. *For all positive integers t, there exists an* $\mathrm{OGHP}_4([2,1], 1; (4t+1) \times 2)$ *of* $(4t+1)t$ *blocks.*

As noted in [19], the case $n \equiv 3 \pmod 4$ seems considerably more difficult. Based on a PBD result, Chee et al.[19] showed that the upper bound (3) is also attainable for sufficiently large $n \equiv 3 \pmod 4$. The term "sufficiently large" remains to be specified. We will address the case $n \equiv 3 \pmod{12}$. Employing Theorem 2, our task is to construct an $\mathrm{OGHP}_4([2,1], 1; n \times 2)$ with $b = \frac{(n-1)^2}{4} + \lfloor \frac{n-3}{12} \rfloor$ blocks. It is not difficult to see that the distance property of an $\mathrm{OGHP}_4([2,1], 1; n \times 2)$ reads as: "any two of its blocks cut across at most one common hole if they share a point in common, and at most two common holes if they are disjoint".

Our construction uses the notion of a transversal design (TD). A $\mathrm{TD}(k, m)$ is a k-GDD of type m^k. From the pointview of existence, a $\mathrm{TD}(k, m)$ is equivalent to $k-2$ mutually orthogonal Latin squares of side m. Here, we only need a $\mathrm{TD}(3, m)$ from a Latin square of side m, which exists for any positive integers m (see, for example, [13]). We describe a TD(3, 3) in the following example for convenience of later use.

Example 2. Take $X = Z_3 \times \{x, y, z\}$ to be point set, and $\{Z_3 \times \{x\}, Z_3 \times \{y\}, Z_3 \times \{z\}\}$ as hole set. Then the following 9 blocks give a TD(3,3):

$$\{(0,x),(0,y),(0,z)\} \text{ mod } (3,-);$$
$$\{(0,x),(1,y),(2,z)\} \text{ mod } (3,-);$$
$$\{(0,x),(2,y),(1,z)\} \text{ mod } (3,-).$$

Here, $\{x, y, z\}$ is an arbitrary triple.

Theorem 3. *Let t be a positive integer and $n = 12t+3$. Then there exists an* $\mathrm{OGHP}_4([2,1], 1; n \times 2)$ *with* $\frac{(n-1)^2}{4} + \lfloor \frac{n-3}{12} \rfloor$ *blocks, or equivalently, an optimal* $(n, M, 4, [n-3, 2, 1]; 3)$-CCC *meeting the Svanström's bound* (3).

Proof. We give the proof by constructing an $\mathrm{OGHP}_4([2,1], 1; n \times 2)$ for any given positive integer $n = 12t + 3$.

Let $(G \times I_2, \mathcal{H}, \mathcal{R}, \mathcal{A})$ be an $\mathrm{OGHP}_4([2,1], 1; (4t+1) \times 2)$ with $(4t+1)t$ blocks of the form $\{(x,1),(y,1),(z,2)\}$ $(x, y, z \in G)$, which exists by Lemma 3. Here, the hole set $\mathcal{H}$ consists of $4t+1$ holes $H_g = \{g\} \times I_2$ $(g \in G)$ and $\mathcal{R}$ consists of the two restricted groups $R_j = G \times \{j\}$ $(j \in I_2)$. For the ease of notation, we write g_j for the point $(g, j) \in G \times I_2$.

Now weight 3 to every point $(g, j) \in G \times I_2$ of the given OGHP, that is, replace every point (g, j) with a set $(Z_3 \times \{g\})_j$ of 3 points. This forms a new point set $X = (Z_3 \times G) \times I_2$, where its point (i, g, j) is written as $(\{i\} \times \{g\})_j$. Let

$$\begin{cases} X = (Z_3 \times G) \times I_2, \\ \widehat{\mathcal{H}} = \{\{\alpha\} \times I_2 : \alpha \in Z_3 \times G\}, \\ \widehat{\mathcal{R}} = \{(Z_3 \times G) \times \{j\} : j \in I_2\}. \end{cases}$$

Next, suppose that $A = \{x_1, y_1, z_2\} \in \mathcal{A}$ is a block of the given OGHP. We employ the TD(3, 3) shown in Example 2 to construct 9 blocks over X from A as follows:

$$\begin{array}{lll} \{(i,x)_1, & (i,y)_1, & (i,z)_2\}; \\ \{(i,x)_1, & (1+i,y)_1, & (2+i,z)_2\}; \\ \{(i,x)_1, & (2+i,y)_1, & (1+i,z)_2\}, \end{array}$$

where i runs over all residues in Z_3 and the addition is reduced by mod 3. Denote by $\mathcal{B}(A)$ these 9 blocks. Doing this for each of $(4t+1)t$ blocks in $\mathcal{A}$ produces $9t(4t+1)$ blocks over X. Let

$$\mathcal{D} = \{\{(0,g)_1, (1,g)_1, (2,g)_2\} : g \in G\}.$$

Write

$$\widehat{\mathcal{A}} = \mathcal{D} \bigcup \Big(\bigcup_{A \in \mathcal{A}} \mathcal{B}(A) \Big).$$

Then $\widehat{\mathcal{A}}$ contains exactly $(4t+1)(9t+1) = \frac{(n-1)^2}{4} + \lfloor \frac{n-3}{12} \rfloor$ blocks over X. It can be easily proved that $(X, \widehat{\mathcal{H}}, \widehat{\mathcal{R}}, \widehat{\mathcal{A}})$ is a GHP$([2,1],1;n\times 2)$ of $\frac{(n-1)^2}{4} + \lfloor \frac{n-3}{12} \rfloor$ blocks, matching the Svanström's bound (3).

To see that the resultant GHP is an OGHP$_4([2,1],1;n\times 2)$, as desired, we need to show that it satisfies the distance property mentioned above. For this, suppose that B_1 and B_2 are the two distinct blocks of $\widehat{\mathcal{A}}$. Note that the holes of the resultant GHP is labelled by the elements of $Z_3 \times G$ while any block A of the given OGHP meets every hole $\{g\} \times I_2 \in \mathcal{H}$ at most one point. It turns out that if $B_1 \in \mathcal{D}$ and $B_2 \in \mathcal{B}(A)$ for some $A \in \mathcal{A}$, then B_1 and B_2 cut across at most one hole of $\widehat{\mathcal{H}}$ in common. When B_1 and B_2 both lie in $\mathcal{B}(A)$ for some $A \in \mathcal{A}$, the case is the same as above, which is guaranteed by the property of a TD.

What remains is to treat the cases $B_1 \in \mathcal{B}(A_1)$ and $B_2 \in \mathcal{B}(A_2)$ where A_1 and A_2 are two distinct blocks of the given OGHP. Let $A_1 = \{a_1, c_1, g_2\}$ and $A_2 = \{b_1, d_1, h_2\}$. Since any two distinct blocks of $\mathcal{A}$ intersect in at most one point, we have $\{a,c\} \neq \{b,d\}$. If $\{a,c\} \cap \{b,d\} = \emptyset$, then B_1 and B_2 clearly cut across at most one hole of $\widehat{\mathcal{H}}$ in common from our construction. When $|\{a,c\} \cap \{b,d\}| = 1$, we may assume that $a = b$ without loss of generality. Then $\{c,g\} \cap \{d,h\} = \emptyset$, as A_1 and A_2 satisfy the distance property in the given OGHP. Hence, the distance property is also true for B_1 and B_2 in this case.

From Theorem 2, the resultant OGHP gives an optimal $(n, M, 4, [n-3,2,1]; 3)$-CCC meeting the Svanström's bound (3).

Example 3. Take $t = 1$ in Theorem 3. Start with the OGHP$_4([2,1],1;5\times 2)$ $(V, \mathcal{H}, \mathcal{R}, \mathcal{A})$ given in Example 1. Applying Theorem 3, we get an OGHP$_4([2,1],1;15\times 2)$ $(X, \widehat{\mathcal{H}}, \widehat{\mathcal{R}}, \widehat{\mathcal{A}})$. Here

$$\begin{cases} X = (Z_3 \times I_5) \times I_2, \\ \widehat{\mathcal{H}} = \{\{\alpha\} \times I_2 : \alpha \in Z_3 \times I_5\}, \\ \widehat{\mathcal{R}} = \{(Z_3 \times I_5) \times \{j\} : j \in I_2\}. \end{cases}$$

Label the five blocks of $\mathcal{A}$ in the following way:

$$A_1 = \{1_1, 2_1, 4_2\}, \quad A_2 = \{2_1, 3_1, 5_2\}, \quad A_3 = \{3_1, 4_1, 1_2\},$$
$$A_4 = \{4_1, 5_1, 2_2\}, \quad A_5 = \{5_1, 1_1, 3_2\}.$$

Then, according to the construction in the proof of Theorem 3, the block set

$$\widehat{\mathcal{A}} = \mathcal{D} \bigcup \Big(\bigcup_{r=1}^{5} \mathcal{B}(A_r) \Big)$$

containing exactly $\frac{(15-1)^2}{4} + \lfloor \frac{15-3}{12} \rfloor = 50$ blocks over X. We indicate the blocks of $\mathcal{B}(A_r)$ $(1 \leqslant r \leqslant 5)$ and $\mathcal{D}$ in Table 2.

Table 2

$\mathcal{B}(\mathcal{A}_1)$	$\{(0,1)_1,(0,2)_1,(0,4)_2\}$	$\{(1,1)_1,(1,2)_1,(1,4)_2\}$	$\{(2,1)_1,(2,2)_1,(2,4)_2\}$
	$\{(0,1)_1,(1,2)_1,(2,4)_2\}$	$\{(1,1)_1,(2,2)_1,(0,4)_2\}$	$\{(2,1)_1,(0,2)_1,(1,4)_2\}$
	$\{(0,1)_1,(2,2)_1,(1,4)_2\}$	$\{(1,1)_1,(0,2)_1,(2,4)_2\}$	$\{(2,1)_1,(1,2)_1,(0,4)_2\}$
$\mathcal{B}(A_2)$	$\{(0,2)_1,(0,3)_1,(0,5)_2\}$	$\{(1,2)_1,(1,3)_1,(1,5)_2\}$	$\{(2,2)_1,(2,3)_1,(2,5)_2\}$
	$\{(0,2)_1,(1,3)_1,(2,5)_2\}$	$\{(1,2)_1,(2,3)_1,(0,5)_2\}$	$\{(2,2)_1,(0,3)_1,(1,5)_2\}$
	$\{(0,2)_1,(2,3)_1,(1,5)_2\}$	$\{(1,2)_1,(0,3)_1,(2,5)_2\}$	$\{(2,2)_1,(1,3)_1,(0,5)_2\}$
$\mathcal{B}(A_3)$	$\{(0,3)_1,(0,4)_1,(0,1)_2\}$	$\{(1,3)_1,(1,4)_1,(1,1)_2\}$	$\{(2,3)_1,(2,4)_1,(2,1)_2\}$
	$\{(0,3)_1,(1,4)_1,(2,1)_2\}$	$\{(1,3)_1,(2,4)_1,(0,1)_2\}$	$\{(2,3)_1,(0,4)_1,(1,1)_2\}$
	$\{(0,3)_1,(2,4)_1,(1,1)_2\}$	$\{(1,3)_1,(0,4)_1,(2,1)_2\}$	$\{(2,3)_1,(1,4)_1,(0,1)_2\}$
$\mathcal{B}(A_4)$	$\{(0,4)_1,(0,5)_1,(0,2)_2\}$	$\{(1,4)_1,(1,5)_1,(1,2)_2\}$	$\{(2,4)_1,(2,5)_1,(2,2)_2\}$
	$\{(0,4)_1,(1,5)_1,(2,2)_2\}$	$\{(1,4)_1,(2,5)_1,(0,2)_2\}$	$\{(2,4)_1,(0,5)_1,(1,2)_2\}$
	$\{(0,4)_1,(2,5)_1,(1,2)_2\}$	$\{(1,4)_1,(0,5)_1,(2,2)_2\}$	$\{(2,4)_1,(1,5)_1,(0,2)_2\}$
$\mathcal{B}(A_5)$	$\{(0,5)_1,(0,1)_1,(0,3)_2\}$	$\{(1,5)_1,(1,1)_1,(1,3)_2\}$	$\{(2,5)_1,(2,1)_1,(2,3)_2\}$
	$\{(0,5)_1,(1,1)_1,(2,3)_2\}$	$\{(1,5)_1,(2,1)_1,(0,3)_2\}$	$\{(2,5)_1,(0,1)_1,(1,3)_2\}$
	$\{(0,5)_1,(2,1)_1,(1,3)_2\}$	$\{(1,5)_1,(0,1)_1,(2,3)_2\}$	$\{(2,5)_1,(1,1)_1,(0,3)_2\}$
$\mathcal{D}$	$\{(0,1)_1,(1,1)_1,(2,1)_2\}$	$\{(0,2)_1,(1,2)_1,(2,2)_2\}$	$\{(0,3)_1,(1,3)_1,(2,3)_2\}$
	$\{(0,4)_1,(1,4)_1,(2,4)_2\}$	$\{(0,5)_1,(1,5)_1,(2,5)_2\}$	

From Theorem 2, this OGHP gives an optimal $(15, 50, 4, [12, 2, 1]; 3)$-CCC over alphabet Z_3, meeting the Svanström's bound (3).

The construction of an OGHP$_4([2,1], 1; (12t+3) \times 2)$ in Theorem 3 relies on a known OGHP$_4([2,1], 1; (4t+1) \times 2)$. However, when $t = 2m+1$ and $4t+1 = 8m+5 > 5$ is a prime power, we can explicitly construct an OGHP$_4([2,1], 1; n \times 2)$ with $n = 12t+3 = 24m+15$ in the following manner.

Let $C_j^{(4)}$ $(0 \leqslant j \leqslant 3)$ be the cyclotomic classes of order 4 in the Galois field GF$(8m+5)$. The linear relations of cyclotomic numbers of order 4 listed in [20, p. 28] show that the equations $1 + Y = X$ with $\{X, Y\} \subseteq C_3^{(4)}$ and $1 + Y = X$ with $Y \in C_2^{(4)}$ and $X \in C_1^{(4)}$ are both solvable in GF$(8m+5)$. Hence, we can take x, y and u in GF$(8m+5)$ in such a way that

$$x \in C_1^{(4)}, y \in C_2^{(4)}, \{u, u-1\} \subseteq C_3^{(4)} \text{ and } x - y = 1 \in C_0^{(4)}.$$

Now we take

$$\begin{cases} X = (\mathrm{GF}(8m+5) \times Z_3) \times I_2, \\ \mathcal{H} = \{\{\alpha\} \times I_2 : \alpha \in \mathrm{GF}(8m+5) \times Z_3\}, \\ \mathcal{R} = \{(\mathrm{GF}(8m+5) \times Z_3) \times \{j\} : j \in I_2\}, \end{cases}$$

and simply write $(a,b)_j$ for the point $(a,b,j) \in X$ as before. Consider the following blocks over X:

$$\begin{aligned}A_{1s} &= \{(2s,0)_1,(-2s,0)_1,(0,1)_2\};\\ A_{2s} &= \{(s,0)_1,(us,0)_1,(0,2)_2\};\\ A_{3s} &= \{(xs,0)_1,(ys,1)_1,(0,2)_2\},\end{aligned}$$

where s runs over all quartic residues of $C_0^{(4)}$. For any $s \in C_0^{(4)}$ and any r $(1 \leqslant r \leqslant 3)$, denote by $\mathcal{A}_{rs}$ the block-orbit spanned by the block A_{rs} under the action of the additive group of $\mathrm{GF}(8m+5) \times Z_3$, that is,

$$\mathcal{A}_{rs} = \{A_{rs} + (g,i) : (g,i) \in \mathrm{GF}(8m+5) \times Z_3\}.$$

Here, $(a,b)_j + (g,i) = (a+g,b+i)_j$ for any $(a,b)_j \in X$ and $(g,i) \in \mathrm{GF}(8m+5) \times Z_3$. Let

$$\mathcal{B} = \{\{(g,0)_1,(g,1)_1,(g,2)_2\} : g \in \mathrm{GF}(8m+5)\}$$

be the block-orbit of length $8m+5$. Let

$$\mathcal{A} = \mathcal{B}\bigcup\Big(\bigcup_{1\leqslant r\leqslant 3}\Big(\bigcup_{s\in C_0^{(4)}}\mathcal{A}_{rs}\Big)\Big).$$

It can be proved that $(X,\mathcal{H},\mathcal{R},\mathcal{A})$ is an $\mathrm{OGHP}_4([2,1],1;n\times 2)$.

3.2 Optimal quaternary CCCs of constant composition $[(n-3)^1 1^3]$ and $d=4$

From Lemma 2, it is easy to show (see [19]) that

$$A(n,4,[(n-3)^1 1^3];4) \leqslant n\left\lfloor\frac{n-1}{2}\right\rfloor. \tag{4}$$

An optimal $(n,M,4,[(n-3)^1 1^3];4)$-CCC with $M = n\left\lfloor\frac{n-1}{2}\right\rfloor$ was shown in [19] to exist for all sufficiently large integers n. As before, the term "sufficiently large" remains to be specified. Applying Theorem 2, such a CCC can be obtained from an $\mathrm{OGHP}_4([1^3],1;n\times 3)$ of $n\left\lfloor\frac{n-1}{2}\right\rfloor$ blocks.

The distance property of an $\mathrm{OGHP}_4([1^3],\ 1;\ n\times 3)$ is the same as that of an $\mathrm{OGHP}_4([2,1],1;n\times 2)$ mentioned above. A simple counting argument shows that every point of an $\mathrm{OGHP}_4([1^3],1;n\times 3)$ occurs in exactly $r = \lfloor (n-1)/2 \rfloor$ blocks. So, if we delete the three points in a certain hole and the $3((n+1)-1)/2$ truncated blocks from an $\mathrm{OGHP}_4([1^3],1;(n+1)\times 3)$ with n even, then the derived design is an $\mathrm{OGHP}_4([1^3],1;n\times 3)$ of

$$(n+1)n/2 - 3n/2 = n(n-2)/2$$

blocks, matching the bound (4). We state this fact in the following lemma, which was first presented in [19].

Lemma 4. *Let n be an even positive integer. If an* $\mathrm{OGHP}_4([1^3],1;(n+1)\times 3)$ *exists, then so does an* $\mathrm{OGHP}_4([1^3],1;n\times 3)$.

In view of Lemma 4, to construct an $\mathrm{OGHP}_4([1^3],1;n\times 3)$ for arbitrary length n, it suffices for us to treat the case where n is odd. We first develop a composite construction below.

Lemma 5. *Let m and n be odd positive integers. If an* $\mathrm{OGHP}_4([1^3],1;n\times 3)$ *and an* $\mathrm{OGHP}_4([1^3],\ 1;m\times 3)$ *both exist, then so does an* $\mathrm{OGHP}_4([1^3],1;mn\times 3)$.

Proof. This proof is analogous to that of Theorem 3. Let $(G\times I_3,\mathcal{H},\mathcal{R},\mathcal{A})$ be an $\mathrm{OGHP}_4([1^3],$ $1;n\times 3)$ given in the hypothesis. Then it contains $n(n-1)/2$ blocks of the form

$$\{(x,1),(y,2),(z,3)\}\ (x,y,z\in G).$$

As in the proof of Theorem 3, we replace every point $(g,j)\in G\times I_3$ of this OGHP with a set $(Z_m\times\{g\})_j$ of m points. This forms a new point set $X=(Z_m\times G)\times I_3$, where its point (i,g,j) is written as $(\{i\}\times\{g\})_j$. Let

$$\begin{cases} X=(Z_m\times G)\times I_3,\\ \widehat{\mathcal{H}}=\{\{\alpha\}\times I_3:\alpha\in Z_m\times G\},\\ \widehat{\mathcal{R}}=\{(Z_m\times G)\times\{j\}:j\in I_3\}. \end{cases}$$

Now employing the same technique as in the proof of Theorem 3, for any block $A=\{x_1,y_2,z_3\}\in\mathcal{A}$ we use a TD$(3,m)$ over $Z_m\times\{x,y,z\}$ to construct m^2 blocks over X, denoted by $\mathcal{B}(A)$. Doing this for each of $n(n-1)/2$ blocks of $\mathcal{A}$ produces $m^2n(n-1)/2$ blocks over X. Next, let

$$((Z_m\times\{g\})\times I_3,\mathcal{H}(g),\mathcal{R}(g),\mathcal{A}(g))$$

be an $\mathrm{OGHP}_4([1^3],1;m\times 3)$ of $m(m-1)/2$ blocks given in the hypothesis, where $g\in G$. Write

$$\widehat{\mathcal{A}}=\Big(\bigcup_{A\in\mathcal{A}}\mathcal{B}(A)\Big)\bigcup\Big(\bigcup_{g\in G}\mathcal{A}(g)\Big).$$

Then $\widehat{\mathcal{A}}$ contains exactly

$$m^2n(n-1)/2+nm(m-1)/2=mn(mn-1)/2$$

blocks, matching the bound (4) for length mn. We claim that $(X,\widehat{\mathcal{H}},\widehat{\mathcal{R}},\widehat{\mathcal{A}})$ is an $\mathrm{OGHP}_4([1^3],1;$ $mn\times 3)$, as desired. Its proof is identical to that of Theorem 3 and omitted here.

The next lemma provides a direct construction of an $\mathrm{OGHP}_4([1^3],1;n\times 3)$.

Lemma 6. *Let $(G,+)$ be an Abelian group of order n. Suppose that n is odd and $3\nmid n$. Then there exists an* $\mathrm{OGHP}_4([1^3],1;n\times 3)$ *over $X=G\times I_3$ of $n\lfloor\frac{n-1}{2}\rfloor$ blocks provided that there exists a partition of $G\setminus\{0\}$ into two subsets S and T of cardinality $t=(n-1)/2$ such that $T=-S=2S$, where $-S=\{-x:x\in S\}$ and $2S=\{2x=x+x:x\in S\}$.*

Proof. Take $H_g=\{g\}\times I_3,g\in G$, as the holes and $R_j=G\times\{j\},j\in I_3$, as the restricted groups. Write $\mathcal{R}=\{R_1,R_2,R_3\}$ and $\mathcal{H}=\{H_g:g\in G\}$. Let $\mathcal{A}$ consist of the following $nt=n(n-1)/2$ blocks:

$$B_{xd}=\{(d,1),(d+x,2),(d-x,3)\},$$

where x runs over all t elements of S and $d\in G$. By the mixed difference method introduced by Bose[21], we see that $(X,\mathcal{H},\mathcal{R},\mathcal{A})$ is a $\mathrm{GHP}([1^3],1;n\times 3)$ of $nt=n\lfloor\frac{n-1}{2}\rfloor$ blocks. To prove that this design is an $\mathrm{OGHP}_4([1^3],1;n\times 3)$, we have to show that any two of the above nt blocks cut across at most one common hole if they share a common point, and at most two common holes if they are disjoint. Suppose that B_{xg} and B_{yh} are the two distinct blocks for arbitrary elements $x, y \in S$ and $d \in G$.

We first consider the case where B_{xg} and B_{yh} intersect at a certain point.

Case 1. $g = h$

In this case, the two blocks B_{xg} and B_{yh} intersect at the point $(g, 1) = (h, 1)$. As any pair of distinct points occurs in at most one block by our construction, we have $g + x \neq h + y$ and $g - x \neq h - y$. By assumption, $\{x, y\} \subseteq S$ and $\{-x, -y\} \subseteq T$. Hence, $g + x \neq h - y$ and $g - x \neq h + y$. So, these two blocks cut across exactly one common hole H_g.

Case 2. $g + x = h + y$

In this case, the two blocks share a point $(g + x, 2) = (h + y, 2)$ in common. This implies $g \neq h$ and $g - x \neq h - y$. As in Case 1, we need only to show that $g \neq h - y$ and $h \neq g - x$. But the condition $g + x = h + y$ means that $x - y = h - g$. So, if $g = h - y$, then we would have $2y = x \in S \cap T = \emptyset$, a contradiction. Similarly, we can derive a contradiction if $h = g - x$.

Case 3. $g - x = h - y$

In this case, B_{xg} and B_{yh} intersect at the point $(g - x, 3) = (h - y, 3)$. The proof is identical to the proof of Case 2.

Now we consider the case where the two blocks B_{xg} and B_{yh} are disjoint. In this case, it is sufficient to show that the two sets $S_1 = \{g, g + x, g - x\}$ and $S_2 = \{h, h + y, h - y\}$ are not identical. Since $B_{xg} \cap B_{yh} = \emptyset$, $g \neq h,\ g + x \neq h + y$ and $g - x \neq h - y$. Thus, if $S_1 = S_2$, then the system of equations

$$\begin{cases} g = h + y, \\ g + x = h - y, \\ g - x = h, \end{cases} \quad \text{or} \quad \begin{cases} g = h - y, \\ g + x = h, \\ g - x = h + y \end{cases}$$

must be solvable with $x, y \in S$ and $g, h \in G$. This leads to

$$y = -x - y = x \text{ or } -y = x + y = -x.$$

We would have $3x = 3y = 0$, which is impossible as $3 \nmid n$ by assumption. Therefore, $S_1 \neq S_2$.

Applying Lemma 6 we obtain the following lemma.

Lemma 7. *Suppose that* $n \equiv 3 \pmod 8$ *is a prime power and* $3 \nmid n$. *Then there exists an* $\mathrm{OGHP}_4([1^3], 1; n \times 3)$, *or equivalently, an optimal* $(n, M, 4, [(n-3)^1 1^3]; 4)$-CCC *meeting the bound* (4).

Proof. Take G to be the additive group of $\mathrm{GF}(n)$. Take $S = C_0^{(2)}$ and $T = C_1^{(2)}$ to be the sets of all quadratic nonzero residues and quadratic non-residues in $\mathrm{GF}(n)$, respectively. Then S and T form a partition of $\mathrm{GF}(n)^*$. Since $n \equiv 3 \pmod 8$, both 2 and -1 are quadratic non-residues in $\mathrm{GF}(n)$. So $T = -S = 2S$. The conclusion then follows from applying Theorem 2 and Lemma 6.

As an immediate consequence of Lemma 5 and Lemma 7, we have the following series of optimal CCCs.

Theorem 4. *Suppose that* $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ *where* $p_i \equiv 3 \pmod 8$ *is a prime greater than* 3 *for* $1 \leqslant i \leqslant t$. *Then there exists an* $\mathrm{OGHP}_4([1^3], 1; n \times 3)$, *or equivalently, an optimal* $(n, M, 4, [(n-3)^1 1^3]; 4)$-CCC *meeting the bound* (4).

Applying Lemma 4 and Theorem 4, we have also the following series of optimal CCCs.

Theorem 5. *Suppose that* $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ *where* $p_i \equiv 3 \pmod 8$ *is a prime greater than* 3 *for* $1 \leqslant i \leqslant t$. *Then there exists an* $\mathrm{OGHP}_4([1^3], 1; (n-1) \times 3)$, *or equivalently, an optimal* $(n, M, 4, [(n-3)^1 1^3]; 4)$-CCC *meeting the bound* (4).

We point out at this stage that the main purpose of this paper is to introduce a feasible combinatorial approach to obtaining optimal CCCs. To our best knowledge, this approach is different from the known ones used in constructions of CCCs. We have illustrated the application of this approach to two types of optimal CCCs in this section. Though the construction of an $\mathrm{OGHP}_d([w_1, \ldots, w_g], 1; n \times g)$ is apparently often highly technical and requires deep methods in combinatorial theory, we believe that the approach taken in this paper will result in some more types of optimal CCCs.

References

1 Luo Y, Fu F W, Han Vinck A J, et al. On constant composition codes over Z_q. *IEEE Trans Inform Theory*, **49**(11): 3010–3016 (2003)

2 Svanström M, Östergard P R J, Bogdanova G T. Bounds and constructions for ternary constant-composition codes. *IEEE Trans Inform Theory*, **48**(1): 101–111 (2002)

3 Csiszar I, Kornner J. Information Theory: Coding Theorems for Discrete Memoryless Channels. New York: Academic Press, 1981

4 Svanström M. Ternary codes with weight constraints. PhD dissertation. Sweden: Linköpings University, 1999

5 Chu W, Colbourn C J, Dukes P. On constant composition codes. *Discrete Appl Math*, **154**: 912–929 (2006)

6 Chu W, Colbourn C J, Dukes P. Tables for constant composition codes. *J Combin Math Combin Comput*, **54**: 57–65 (2005)

7 Ding C, Yin J. Algebraic constructions of constant composite codes. *IEEE Trans Inform Theory*, **51**(4): 1585–1589 (2005)

8 Ding C, Yin J. Combinatorial constructions of optimal constant composition codes. *IEEE Trans Inform Theory*, **51**(10): 3671–3674 (2005)

9 Ding C, Yin J. A construction of optimal constant composition codes. *Des Codes Cryptogr*, **40** (2): 157–165 (2006)

10 Ding C, Yuan J. A family of optimal constant-composition codes. *IEEE Trans Inform Theory*, **51**(10): 3668–3671 (2005)

11 Svanström M. Construction of ternary constant-composition codes with weight three. *IEEE Trans Inform Theory*, **46**(7): 2644–2647 (2000)

12 Beth T, Jungnickel D, Lenz H. Design Theory. Cambridge: Cambridge University Press, 1999

13 Colbourn C J, Dinitz J H. The CRC Handbook of Combinatorial Designs. Boca Raton: CRC Press, 2007

14 Yin J. Packing designs with equal-sized holes. *J Statist Plann Inference*, **94**: 393–403 (2001)

15 MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes (Part I). Amsterdam: North-Holland Publishing Company, 1977

16 Etzion T. Optimal constant weight codes over Z_k and generalized designs. *Discrete Math*, **169**: 55–82 (1997)

17 Yin J, Lu Y, Wang J. Maximum distance holey packings and related codes. *Sci China Ser A-Math*, **42**: 1262–1269 (1999)

18 Yin J. A survey on maximum distance holey packings. *Discrete Appl Math*, **121**: 279–294 (2002)

19 Chee Y M, Ling A C H, Ling S, et al. The PBD-closure of constant-composition codes. *IEEE Trans Inform Theory*, **53**(8): 2685–2692 (2007)

20 Storer T. Cyclotomy and Difference Sets. Chicago: Markhan, 1967

21 Bose R C. On the construction of balanced incomplete block designs. *Ann Eugenics*, **9**: 353–399 (1939)