Constructions of Optimal and Near-Optimal Multiply Constant-Weight Codes

Yeow Meng Chee, *Senior Member, IEEE*, Han Mao Kiah, Hui Zhang, and Xiande Zhang

***Abstract*— Multiply constant-weight codes (MCWCs) have been recently studied to improve the reliability of certain physically unclonable function response. In this paper, we give combinatorial constructions for the MCWCs, which yield several new infinite families of optimal MCWCs. Furthermore, we demonstrate that the Johnson-type upper bounds of the MCWCs are asymptotically tight for fixed Hamming weights and distances. Finally, we provide bounds and constructions of the 2-D MCWCs.**

***Index Terms*— Multiply constant-weight codes, physically unclonable functions, generalized packing designs, two dimensional multiply constant-weight codes.**

I. Introduction

A MULTIPLY constant-weight code (MCWC) is a binary code of length mn where each codeword is partitioned into m equal parts and has Hamming weight exactly w in each part [1], [2]. This notion therefore generalizes the definition of *constant-weight codes* (where $m = 1$) and a subclass of *doubly constant-weight codes* (where $m = 2$), introduced by Johnson [3] and Levenshteĭn [4].

Multiply constant-weight codes have attracted recent attention due to an application in the design of certain *physically unclonable functions* (PUFs) [1], [2], [5]. Introduced by Pappu *et al.* [6], PUFs provide innovative low-cost authentication methods that are derived from complex physical characteristics of electronic devices and have recently become an attractive option to provide security in low cost devices such as RFIDs and smart cards [5]–[8]. Reliability and implementation considerations on programmable circuits for the design of Loop PUFs [5] lead to the study of multiply constant-weight codes.

If we arrange each codeword of an MCWC as an $m \times n$ array, then an MCWC can be regarded as a code over binary matrices, where each matrix has constant row weight w. Furthermore, if certain weight constraints are also satisfied by all columns, we obtain *two-dimensional weight-constrained codes* that are used in the design of optical storage in holographic memory [9], and have possible applications in next generation memory technologies based on crossbar arrays of resistive devices, such as memristors [10]. Recently, these codes were also studied by Chee *et al.* [11] due to an application in power line communications.

The theory of MCWC is at a rudimentary stage. Chee *et al.* [1] established certain preliminary upper and lower bounds for possible sizes of MCWCs. In particular, they extended techniques of Johnson [3] to derive certain upper bounds and showed that these bounds are asymptotically tight to a constant factor. However, the only nontrivial infinite class of optimal codes was constructed from Reed-Solomon codes under the conditions that $n/w \geq mw - 1$ is a prime power and distance $d \geq 2m(w-1)+2$.

In this paper, we continue this study and provide constructions of optimal or near-optimal MCWCs based on combinatorial techniques. Our main contributions are as follows:

(i) determining completely the maximum sizes of MCWCs with total weight four and distance four;
(ii) constructing infinite families of optimal MCWCs with distance four and weight two or three in each part;
(iii) establishing that the Johnson type upper bounds are asymptotically tight for fixed weights and distances.

Our paper is organized as follows. In Section II, we give necessary definitions and notations, where a more general concept of MCWCs with different lengths and weights in different parts is introduced. Section III links the general MCWCs to generalized packing designs, a class of combinatorial objects recently studied by Bailey and Burgess [12]. By establishing the existence of optimal generalized packing designs, we completely determine the maximum sizes of MCWCs with total weight four and distance four. Combining results in [12], the maximum sizes of MCWCs with total weight less than or equal to four are determined except for only one small case. Section IV gives a product construction of MCWCs with equal length and equal weight in each part. Based on the existence of large sets of optimal packings, this construction yields infinite families of optimal MCWCs with distance four and weight two or three in each part. Section V exhibits that the Johnson type upper bounds of general MCWCs are asymptotically tight for fixed weights and distances by applying a theorem on fractional matchings due to Kahn [13]. This improves

Manuscript received October 20, 2014; revised June 7, 2016; accepted November 23, 2016. Date of publication April 3, 2017; date of current version May 18, 2017. X. Zhang was supported by the National Natural Science Foundation of China under Grant 11301503. *(Corresponding author: Xiande Zhang.)*

Y. M. Chee and H. M. Kiah are with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371 (e-mail: ymchee@ntu.edu.sg; hmkiah@ntu.edu.sg).

H. Zhang was with the Nanyang Technological University, Singapore 637371. She is now with the Department of Computer Science, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: hzhang.chn@gmail.com).

X. Zhang is with the School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China (e-mail: drzhangx@ustc.edu.cn).

Communicated by S. ten Brink, Associate Editor for Communications.

Digital Object Identifier 10.1109/TIT.2017.2690450

the previous result in [1] which states that the bounds are asymptotically tight to a constant factor and for a smaller class of MCWCs. Finally in Section VI, we formally define the notion of two dimensional MCWCs and provide several bounds and constructions.

II. Preliminaries

Given a positive integer n, the set $\{1, 2, \ldots, n\}$ is denoted by $[n]$, and the ring $\mathbb{Z}/n\mathbb{Z}$ is denoted by $\mathbb{Z}_n$.

Through out this paper, let X be a finite set of size N. Then $\{0,1\}^X$ denotes the set of all binary vectors of length N, where each component of a vector $\mathsf{u} \in \{0,1\}^X$ is indexed by an element of X, that is, $\mathsf{u} = (\mathsf{u}_x)_{x\in X}$, and $\mathsf{u}_x \in \{0,1\}$ for each $x \in X$.

A *binary code of length* N is a set $\mathcal{C} \subseteq \{0,1\}^X$ for some X of size N. The elements of $\mathcal{C}$ are called *codewords*. The *Hamming weight* of a vector $\mathsf{u} \in \{0,1\}^X$ is given by the number of nonzero coordinates in u. Endow the space $\{0,1\}^X$ with the *Hamming distance* metric, denoted d_H, so that $d_H(\mathsf{u},\mathsf{v}) = |\{x \in X : \mathsf{u}_x \neq \mathsf{v}_x\}|$, for $\mathsf{u},\mathsf{v} \in \{0,1\}^X$. A code $\mathcal{C}$ is said to have (minimum Hamming) *distance* d if $d_H(\mathsf{u},\mathsf{v}) \geq d$ for all distinct $\mathsf{u},\mathsf{v} \in \mathcal{C}$, denoted by (N,d) code. The largest size of an (N,d) code is denoted by $A(N,d)$.

Suppose that $X_1, X_2, \ldots, X_m$ is a partition of X with $|X_i| = n_i$, $i \in [m]$. Clearly, $N = n_1 + \cdots + n_m$. Define $\mathbf{X} = (X_1, X_2, \ldots, X_m)$ and $\mathbf{n} = (n_1, n_2, \ldots, n_m)$. For any vector $\mathsf{u} \in \{0,1\}^X$, define the *support of* u *associated with* $\mathbf{X}$ as $\mathrm{supp}(\mathsf{u})_{\mathbf{X}} = (U_1, U_2, \ldots, U_m)$, where $U_i = \{x \in X_i : \mathsf{u}_x = 1\}$. If the subscript $\mathbf{X}$ is omitted, then $\mathrm{supp}(\mathsf{u}) = \cup_{i\in[m]} U_i$ is the usual support set.

Let $\mathbf{x} = (x_1, \ldots, x_m)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ be two m-tuples of nonnegative integers. We write $\mathbf{x} \leq \mathbf{y}$ to mean that $x_i \leq y_i$ for all $i \in [m]$. For any integer k, use the notation $\binom{X}{k}$ to denote the set of all k-subsets of X. Suppose $\mathbf{w} = (w_1, w_2, \ldots, w_m)$ is an m-tuple of integers such that $\mathbf{w} \leq \mathbf{n}$. Let $W \triangleq w_1 + \cdots + w_m$. Define

$$\binom{\mathbf{X}}{\mathbf{w}} = \binom{X_1}{w_1} \times \binom{X_2}{w_2} \times \cdots \times \binom{X_m}{w_m},$$

that is, a member of $\binom{\mathbf{X}}{\mathbf{w}}$ is an m-tuple of sets, of sizes $(w_1, w_2, \ldots, w_m)$. Let $\mathcal{C} \subseteq \{0,1\}^X$ be an (N,d) code. If for each $\mathsf{u} \in \mathcal{C}$, $\mathrm{supp}(\mathsf{u})_{\mathbf{X}} \in \binom{\mathbf{X}}{\mathbf{w}}$, then $\mathcal{C}$ is said to be of *multiply constant-weight*, denoted by $\mathrm{MCWC}(\mathbf{n}, d, \mathbf{w})$. The number of codewords in an $\mathrm{MCWC}(\mathbf{n}, d, \mathbf{w})$ is called the *size* of the code. The maximum size of an $\mathrm{MCWC}(\mathbf{n}, d, \mathbf{w})$ is denoted $T(\mathbf{n}, d, \mathbf{w})$, and the $\mathrm{MCWC}(\mathbf{n}, d, \mathbf{w})$ achieving this size is said to be *optimal*.

Specifically, when $m = 1$, an $\mathrm{MCWC}(\mathbf{n}, d, \mathbf{w})$ is a *constant-weight code*, denoted by $\mathrm{CWC}(n, d, w)$ with $n = n_1$ and $w = w_1$; when $m = 2$, an $\mathrm{MCWC}(\mathbf{n}, d, \mathbf{w})$ is a *doubly constant-weight code* [14]. The largest size of a $\mathrm{CWC}(n, d, w)$ is denoted by $A(n, d, w)$. For general m, when $n_i = n$ and $w_i = w$ for all $i \in [m]$, $\mathcal{C}$ is denoted by $\mathrm{MCWC}(m, n, d, w)$. In this case, we use the notation $M(m, n, d, w)$ to denote the maximum size of such a code. Observe that by definition,

$$M(1, n, d, w) = A(n, d, w) \text{ and}$$
$$M(2, n, d, w) = T((n, n), d, (w, w)).$$

Moreover, the functions $A(n, d, w)$ and $T((n, n), d, (w, w))$ have been well studied, see for example [3], [14]–[17]. For the general case $T(\mathbf{n}, d, \mathbf{w})$, some lower and upper bounds were studied in [1]. The techniques of Johnson bound have been applied to get the following recursive bounds in [1] and [2].

Proposition 1: We have

1) *for each* $i \in [m]$,

$$T(\mathbf{n}, d, \mathbf{w}) \leq \lfloor \frac{n_i}{w_i} T(\mathbf{n}', d, \mathbf{w}') \rfloor$$

where $\mathbf{n}' = (n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_m)$ *and* $\mathbf{w}' = (w_1, \ldots, w_{i-1}, w_i - 1, w_{i+1}, \ldots, w_m)$*;*

2) $M(m, n, d, w) \leq \left\lfloor \frac{n^m}{w^m} M(m, n-1, d, w-1) \right\rfloor$.

Since all the codes we consider in this paper are binary, we can assume that the distance d is even and let $d \triangleq 2\delta$ for convenience. Trivial cases are as follows.

Lemma 1: If $d > 2W$, *then* $T(\mathbf{n}, d, \mathbf{w}) = 1$*; if* $d = 2W$, *then* $T(\mathbf{n}, d, \mathbf{w}) = \min_{i\in[m]} \lfloor \frac{n_i}{w_i} \rfloor$*; if* $d = 2$, *then* $T(\mathbf{n}, d, \mathbf{w}) = \prod_{i\in[m]} \binom{n_i}{w_i}$.

III. Optimal MCWCs With Small Weight

We construct optimal multiply constant-weight codes with total weight four in this section. Our approach is based on combinatorial design theory. First, we introduce necessary concepts and establish connections to multiply constant-weight codes.

A. Generalized Packing Designs

A *set system* is a pair $(X, \mathcal{B})$ such that X is a finite set of *points* and $\mathcal{B}$ is a set of subsets of X, called *blocks*. The *order* of the set system is $|X|$, the number of points. For a set K of nonnegative integers, a set system $(X, \mathcal{B})$ is said to be K*-uniform* if $|B| \in K$ for all $B \in \mathcal{B}$. When $K = \{k\}$, we simply write that the system is k-uniform.

Let $N \geq t$ and $\lambda \geq 1$. A t*-*(N, K, λ) *packing* is a K-uniform set system $(X, \mathcal{B})$ of order N, such that every t-subset of X occurs in at most λ blocks in $\mathcal{B}$. If $K = \{k\}$ and each pair occurs in exactly λ blocks, then we call it a *balanced incomplete block design*, and denote it by $\mathrm{BIBD}(N, k, \lambda)$. A $\mathrm{BIBD}(N, 3, 1)$ is known as a *Steiner triple systems* of order N, denoted by $\mathrm{STS}(N)$.

In [18], Cameron introduced a new class of combinatorial designs, which simultaneously generalizes various well-known classes of designs, including t-designs, mutually orthogonal Latin squares, orthogonal arrays and 1-factorizations of complete graphs. In a recent paper [12], Bailey and Burgess considered the analogue of Cameron's generalization for packings, which are called *generalized packing designs*. To define generalized packing designs, we require various pieces of notation and terminology.

If $\mathbf{A} = (A_1, \ldots, A_m)$ and $\mathbf{B} = (B_1, \ldots, B_m)$ are m-tuples of sets, we write $\mathbf{A} \subseteq \mathbf{B}$ to mean that $A_i \subseteq B_i$ for all $i \in [m]$, and say $\mathbf{A}$ is contained in $\mathbf{B}$.

Again let $\mathbf{X} = (X_1, X_2, \ldots, X_m)$ and $\mathbf{n} = (n_1, n_2, \ldots, n_m)$ as in Section II. Assume that $\mathbf{k} = (k_1, \ldots, k_m)$ is an

m-tuple of positive integers with sum k such that $\mathbf{k} \le \mathbf{n}$. Let $\mathbf{t} = (t_1, \dots, t_m)$ be an m-tuple of nonnegative integers. We say $\mathbf{t}$ is $(\mathbf{k}, t)$-*admissible* if $\mathbf{t} \le \mathbf{k}$ and $\sum_{i\in[m]} t_i = t$. In a similar manner, if $\mathbf{T} = (T_1, \dots, T_m)$ is an m-tuple of disjoint sets, we say that $\mathbf{T}$ is $(\mathbf{n}, \mathbf{k}, t)$-*admissible* if each T_i is a t_i-subset of X_i, where $(t_1, \dots, t_m)$ is $(\mathbf{k}, t)$-admissible. Note that since t_i is allowed to be zero, the corresponding set T_i is allowed to be empty.

A t-$(\mathbf{n}, \mathbf{k}, \lambda)$ *generalized packing design*, or more succinctly a *generalized packing*, is a pair $(\mathbf{X}, \mathcal{P})$, such that $\mathcal{P}$ is a family of elements of $\binom{\mathbf{X}}{\mathbf{k}}$, called *blocks*, with the property that every $\mathbf{T} = (T_1, \dots, T_m)$ which is $(\mathbf{n}, \mathbf{k}, t)$-admissible is contained in at most λ blocks in $\mathcal{P}$. As with ordinary packings, the *generalized packing number* $D_\lambda(\mathbf{n}, \mathbf{k}, t)$ is the maximum possible number of blocks in a t-$(\mathbf{n}, \mathbf{k}, \lambda)$ generalized packing. When $\mathbf{n}$ and $\mathbf{k}$ have only one component, we simply write $D_\lambda(N, k, t)$, which is the usual packing number. When λ is omitted, we mean $\lambda = 1$. The equivalence between multiply constant-weight codes and generalized packing designs is obvious.

Proposition 2: There exists an MCWC$(\mathbf{n}, d, \mathbf{w})$ *of size b if and only if a* t-$(\mathbf{n}, \mathbf{w}, 1)$ *generalized packing of size b exists, where* $t = W - d/2 + 1$.

Corollary 1: $T(\mathbf{n}, d, \mathbf{w}) = D(\mathbf{n}, \mathbf{w}, t)$ *where* $t = W – d/2 + 1$.

A few general upper bounds for $D(\mathbf{n}, \mathbf{k}, t)$ can be found in [12]. The cases for $t = 2$ and $k = 3$ or 4 were completely determined except when $\mathbf{k} = (2, 2)$, n_1, n_2 are both odd and $n_1 \le n_2 \le 2n_1 - 1$ [12]. When $t = 3$ and $k = 3$, the designs are trivial. In the following subsection, we determine $D(\mathbf{n}, \mathbf{k}, 3)$ for $k = 4$ completely. Note that the upper bounds for all cases discussed later could be easily obtained by applying techniques of Johnson [3].

B. Determination of $D(\mathbf{n}, \mathbf{k}, 3)$ *for* $k = 4$

We split the problem into five cases.

Case 1: $\mathbf{k} = (4)$.

Let $\mathbf{n} = (n)$, then a 3-$(\mathbf{n}, \mathbf{k}, 1)$ generalized packing design is indeed a 3-$(n, 4, 1)$ packing, for which the determination of packing numbers $D(n, 4, 3)$ has been completed by Bao and Ji in [19]. Hence, we have the following result.

Proposition 3: For any positive integer n,

$$D((n), (4), 3) = \begin{cases} \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \left\lfloor \frac{n-2}{2} \right\rfloor \right\rfloor \right\rfloor & n \not\equiv 0 \pmod 6, \\ \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \left\lfloor \frac{n-2}{2} \right\rfloor \right\rfloor - 1 \right\rfloor & n \equiv 0 \pmod 6. \end{cases}$$

Case 2: $\mathbf{k} = (3, 1)$.

Let $\mathbf{n} = (n_1, n_2)$, then we have $D(\mathbf{n}, \mathbf{k}, 3) \le \min\{\binom{n_1}{3}, n_2 D(n_1, 3, 2)\}$. We prove that the upper bound is achievable by using disjoint partial triple systems. Two 2-$(N,k,1)$ packings $(X,\mathcal{A})$ and $(X, \mathcal{B})$ are *disjoint* if $\mathcal{A} \cap \mathcal{B} = \emptyset$.

When $n \equiv 1, 3 \pmod 6$, $n \ne 7$, there exists a *large set* of Steiner triple systems of order n, that is, a set of $n - 2$ pairwise disjoint optimal 2-$(n, 3, 1)$ packings, [20]–[22]. By collecting from each STS(n) the blocks not containing a fixed point, we obtain a set of $n - 2$ disjoint optimal 2-$(n - 1, 3, 1)$ packings. For $n \equiv 4 \pmod 6$, it was proved by Etzion [23], [24] that there exists a partition of all triples into $n - 1$ optimal 2-$(n, 3, 1)$ packings and one 2-$(n, 3, 1)$ packing of size $(n - 1)/3$. For $n \equiv 5 \pmod 6$, $n \ge 11$, Ji [25] proved that there is a partition of triples into $n - 2$ optimal 2-$(n, 3, 1)$ packings and one packing of size $4(n - 2)/3$. Let $M(n)$ denote the maximum number of disjoint optimal 2-$(n, 3, 1)$ packings. Then for $n \ge 8$, $M(n) = n - 2$ when n is odd and $M(n) = n - 1$ when n is even.

Proposition 4:

$$D((n_1, n_2), (3, 1), 3) = \min\left\{\binom{n_1}{3}, n_2 D(n_1, 3, 2)\right\}$$

for all n_1, $n_2 > 0$ *except for* $(n_1, n_2) \in \{(6, 5), (7, 3), (7, 4), (7, 5)\}$*, whose values are listed below.*

(n_1, n_2)	$(6, 5)$	$(7, 3)$	$(7, 4)$	$(7, 5)$
$D((n_1, n_2), (3, 1), 3)$	18	20	26	31

Proof: Let $\mathbf{X} = (X_1, X_2)$ with $|X_i| = n_i$, $i = 1, 2$. Assume that $(X_1, \mathcal{B}_i)$, $i \in [M(n_1) + \delta]$ are disjoint 2-$(n_1, 3, 1)$ packings as above with the first $M(n_1)$ being optimal. Here $\delta = 1$ when $n_1 \equiv 4, 5 \pmod 6$ and 0 otherwise. For each $j \le \min\{M(n_1) + \delta, n_2\}$, define

$$\begin{aligned} \mathcal{C}(j) = \{(B, \{x\}) :& \\ & B \in \mathcal{B}_i \text{ and } x \text{ is } i\text{-th element of } X_2, 1 \le i \le j\}. \end{aligned}$$

For $n_1 \ge 8$, if $n_2 \le M(n_1)$, then $(\mathbf{X}, \mathcal{C}(n_2))$ is an optimal generalized packing of size $n_2 D(n_1, 3, 2)$; if $n_2 > M(n_1)$, then $(\mathbf{X}, \mathcal{C}(M(n_1 + \delta)))$ is optimal with $\binom{n_1}{3}$ blocks.

For $n_1 \le 4$, the optimal packings are trivial. For $n_1 = 5$, the triples in X_1 can be partitioned into five disjoint optimal 2-$(5, 3, 1)$ packings, that is, $M(5) = 5$. For example, let $\mathcal{B}_1 = \{125, 345\}$, $\mathcal{B}_2 = \{135, 234\}$, $\mathcal{B}_3 = \{145, 123\}$, $\mathcal{B}_4 = \{235, 124\}$ and $\mathcal{B}_5 = \{245, 134\}$, then $([5], \mathcal{B}_i)$, $i \in [5]$ are disjoint optimal 2-$(5, 3, 1)$ packings. Then by the same construction, we have $D(\mathbf{n}, \mathbf{k}, 3) = 2n_2$ if $n_2 \le 5$ and $D(\mathbf{n}, \mathbf{k}, 3) = \binom{5}{3} = 10$ if $n_2 > 5$.

For $n_1 = 7$, Cayley [26] showed that there are only two mutually disjoint STS(7)s, that is, $M(7) = 2$. Now consider the following six disjoint 2-$(7, 3, 1)$ packings $([7], \mathcal{B}_i)$ with $i \in [6]$:

$$\begin{aligned} \mathcal{B}_1 &= \{123, 145, 167, 246, 257, 347, 356\}, \\ \mathcal{B}_2 &= \{124, 137, 156, 235, 267, 346, 457\}, \\ \mathcal{B}_3 &= \{146, 157, 247, 256, 345, 367\}, \\ \mathcal{B}_4 &= \{125, 136, 147, 234, 357, 456\}, \\ \mathcal{B}_5 &= \{126, 135, 237, 245, 567\}, \\ \mathcal{B}_6 &= \{127, 134, 236, 467\}. \end{aligned}$$

So for $n_2 \le 2$, $(\mathbf{X}, \mathcal{C}(n_2))$ is an optimal generalized packing of size $n_2 D(n_1, 3, 2)$; for $n_2 = 3$ or 4, $(\mathbf{X}, \mathcal{C}(n_2))$ is an optimal generalized packing of size $n_2 D(n_1, 3, 2) - n_2 + 2$; for $n_2 = 5$, $(\mathbf{X}, \mathcal{C}(5))$ is a generalized packing of size 31, which is also optimal by exhaustive search; for all $n_2 \ge 6$, $(\mathbf{X}, \mathcal{C}(6))$ is an optimal generalized packing of size $\binom{n_1}{3}$.

For $n_1 = 6$, delete all blocks containing the element 2 from the above six 2-$(7, 3, 1)$ packings over [7], then we get six disjoint 2-$(6, 3, 1)$ packings over $[7] \setminus \{2\}$ with blocks set $\mathcal{B}'_i$, where $|\mathcal{B}'_i| = 4$ for $1 \le i \le 4$ and $|\mathcal{B}'_i| = 2$ for $i = 5, 6$. So for $n_2 \leq 4$, $(\mathbf{X}, \mathcal{C}(n_2))$ is an optimal generalized packing of size $n_2 D(n_1, 3, 2)$; for $n_2 = 5$, $(\mathbf{X}, \mathcal{C}(5))$ is optimal of size 18 by exhaustive search; for all $n_2 \geq 6$, $(\mathbf{X}, \mathcal{C}(6))$ is an optimal generalized packing of size $\binom{n_1}{3}$. ■

Case 3: $\mathbf{k} = (2, 2)$.

Let $\mathbf{n} = (n_1, n_2)$ and assume $n_1 \leq n_2$ without loss of generality. Then the upper bound is $D(\mathbf{n}, \mathbf{k}, 3) \leq \frac{n_1(n_1-1)}{2} \left\lfloor \frac{n_2}{2} \right\rfloor$.

Denote K_n a complete graph with n vertices. Let $\mathcal{F}(n) = \{F_1, F_2, \ldots, F_{\gamma(n)}\}$ be a 1-*factorization* of K_n if $n \equiv 0 \pmod 2$, or a *near* 1-*factorization* of K_n if $n \equiv 1 \pmod 2$. Then $\gamma(n) = n - 1$ if $n \equiv 0 \pmod 2$, and $\gamma(n) = n$ if $n \equiv 1 \pmod 2$. Further, each 1-*factor* F_i is of size $\left\lfloor \frac{n}{2} \right\rfloor$, $i \in [\gamma(n)]$.

Proposition 5: For positive integers $n_1 \leq n_2$,

$$D((n_1, n_2), (2, 2), 3) = \frac{n_1(n_1-1)}{2} \left\lfloor \frac{n_2}{2} \right\rfloor.$$

Proof: Let $\mathbf{X} = (X_1, X_2)$ with $|X_i| = n_i$, $i = 1, 2$. Suppose that $\mathcal{F}(n_i)$ is a (near) 1-factorization of K_{n_i} with vertex set X_i, $i = 1, 2$. The upper bound is achieved by taking all blocks in $\{(P, Q) : P \in F_i \in \mathcal{F}(n_1), Q \in F_i' \in \mathcal{F}(n_2), 1 \leq i \leq \gamma(n_1)\}$. ■

Case 4: $\mathbf{k} = (2, 1, 1)$.

Let $\mathbf{n} = (n_1, n_2, n_3)$ and assume $n_2 \leq n_3$ without loss of generality. Then the upper bound is $D(\mathbf{n}, \mathbf{k}, 3) \leq \min\{\frac{n_1(n_1-1)n_2}{2}, \left\lfloor \frac{n_1}{2} \right\rfloor n_2 n_3\}$.

An $n_2 \times n_3$ *Latin rectangle* ($LR(n_2, n_3)$) is an $n_2 \times n_3$ array over $[n_3]$ such that each symbol occurs exactly once in each row, and at most once in each column. When $n_2 = n_3$, it is also called a *Latin square* of order n_3. An $LR(n_2, n_3)$ can always be obtained from a Latin square of order n_3 by collecting any n_2 rows.

Proposition 6: Let $n_2 \leq n_3$. Then

$$D((n_1, n_2, n_3), (2, 1, 1), 3) = \min\left\{\frac{n_1(n_1-1)n_2}{2}, \left\lfloor \frac{n_1}{2} \right\rfloor n_2 n_3\right\}.$$

Proof: Let $\mathbf{X} = ([n_1], [n_2], [n_3])$. Suppose that $M = (m_{ij})$ is an $LR(n_2, n_3)$ over $[n_3]$ and $\mathcal{F}(n_1)$ is a (near) 1-factorization of K_{n_1} with vertex set $[n_1]$. For each $s \leq \min\{\gamma(n_1), n_3\}$, define

$$\mathcal{C}(s) = \{(P, \{i\}, \{j\}) : P \in F_x \in \mathcal{F}(n_1) \text{ and } i \in [n_2], j \in [n_3] \text{ with } m_{ij} = x, 1 \leq x \leq s\}.$$

Then when $\gamma(n_1) \geq n_3$, $(\mathbf{X}, \mathcal{C}(n_3))$ is an optimal generalized packing of size $\left\lfloor \frac{n_1}{2} \right\rfloor n_2 n_3$; when $\gamma(n_1) < n_3$, $(\mathbf{X}, \mathcal{C}(\gamma(n_1)))$ is an optimal generalized packing of size $\frac{n_1(n_1-1)n_2}{2}$. ■

Case 5: $\mathbf{k} = (1, 1, 1, 1)$.

Proposition 7: Let $\mathbf{n} = (n_1, n_2, n_3, n_4)$ and $n_1 \leq n_2 \leq n_3 \leq n_4$. Then $D(\mathbf{n}, (1, 1, 1, 1), 3) = n_1 n_2 n_3$.

Proof: It is clear that $D(\mathbf{n}, \mathbf{k}, 3) \leq n_1 n_2 n_3$. Consider $\mathbb{Z}_{n_4}$ and let $X_i = \{s_i : 0 \leq s_i \leq n_i - 1\}$ for $i \in [4]$. Equality then follows from considering all blocks of the form $(\{s_1\}, \{s_2\}, \{s_3\}, \{s_4\})$, where $s_i \in X_i$ and $\sum_{i \in [4]} s_i = 0$. Here the addition is over $\mathbb{Z}_{n_4}$. ■

Combining results in [12], we have determined $T(\mathbf{n}, d, \mathbf{w})$ for total weight less than or equal to four completely except when $\mathbf{w} = (2, 2)$, $d = 6$ and $n_1 \leq n_2 \leq 2n_1 - 1$, both n_1 and n_2 are odd. Note that a recent paper of Wang *et al.* [27] almost completely determines the remaining cases.

IV. Optimal MCWCs With Minimum Distance Four

In this section we handle the multiply constant-weight codes MCWC(m, n, d, w) with minimum distance four and small weight w. For convenience, we sometimes arrange a codeword as an $m \times n$ binary matrix.

When $w = 1$, an MCWC$(m, n, d, 1)$ is equivalent to an n-ary code of length m and distance $d/2$ by a bijection from row words to the set $\{0, 1, \ldots, n-1\}$.

Lemma 2 (Chee et al. [1]): $M(m, n, d, 1) = A_n(m, \delta)$, where $A_n(m, \delta)$ is the maximum size of an n-ary code of length m and distance $\delta = d/2$.

When $\delta = 2$, $A_n(m, 2) = n^{m-1}$, which can be achieved by a code over $\mathbb{Z}_n$ consisting of all m-tuples with a constant sum.

Corollary 2: $M(m, n, 4, 1) = n^{m-1}$.

Applying Proposition 1 1) iteratively w times for each $i \in [m-1]$, we obtain the following consequence.

Proposition 8: $M(m, n, d, w) \leq \binom{n}{w}^{m-1} A(n, d, w)$.

By Corollary 2, the bound in Proposition 8 is tight when $w = 1$ and $d = 4$. Next, we show that it is also tight for some other small values w. The following two corollaries are immediate consequences of Proposition 8.

Corollary 3: $M(m, n, 4, 2) \leq \binom{n}{2}^{m-1} \lfloor \frac{n}{2} \rfloor$.

Corollary 4: $M(m, n, 4, 3) \leq \binom{n}{3}^{m-1} \lfloor \frac{n}{3} \lfloor \frac{n-1}{2} \rfloor \rfloor$.

A. Product Construction

We give a product construction as follows by generalizing the method used in [14, Sec. 6], which is a partial case of the generalized concatenation construction in [28].

Let Y be a finite set of size n. Suppose that $\mathcal{C}_i \subseteq \{0, 1\}^Y$ is a CWC(n, d_1, w) for each $i \in [s]$ and $\cup_{i \in [s]} \mathcal{C}_i$ is a CWC(n, d_2, w). Obviously, we have $d_2 \leq d_1$. Further, let $\mathcal{C}_0 \subset \{0, 1\}^{[m] \times [s]}$ be an MCWC$(m, s, d_3, 1)$. Let $X = [m] \times Y$ and $\mathbf{X} = (\{1\} \times Y, \ldots, \{m\} \times Y)$. For each codeword $\mathsf{u} \in \mathcal{C}_0$, define a code $\mathcal{D}_{\mathsf{u}} \subset \{0, 1\}^X$ as

$$\mathcal{D}_{\mathsf{u}} = \{\mathsf{v}^{j_1} | \mathsf{v}^{j_2} | \cdots | \mathsf{v}^{j_m} : \mathsf{v}^{j_i} \in \mathcal{C}_{j_i}, (i, j_i) \in \text{supp}(\mathsf{u}) \text{ and } i \in [m]\},$$

where the | operator concatenates codewords as strings.

Then for each $c \in \mathcal{D}_{\mathsf{u}}$, $\text{supp}(c)_{\mathbf{X}} \in \binom{\mathbf{X}}{\mathbf{w}}$, where $\mathbf{w} = (w, \ldots, w)$. Let $\mathcal{D} = \cup_{\mathsf{u} \in \mathcal{C}_0} \mathcal{D}_{\mathsf{u}}$. It is easy to check that $\mathcal{D}$ is an MCWC(m, n, d, w) with minimum distance $d \geq \min(d_3 d_2/2, d_1)$. In fact, for any two codewords in $\mathcal{D}_{\mathsf{u}}$, the distance is at least d_1. For two codewords $c \in \mathcal{D}_{\mathsf{u}}$ and $c' \in \mathcal{D}_{\mathsf{v}}$ with $\mathsf{u} \neq \mathsf{v}$, since $d_H(\mathsf{u}, \mathsf{v}) \geq d_3$, $|\text{supp}(\mathsf{u}) \setminus \text{supp}(\mathsf{v})| \geq d_3/2$. Hence $d_H(c, c') \geq d_3 d_2/2$. Further, if all $\mathcal{C}_i$ have the same size M, then $|\mathcal{D}| = |\mathcal{C}_0| M^m$. Note that one can also treat $\mathcal{C}_0$ as an s-ary code of length m and distance $d_3/2$ to get the same $\mathcal{D}$.

B. Optimal MCWCs

Now we apply the product construction with special families of constant-weight codes to obtain optimal multiply constant-weight codes.

Proposition 9: $M(m, n, 4, 2) = \binom{n}{2}^{m-1} \lfloor \frac{n}{2} \rfloor$ for all positive integers n and m.

Proof: When n is even, let $s = n - 1$. For each $i \in [s]$, let $\mathcal{C}_i \subset \{0,1\}^Y$ be a CWC$(n, 4, 2)$ such that $F_i = \{\mathrm{supp}(\mathsf{u}) : \mathsf{u} \in \mathcal{C}_i\}$ is a 1-factor and $\{F_i : i \in [s]\}$ is a 1-factorization of K_n with vertex set Y. Then apply the product construction with $d_1 = d_3 = 4$, $d_2 = 2$ and $w = 2$.

When n is odd, let $s = n$. Then use the similar codes such that each F_i is a near 1-factor and $\{F_i : i \in [s]\}$ is a near 1-factorization. ■

To get the following result, we again use the existence of partitions of triples into disjoint optimal packings as described in Section III.

Proposition 10: $M(m, n, 4, 3) = \binom{n}{3}^{m-1} \lfloor \frac{n}{3} \lfloor \frac{n-1}{2} \rfloor \rfloor$ for all positive integers m and $n \equiv 0, 1, 2, 3 \pmod 6$ with $n \neq 6, 7$.

Proof: For each $n \equiv 1, 3 \pmod 6$ and $n \neq 7$, let $s = n-2$. For each $i \in [s]$, let $\mathcal{C}_i \subset \{0,1\}^Y$ be a CWC$(n, 4, 3)$ such that $F_i = \{\mathrm{supp}(\mathsf{u}) : \mathsf{u} \in \mathcal{C}_i\}$ is the block set of a Steiner triple system over Y and $\{F_i : i \in [s]\}$ forms a large set of Steiner triple systems. Then apply the product construction with $d_1 = d_3 = 4$, $d_2 = 2$ and $w = 3$.

For each $n \equiv 0, 2 \pmod 6$ and $n \neq 6$, let $s = n - 1$. For each $i \in [s]$, let $\mathcal{C}_i \subset \{0,1\}^Y$ be a CWC$(n, 4, 3)$ such that $F_i = \{\mathrm{supp}(\mathsf{u}) : \mathsf{u} \in \mathcal{C}_i\}$ is an optimal 2-$(n, 3, 1)$ packing over Y of size $n(n-2)/6$ and $\{F_i : i \in [s]\}$ is a set of $n - 1$ disjoint optimal 2-$(n, 3, 1)$ packings. Then apply the product construction with same values of d_1, d_2, d_3 and w. ■

Note that when $n \equiv 4, 5 \pmod 6$, there is no partition of all triples into optimal packings [23]–[25], but only a partition with almost all packings except one being optimal. By the product construction, if not all $\mathcal{C}_i$ have the same size, then it is difficult to compute the exact size of $\mathcal{D}$. So we can only get a lower bound of $\mathcal{D}$ by using disjoint optimal packings for these cases.

Proposition 11: Let $n \geq 10$. For all positive integers m, $M(m, n, 4, 3) \geq (\frac{n(n-2)-2}{6})^m (n-1)^{m-1}$ when $n \equiv 4 \pmod 6$ and $M(m, n, 4, 3) \geq (\frac{n(n-1)-8}{6})^m (n-2)^{m-1}$ when $n \equiv 5 \pmod 6$.

V. Asymptotic Sizes of $T(\mathbf{n}, d, \mathbf{w})$

The following result for $M(m, n, d, w)$ was proved in [1].

Proposition 12 (Chee et al. [1]): Given $m, d = 2\delta, w$, let s be the smallest integer such that $m(w - s) - \delta + 1 < m$ and $r = m(w - s) - \delta + 1$. Then

$$M(m, n, d, w) \leq \left\lfloor \frac{n^m}{w^m} \left\lfloor \frac{(n-1)^m}{(w-1)^m} \cdots \left\lfloor \frac{(n-s+1)^m}{(w-s+1)^m} \left\lfloor \frac{(n-s)^r}{(w-s)^r} \right\rfloor \right\rfloor \cdots \right\rfloor \right\rfloor. \quad (1)$$

Further, let $t = mw - \delta + 1$ and consider $M(m, n, d, w)$ as a function of n, then

$$1 \leq \limsup_{n \to \infty} \frac{M(m, n, d, w)}{n^t / w^t} \leq \frac{w^t}{(w - s)^t}.$$

In addition, when $t \leq m$, $n/w \geq mw - 1$ and n/w is a prime power, $M(m, n, d, w) = \frac{n^t}{w^t}$ holds.

The last statement of Proposition 12 shows that under certain restrictions, the upper estimate (1) is asymptotically sharp. In this section, we prove that (1) is asymptotically sharp for all cases. In fact, we give a more general result for $T(\mathbf{n}, d, \mathbf{w})$ when all the components of $\mathbf{n}$ grow in any fixed proportion.

A. Asymptotic Theorem

Since $T(\mathbf{n}, d, \mathbf{w}) = D(\mathbf{n}, \mathbf{w}, t)$, where $t = W - \delta + 1$ by Corollary 1, we study the upper bound of generalized packing numbers $D(\mathbf{n}, \mathbf{w}, t)$ instead.

Let $\mathbf{X}, \mathbf{n}, \mathbf{w}, t$ be defined as before. Suppose that $n_i = c_i v$, $i \in [m]$ for some integer v. Given a $(\mathbf{w}, t)$-admissible $\mathbf{t}$, since every element of $\binom{\mathbf{X}}{\mathbf{t}}$ occurs at most once in a block, we have

$$\begin{aligned} D(\mathbf{n}, \mathbf{w}, t) &\leq \prod_{i \in [m]} \binom{c_i v}{t_i} \Big/ \binom{w_i}{t_i} \\ &\leq \frac{v^t}{\prod_{i \in [m]} w_i!} \prod_{i \in [m]} c_i^{t_i} (w_i - t_i)!. \quad (2) \end{aligned}$$

Let $C \triangleq \min\{\prod_{i \in [m]} c_i^{t_i} (w_i - t_i)! : \mathbf{t}$ is $(\mathbf{w}, t)$-admissible$\}$. Then our asymptotic result can be stated as follows.

Theorem 1: Let $t = W - \delta + 1$ and $d = 2\delta$. Then

$$\lim_{v \to \infty} \frac{T(\mathbf{n}, d, \mathbf{w})}{v^t} = \lim_{v \to \infty} \frac{D(\mathbf{n}, \mathbf{w}, t)}{v^t} = \frac{C}{\prod_{i \in [m]} w_i!}.$$

For an MCWC(m, n, d, w), we can let $c_i = 1$ for all $i \in [m]$ and $v = n$. Then C can be achieved when the m-tuple $\mathbf{t}$ is an almost constant tuple, that is, values of t_i differ at most one. Applying Theorem 1, we get the asymptotic sizes for $M(m, n, d, w)$.

Corollary 5: Given $m, d = 2\delta, w$, let s be the smallest integer such that $m(w-s)-\delta+1 < m$ and $r = m(w-s)-\delta+1$. Let $t = mw - \delta + 1$. Then

$$\lim_{n \to \infty} \frac{M(m, n, d, w)}{n^t} = \frac{1}{w^m (w-1)^m \cdots (w-s+1)^m (w-s)^r}.$$

B. Proof of Theorem 1

Given a hypergraph $\mathcal{H}$, let $E(\mathcal{H})$ be the edge set and $V(\mathcal{H})$ be the vertex set. Denote $\nu(\mathcal{H})$ the maximum size of a matching in $\mathcal{H}$.

A function $\theta : E(\mathcal{H}) \longrightarrow R$ is a *fractional matching* of the hypergraph $\mathcal{H}$ if $\sum_{e \in E(\mathcal{H}); x \in e} \theta(e) \leq 1$ holds for every vertex $x \in V(\mathcal{H})$. Let $\theta(\mathcal{H}) = \sum_{e \in E(\mathcal{H})} \theta(e)$. The *fractional matching number*, denoted $\nu^*(\mathcal{H})$ is the maximum of $\theta(\mathcal{H})$ over all fractional matchings. Clearly,

$$\nu(\mathcal{H}) \leq \nu^*(\mathcal{H}).$$

Kahn [13] proved that under certain conditions, asymptotic equality holds. For a subset $S \subset V(\mathcal{H})$, define $\bar{\theta}(S) = \sum_{e \in E(\mathcal{H}); S \subset e} \theta(e)$ and $\alpha(\theta) = \max\{\bar{\theta}(\{x, y\}) : x, y \in V(\mathcal{H}), x \neq y\}$. Here $\alpha(\theta)$ is a fractional generalization of the codegree. We say that $\mathcal{H}$ is *l-bounded* if each of its edges has size at most l.

Theorem 2 (Kahn [13]): For every l and every $\varepsilon > 0$ there is a σ such that whenever $\mathcal{H}$ is an l-bounded hypergraph and θ is a fractional matching with $\alpha(\theta) < \sigma$, then

$$\nu(\mathcal{H}) > (1 - \varepsilon)\theta(\mathcal{H}).$$

We apply Kahn's Theorem to prove Theorem 1. First, we define a hypergraph Γ_v with v defined in $\mathbf{n} = (c_1 v, \dots, c_m v)$.

Let $\mathcal{T}$ be the set of all $(\mathbf{w}, t)$-admissible m-tuples. Given $\mathbf{A} \in \binom{\mathbf{X}}{\mathbf{w}}$, let $\mathcal{E}(\mathbf{A}) = \cup_{\mathbf{t}\in\mathcal{T}}\binom{\mathbf{A}}{\mathbf{t}}$. Then construct a hypergraph Γ_v with vertex set $\cup_{\mathbf{t}\in\mathcal{T}}\binom{\mathbf{X}}{\mathbf{t}}$ and edge set $\{\mathcal{E}(\mathbf{A}) : \mathbf{A} \in \binom{\mathbf{X}}{\mathbf{w}}\}$. Note that for any two distinct blocks $\mathbf{A}_1$ and $\mathbf{A}_2$ in the generalized packing, we have $\mathcal{E}(\mathbf{A}_1) \cap \mathcal{E}(\mathbf{A}_2) = \emptyset$. Hence a t-$(\mathbf{n}, \mathbf{w}, 1)$ generalized packing corresponds to a matching in Γ_v, that is, $\nu(\Gamma_v) = D(\mathbf{n}, \mathbf{w}, t)$.

It suffices to verify the conditions of Theorem 2 and to produce a fractional matching θ of the hypergraph Γ_v of the desired size. It is easy to know that Γ_v is l-bounded with $l = \sum_{\mathbf{t}\in\mathcal{T}} \prod_{i\in[m]} \binom{w_i}{t_i}$. Now consider the function $\theta : E(\Gamma_v) \longrightarrow R$ by

$$\theta(e) = \frac{C}{v^{W-t}\prod_{i\in[m]} c_i^{w_i}},$$

for every $e \in E(\Gamma_v)$. We first check θ is a fractional matching. For any vertex $x \in V(\Gamma_v)$, which is an $(\mathbf{n}, \mathbf{w}, t)$-admissible m-tuple of disjoint sets of sizes $\mathbf{t}$, we have

$$\begin{aligned}\deg(x) &= \prod_{i\in[m]}\binom{c_i v - t_i}{w_i - t_i} \le \prod_{i\in[m]} \frac{(c_i v)^{w_i - t_i}}{(w_i - t_i)!}\\ &= v^{W-t}\prod_{i\in[m]}\frac{c_i^{w_i}}{c_i^{t_i}(w_i - t_i)!} \le \frac{v^{W-t}\prod_{i\in[m]} c_i^{w_i}}{C}.\end{aligned}$$

Hence, $\sum_{e\in E(\Gamma_v); x\in e}\theta(e) \le 1$ and θ is indeed a fractional matching. Next, we compute $\alpha(\theta)$. For every $x, y \in V(\Gamma_v)$, then $x \cup y$ is $(\mathbf{n}, \mathbf{w}, t')$-admissible with $t' \ge t + 1$. Here, the union operation is component-wise. Then the codegree of x and y is

$$\deg(x, y) = O(v^{W-t-1}).$$

Hence $\alpha(\theta) = \deg(x, y)\cdot\theta(e) = o(1)$ when $v \to \infty$.

Finally, we apply Kahn's Theorem.

$$\begin{aligned}&\lim_{v\to\infty}\frac{D(\mathbf{n}, \mathbf{w}, t)}{v^t}\\ &= \lim_{v\to\infty}\frac{\nu(\Gamma_v)}{v^t} \ge \lim_{v\to\infty}\frac{\theta(\Gamma_v)}{v^t}\\ &= \lim_{v\to\infty}\frac{|E(\Gamma_v)| \times \theta(e)}{v^t}\\ &= \lim_{v\to\infty}\prod_{i\in[m]}\binom{c_i v}{w_i} \times \frac{C}{v^{W-t}\prod_{i\in[m]} c_i^{w_i}}/v^t\\ &= \frac{C}{\prod_{i\in[m]} w_i!}.\end{aligned}$$

The other inequality comes from the upper bound (2).

VI. Two Dimensional Multiply Constant-Weight Codes

Recall that if the lengths of different parts of a codeword are constant, say $\mathbf{n} = (n, n, \dots, n)$, then each codeword could be considered as an $m \times n$ binary matrix. In this section, we impose additional weight constraints on all columns. We note that these codes have applications in optical storage in holographic memory [9], crossbar arrays of resistive devices [10], and power line communications [11].

Let $\mathbf{n} = (n, n, \dots, n)$ and $\mathbf{w} = (w_1, \dots, w_m)$. A *two dimensional multiply constant-weight code* 2DMCWC$(m, n, d, \mathbf{w}, l)$ is an MCWC$(\mathbf{n}, d, \mathbf{w})$ in a matrix form such that each column of codewords has constant weight l. Let $M(m, n, d, \mathbf{w}, l)$ denote the largest size of a 2DMCWC$(m, n, d, \mathbf{w}, l)$. If $w_i = w$ for all $i \in [m]$, we simply write 2DMCWC(m, n, d, w, l) and $M(m, n, d, w, l)$.

A. Upper Bounds

An *α-parallel class* of a set system is a subset of the blocks such that each point appears exactly α times.

Definition 1: Let $(Y, \mathcal{B})$ be a 2-(M, K, λ) packing, where K is a set of positive integers. If the blocks can be arranged into an $m \times n$ array $\mathcal{R}$ such that

(1) *each entry in $\mathcal{R}$ is either empty or a block;*
(2) *the blocks in the i-th row form a w_i-parallel class;*
(3) *the blocks in each column form an l-parallel class.*

Then, we call it a double resolvable packing, *and denote it by DRP$(M, \lambda; \mathbf{w}, l; m, n)$. Again we write DRP$(M, \lambda; w, l; m, n)$ if $w_i = w$ for all $i \in [m]$.*

Note that we omit the parameter K in the notation DRP$(M, \lambda; \mathbf{w}, l; m, n)$ since it can not provide any information about a 2DMCWC constructed from a DRP. Further, as in the following proposition, we can not determine K of a DRP constructed from a 2DMCWC. A more general version of DRP can be found in [29], which was introduced to construct optimal constant-composition codes.

Proposition 13: A DRP$(M, \lambda; \mathbf{w}, l; m, n)$ is equivalent to a 2DMCWC$(m, n, d,\ \mathbf{w}, l)$ of size M, where $d = 2(W - \lambda)$.

Proof: Suppose $(Y, \mathcal{B})$ is a DRP$(M, \lambda; \mathbf{w}, l; m, n)$ such that the blocks are arranged into an $m \times n$ array $\mathcal{R}$. Denote the (i, j)-th entry of $\mathcal{R}$ by $\mathcal{R}_{ij}$, where $i \in [m]$ and $j \in [n]$.

For each $x \in Y$, we construct an $m \times n$ binary matrix u^x with the (i, j)-th entry defined as

$$\mathsf{u}^x_{ij} = \begin{cases}1, & \text{if } x \in \mathcal{R}_{ij};\\ 0, & \text{otherwise.}\end{cases}$$

Then $\mathcal{C} = \{\mathsf{u}^x \mid x \in Y\}$ is a 2DMCWC$(m, n, d, \mathbf{w}, l)$ of size M, where $d = 2(W - \lambda)$.

The construction can be easily reversed to obtain the converse. ■

Example 1: Here is an example of a DRP$(3, 3; 2, 2; 3, 3)$ over $Y = \mathbb{Z}_3$,

01	12	02
02	01	12
12	02	01

from which we obtain a 2DMCWC$(3, 3, 6, 2, 2)$ by taking the codewords

$$\mathsf{u}^0 = \begin{pmatrix}1 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix},\quad \mathsf{u}^1 = \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}$$

and

$$\mathsf{u}^2 = \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}.$$

Lemma 3 (Upper Bound): If $\sum_{i\in[m]} w_i^2 - n\lambda > 0$*, and there exists a DRP*$(M,\lambda;\ \mathbf{w},l;m,n)$*, or equivalently a 2DMCWC*$(m,n,d,\mathbf{w},l)$ *of size M, where* $d = 2(W-\lambda)$*, then*

$$M \le \frac{n(nl-\lambda)}{\sum_{i\in[m]} w_i^2 - n\lambda}.$$

Proof: Let $\mathcal{R}$ be the $m\times n$ array of a DRP$(M,\lambda;\ \mathbf{w},l;m,n)$ and $f_{ij} = |\mathcal{R}_{ij}|$. Then

$$\sum_{i\in[m]}\sum_{j\in[n]} f_{ij} = Mnl = M\sum_{i\in[m]} w_i.$$

By the definition of a double resolvable packing,

$$\lambda M(M-1) \ge \sum_{i\in[m]}\sum_{j\in[n]} f_{ij}(f_{ij}-1) = \sum_{i\in[m]}\sum_{j\in[n]} f_{ij}^2 - Mnl.$$

By Cauchy–Schwartz inequality, for any $i\in[m]$,

$$\sum_{j\in[n]} f_{ij}^2 \ge \frac{(\sum_{j\in[n]} f_{ij})^2}{n} = \frac{(Mw_i)^2}{n}.$$

So

$$\lambda M(M-1) \ge \sum_{i\in[m]} \frac{(Mw_i)^2}{n} - Mnl.$$

Hence

$$M \le \frac{n(nl-\lambda)}{\sum_{i\in[m]} w_i^2 - n\lambda},$$

provided that $\sum_{i\in[m]} w_i^2 - n\lambda > 0$. Note that the right hand side is always positive since $n^2 l = n\sum_{i\in[m]} w_i \ge \sum_{i\in[m]} w_i^2$. ■

If the bound in Lemma 3 is achieved, then all the blocks in the i-th row are of the same size $\frac{Mw_i}{n}$, and each pair appears in exactly λ blocks. It is easy to check that the 2DMCWC$(3,3,6,2,2)$ constructed in Example 1 is optimal.

Further, if we let $f = \left\lfloor \frac{Ml}{m} \right\rfloor$ and $r = Ml - mf$, then we can improve the above bound by using

$$\sum_{i\in[m]} f_{ij}^2 \ge (m-r)f^2 + r(f+1)^2.$$

Lemma 4 (Improved Upper Bound): If there exists a DRP$(M,\lambda;\mathbf{w},l;m,n)$*, or equivalently a 2DMCWC*$(m, n,d,\mathbf{w},l)$ *of size M, where* $d = 2(W-\lambda)$*, then*

$$\lambda M(M-1) \ge n[(m-r)f^2 + r(f+1)^2] - Mnl = n(mf^2 + 2rf + r) - Mnl,$$

where $f = \left\lfloor \frac{Ml}{m} \right\rfloor$ *and* $r = Ml - mf$*.*

Note that the upper bound of $M(m,n,d,\mathbf{w},l)$ is the largest M that satisfies the inequality in Lemma 4, which is usually achieved when the equality holds.

Example 2: Here are two examples of optimal two dimensional multiply constant-weight codes that achieve the bound in Lemma 4. We list the equivalent double resolvable packings instead.

An optimal 2DMCWC$(6,6,20,2,2)$ *of size* 4*:*

01	23	0	1	2	3
23	01	3	0	1	2
2	3	02	13	0	1
1	2	13	02	3	0
0	1	2	3	03	12
3	0	1	2	12	03

.

An optimal 2DMCWC$(9,9,32,2,2)$ *of size* 6*:*

01	45	12	2	3	0	3	5	4
25	13	04	3	0	1	4	2	5
34	02	35	0	1	2	5	4	1
4	5	5	03	14	03	2	1	2
3	4	2	15	05	24	1	3	0
5	1	4	24	23	15	0	0	3
0	2	3	5	4	3	01	45	12
1	3	0	4	2	5	25	13	04
2	0	1	1	5	4	34	02	35

.

B. Constructions

First we show that concatenating small optimal two dimensional MCWCs gives big optimal two dimensional MCWCs.

Proposition 14: Let a be a positive integer. Suppose there exists an optimal 2DMCWC$(m,n,d,\mathbf{w},l)$ *of size M achieving the bound in Lemma 3 or Lemma 4. Then there exists an optimal 2DMCWC*$(am,n,\ ad,\mathbf{w}',al)$ *of size M, where* $\mathbf{w}'$ *is a vector of length am by copying* $\mathbf{w}$ *a times.*

Proof: First, we check that the two codes have the same upper bounds of sizes. Suppose that a 2DMCWC$(m,n,d,\mathbf{w},l)$ corresponds to a DRP$(M,\lambda;\mathbf{w},l;m,n)$ and a 2DMCWC$(am,n,ad,\mathbf{w}',al)$ corresponds to a DRP$(M_1,\lambda_1;\mathbf{w}',al;am,n)$, then $\lambda_1 = a\lambda$. By Lemma 3, M and M_1 satisfy the same inequality. Now we check for Lemma 4. Let $f_1 = \left\lfloor \frac{M_1 al}{am} \right\rfloor = \left\lfloor \frac{M_1 l}{m} \right\rfloor$ and $r_1 = M_1 al - amf_1 = a(M_1 l - mf_1)$. Then

$$\lambda_1 M_1(M_1-1) \ge n[(am-r_1)f_1^2 + r_1(f_1+1)^2] - aM_1 nl,$$

that is,

$$\lambda M_1(M_1-1) \ge n[(m-r_1/a)f_1^2 + (r_1/a)(f_1+1)^2] - M_1 nl.$$

Being considered as an inequality with indeterminate M_1, it is exactly the same inequality as in Lemma 4. Hence, M and M_1 have the same restrictions.

So if there exists an optimal 2DMCWC$(m,n,d,\mathbf{w},l)$ $\mathcal{C}$, then we can obtain an optimal 2DMCWC$(am,n,\ ad,\mathbf{w}',al)$ by concatenating each codeword from $\mathcal{C}$ a times in the vertical direction. ■

By applying the same technique but concatenating each codeword in $\mathcal{C}$ b times in the horizontal direction, we have that $M(m,n,d,\mathbf{w},l) = M$ achieving the bound in Lemma 3 or Lemma 4 implies $M(am,bn,abd,b\mathbf{w}',al) = M$. Hence, we only consider the codes with parameters m, l and d (or n, $\mathbf{w}$ and d) having no common divisors.

Lemma 5: For any positive integer n, $M(n, n, 2n, 1, 1) = n$.

Proof: For any positive integer n, a Latin square of order n is a DRP$(n, 0; 1, 1; n, n)$. ■

The construction of 2DMCWC$(nl, n, d, 1, l)$s has been investigated in many papers as equidistant frequency permutation arrays and constant-composition codes [30], [31]. Most of the constructions can be generalized to construct 2DMCWC(m, n, d, w, l).

Construction 1: If there exists an α-resolvable BIBD(M, k, λ) with $r = \frac{(M-1)\lambda}{(k-1)\alpha}$ α-parallel classes (each has $b = \frac{\alpha M}{k}$ blocks), then for any pair of positive integers (s, t) with $st = r$, there exists a DRP$(M, b\lambda; \alpha t, \alpha s; bs, bt)$, that is, an optimal 2DMCWC$(bs, bt, d, \alpha t, \alpha s)$ of distance $d = 2b(\alpha r - \lambda)$.

Proof: We construct a $bs \times bt$ array $\mathcal{R}$ of a DRP$(M, b\lambda; \alpha t, \alpha s; bs, bt)$ as follows. For each $1 \leq i \leq r$, let A_i be a $b \times b$ array with the first column occupied by the blocks in the i-th α-parallel class, and other columns being cyclic shifts of the first one. Then the $bs \times bt$ array $\mathcal{R}$ is formed by arranging all A_i's into an $s \times t$ array. The optimality is easy to be checked by Lemma 3. ■

By Construction 1, the existence of α-resolvable BIBD(M, k, λ)s implies the existence of optimal two dimensional multiply constant-weight codes with certain parameters. Necessary conditions for the existence of an α-resolvable BIBD(M, k, λ) are (1) $\lambda(M-1) \equiv 0 \pmod{\alpha(k-1)}$, (2) $\lambda M(M-1) \equiv 0 \pmod{k(k-1)}$, and (3) $\alpha M \equiv 0 \pmod{k}$. For $k \in \{2, 3, 4\}$, the necessary conditions are sufficient except for $(M, k, \lambda, \alpha) \in \{(6, 3, \lambda, 1) : \lambda \equiv 2 \pmod{4}\} \cup \{(10, 4, 2, 2)\}$ [32], [33]. Hence we can obtain several families of optimal two dimensional multiply constant-weight codes by Construction 1.

VII. Conclusion

Several new combinatorial constructions for multiply constant-weight codes are given to yield new infinite families of optimal MCWCs with small weight or small distance. The Johnson upper bounds of MCWCs are shown to be asymptotically tight for given weights and distances, which greatly improves the previous result saying that the bounds are asymptotically tight to a constant factor and for a smaller class of MCWCs. Finally, we introduce the concept of two dimensional MCWCs, for which bounds and constructions are studied.

Acknowledgment

The authors thank the anonymous referees and Prof. Stephan ten Brink for their constructive comments and suggestions.

References

[1] Y. M. Chee *et al.*, "Multiply constant-weight codes and the reliability of loop physically unclonable functions," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7026–7034, Nov. 2014.

[2] Z. Cherif, J.-L. Danger, S. Guilley, J.-L. Kim, and P. Solé, "Multiply constant weight codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 306–310.

[3] S. Johnson, "Upper bounds for constant weight error correcting codes," *Discrete Math.*, vol. 3, nos. 1–3, pp. 109–124, Jan. 1972.

[4] V. I. Levenshtein, "Upper-bound estimates for fixed-weight codes," *Problems Inform. Transmiss.*, vol. 7, no. 4, pp. 281–287, 1971.

[5] Z. Cherif, J.-L. Danger, S. Guilley, and L. Bossuet, "An easy-to-design PUF based on a single oscillator: The loop PUF," in *Proc. 15th Euromicro Conf. Digit. Syst. Design*, Sep. 2012, pp. 156–162.

[6] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[7] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, Nov. 2002, pp. 148–160.

[8] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Design Autom. Conf.*, Jun. 2007, pp. 9–14.

[9] E. Ordentlich and R. M. Roth, "Two-dimensional weight-constrained codes through enumeration bounds," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1292–1301, Jul. 2000.

[10] E. Ordentlich and R. M. Roth, "Low complexity two-dimensional weight-constrained codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3892–3899, Jun. 2012.

[11] Y. M. Chee, H. M. Kiah, and P. Purkayastha, "Matrix codes and multitone frequency shift keying for power line communications," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2013, pp. 2870–2874.

[12] R. F. Bailey and A. C. Burgess, "Generalized packing designs," *Discrete Math.*, vol. 313, no. 11, pp. 1167–1190, Jun. 2013.

[13] J. Kahn, "A linear programming perspective on the Frankl–Rödl–Pippenger theorem," *Random Struct. Algorithms*, vol. 8, no. 2, pp. 149–157, Mar. 1996.

[14] T. Etzion, "Optimal doubly constant weight codes," *J. Combinat. Design*, vol. 16, no. 2, pp. 137–151, Mar. 2008.

[15] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2373–2395, Nov. 2000.

[16] A. Brouwer, J. B. Shearer, N. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1334–1380, Nov. 1990.

[17] D. H. Smith, L. A. Hughes, and S. Perkins, "A new table of constant weight codes of length greater than 28," *Electron. J. Combin.*, vol. 13, no. 1, p. 18, Dec. 2006.

[18] P. J. Cameron, "A generalisation of t-designs," *Discrete Math.*, vol. 309, no. 14, pp. 4835–4842, Jul. 2009.

[19] J. Bao and L. Ji, "The completion determination of optimal (3,4)-packings," *Designs, Codes Cryptography*, vol. 77, no. 1, pp. 217–229, Oct. 2015.

[20] J. X. Lu, "On large sets of disjoint Steiner triple systems III," *J. Combin. Theory, Ser. A*, vol. 34, no. 2, pp. 156–182, Mar. 1983.

[21] J. X. Lu, "On large sets of disjoint Steiner triple systems, VI," *J. Combin. Theory, Ser. A*, vol. 37, no. 2, pp. 189–192, Sep. 1984.

[22] L. Teirlinck, "A completion of Lu's determination of the spectrum for large sets of disjoint Steiner triple systems," *J. Combin. Theory Ser. A*, vol. 57, no. 2, pp. 302–305, Jul. 1991.

[23] T. Etzion, "Optimal partitions for triples," *J. Combin. Theory, Ser. A*, vol. 59, no. 2, pp. 161–176, Mar. 1992.

[24] T. Etzion, "Partitions of triples into optimal packings," *J. Combin. Theory, Ser. A*, vol. 59, no. 2, pp. 269–284, Mar. 1992.

[25] L. Ji, "Partition of triples of order $6k + 5$ into $6k + 3$ optimal packings and one packing of size $8k + 4$," *Graphs Combin.*, vol. 22, no. 2, pp. 251–260, Jun. 2006.

[26] A. Cayley, "IV. On the triadic arrangements of seven and fifteen things," *Philos. Mag. Ser.*, vol. 37, no. 247, pp. 50–53, Jul. 1850.

[27] X. Wang, H. Wei, C. Shangguan, and G. Ge, "New bounds and constructions for multiply constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6315–6327, 2016.

[28] V. A. Zinov'ev, "Generalized cascade codes," *Probl. Peredachi Inf.*, vol. 12, no. 1, pp. 5–15, 1976.

[29] C. Ding and J. Yin, "Combinatorial constructions of optimal constant-composition codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3671–3674, Oct. 2005.

[30] C. Ding and J. Yin, "A construction of optimal constant composition codes," *Designs, Codes Cryptogr.*, vol. 40, no. 2, pp. 157–165, Aug. 2006.

[31] S. Huczynska, "Equidistant frequency permutation arrays and related constant composition codes," *Designs, Codes Cryptogr.*, vol. 54, no. 2, pp. 109–120, Feb. 2010.

[32] D. Jungnickel, R. Mullin, and S. Vanstone, "The spectrum of α-resolvable block designs with block size 3," *Discrete Math.*, vol. 97, nos. 1–3, pp. 269–277, Dec. 1991.

[33] T. M. J. Vasiga, S. Furino, and A. C. H. Ling, "The spectrum of α-resolvable designs with block size four," *J. Combin. Designs*, vol. 9, no. 1, pp. 1–16, Jan. 2001.

Yeow Meng Chee (SM'08) received the B.Math. degree in computer science and combinatorics and optimization and the M.Math. and Ph.D. degrees in computer science from the University of Waterloo, Waterloo, ON, Canada, in 1988, 1989, and 1996, respectively.

Currently, he is a Professor at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Prior to this, he was Program Director of Interactive Digital Media R&D in the Media Development Authority of Singapore, Postdoctoral Fellow at the University of Waterloo and IBMs Zürich Research Laboratory, General Manager of the Singapore Computer Emergency Response Team, and Deputy Director of Strategic Programs at the Infocomm Development Authority, Singapore.

His research interest lies in the interplay between combinatorics and computer science/engineering, particularly combinatorial design theory, coding theory, extremal set systems, and electronic design automation.

Han Mao Kiah received his Ph.D. degree in mathematics from the Nanyang Technological University, Singapore in 2014. From 2014 to 2015, he was a Postdoctoral Research Associate at the Coordinated Science Laboratory, University of Illinois at Urbana–Champaign. Currently, he is a lecturer at the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. His research interests include combinatorial design theory, coding theory, and enumerative combinatorics.

Hui Zhang received the Ph.D. degree in Applied Mathematics from Zhejiang University, Hangzhou, Zhejiang, P. R. China in 2013. From 2013 to 2015, she was a Research Fellow in Nanyang Technological University in Singapore. Currently, she is working as Postdoctoral Researcher at the Department of Computer Science, Technion–Israel Institute of Technology. Her research interests include combinatorial theory, coding theory and cryptography, and their intersections.

Xiande Zhang received the Ph.D. degree in mathematics from Zhejiang University, Hangzhou, Zhejiang, P. R. China in 2009. From 2009 to 2015, she held postdoctoral positions in Nanyang Technological University and Monash University. Currently, she is a Research Professor at school of Mathematical Sciences, University of Science and Technology of China. Her research interests include combinatorial design theory, coding theory, cryptography, and their interactions.