Geometric Orthogonal Codes of Size Larger Than Optical Orthogonal Codes

Yeow Meng Chee, *Senior Member, IEEE*, Han Mao Kiah, San Ling, and Hengjia Wei

Dedicated to the memory of Solomon W. Golomb (1932–2016)

***Abstract*— The class of geometric orthogonal codes (GOCs) was introduced by Doty and Winslow (2016) for more robust macrobonding in DNA origami. They observed that GOCs are closely related to optical orthogonal codes (OOCs). It is possible for GOCs to have size greater than OOCs of corresponding parameters due to slightly more relaxed constraints on correlations. However, the existence of GOCs exceeding the size of optimal OOCs of corresponding parameters has never been demonstrated. This paper gives the first infinite family of GOCs of size greater than optimal OOCs.**

***Index Terms*— Base stacking, bonds, DNA nanotechnology, geometric orthogonal codes, optical orthogonal codes, optical orthogonal signature pattern codes.**

I. Introduction

NUCLEIC acids play an important role in the self assembly of nanostructures owing the specificity of the Watson-Crick base pairing. Rothemund [2] showed how a long strand of (scaffold) DNA can be folded into a specific shape (DNA origami) with the help of a carefully designed set of short "staple" DNAs that bind to intended sites on the scaffold DNA, forcing the scaffold DNA to fold in desired ways. Beyond base pairing, *base stacking* between base pairs is another dominant cause of DNA binding. Woo and Rothemund [3] showed that by careful placement of blunt ends in the DNA origami of Rothemund, we can force a set of DNA origamis to bind through base stacking to form intended arrangements. This geometric placement of blunt ends within a DNA origami forms a *macrobond*. Gerling *et al.* [4] extended the work of Woo and Rothemund [3] by studying the self-assembly of three-dimensional (3D) DNA origami. Doty and Winslow [5] then provided a theoretical foundation for the work of [3] and [4] by introducing the class of *geometric orthogonal codes* (GOCs). Doty and Winslow described how the class of codes can be used to design sets of macrobonds in 3D DNA origami so as to reduce undesirable bonding arising from misalignment and mismatches. We provide a short description of this connection in Fig. 1 and refer the interested readers to Doty and Winslow [5] for a detailed and excellent discussion. GOCs of large size are desirable because they give rise to large number of binding interactions, thereby increasing the number of structures that can potentially be formed.

Doty and Winslow also observed that GOCs are closely related to *optical orthogonal codes* (OOCs) introduced by Chung *et al.* [6]. Although it is possible for GOCs to have size larger than OOCs of corresponding parameters, this has never been demonstrated. The main contribution of this paper is the first construction of GOCs that is better than optimal OOCs. We also improve an upper bound of Doty and Winslow [5] on the size of GOCs.

Manuscript received May 30, 2017; revised October 30, 2017; accepted December 2, 2017. Date of publication December 29, 2017; date of current version March 15, 2018. This work was supported by the Singapore Ministry of Education under Research Grant MOE2015-T2-2-086. This paper was presented at the 2017 Proceedings of the IEEE International Symposium on Information Theory [1].

The authors are with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371 (e-mail: ymchee@ntu.edu.sg; hmkiah@ntu.edu.sg; lingsan@ntu.edu.sg; hjwei@ntu.edu.sg).

Communicated by P. V. Kumar, Guest Editor.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2017.2788140

II. Preliminaries

For integers $a \leq b$, $[a, b]$ denotes the set $\{a, a+1, \ldots, b\}$. For an integer $n \geq 2$, $[n]$ denotes the set $[0, n-1]$. Given $M \subseteq [n]^2$ and $\mathbf{v} \in \mathbb{Z}^2$, the *translation of M by* $\mathbf{v}$ is defined to be $M + \mathbf{v} = \{\mathbf{m} + \mathbf{v} : \mathbf{m} \in M\}$. We also refer to $M + \mathbf{v}$ as an *aperiodic translate of M*. The *aperiodic auto-correlation* of M is defined as $\max_{\mathbf{v} \in \mathbb{Z}^2 \setminus \{(0,0)\}} |M \cap (M + \mathbf{v})|$. For two subsets $M, M' \subseteq [n]^2$, the *aperiodic cross-correlation* of M and M' is defined as $\max_{\mathbf{v} \in \mathbb{Z}^2} |M \cap (M' + \mathbf{v})|$.

Let $w \in [2, n^2]$ and let $\lambda \in [1, w-1]$. A family $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ of size-w subsets (or w-subsets for short) of $[n]^2$ is an (n, w, λ)-*geometric orthogonal code* (GOC) if

(i) the aperiodic auto-correlation of M is $\leq \lambda$, for all $M \in \mathcal{M}$, and

(ii) the aperiodic cross-correlation of M and M' is $\leq \lambda$, for all $M, M' \in \mathcal{M}$ with $M \neq M'$.

The parameter w is called the *macrobond strength* (or *weight*) of $\mathcal{M}$, while λ is its *mismatch strength limit*. The values for macrobond strength w and mismatch strength limit λ are dependent on experimental conditions (e.g., temperature, concentrations) and their ratio is varied (see Doty and Winslow [5] for a discussion). Hence, we construct GOCs for a range of parameters of λ and w in this paper.

We note further that every $M \subseteq [n]^2$ may be identified with an $n \times n$ $(0,1)$-matrix $(m_{i,j})_{0 \leq i,j \leq n-1}$, where $m_{i,j} = 1$

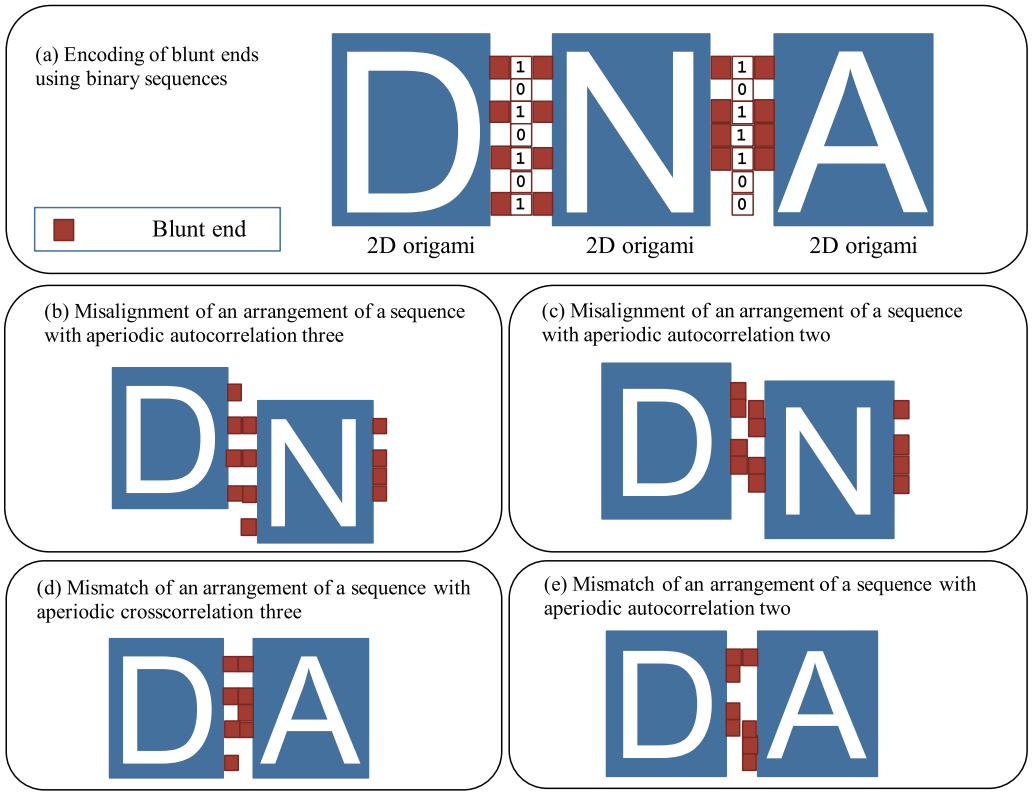

Fig. 1. (a) By carefully arranging blunt ends at the sides of DNA origamis, a set of DNA origamis may self-assemble into an intended arrangement. We can use binary sequences to encode the arrangements of blunt ends. (b) and (c) Misalignments of the intended pair, "D" and "N." We observe that we may reduce the probability of misalignment by choosing a sequence with low aperiodic auto-correlation. (d) and (e) A mismatch or binding of an unintended pair, "D" and "A." Again, the probability of mismatch is reduced by choosing sequences with low aperiodic cross-correlation.

if $(i, j) \in M$ and $m_{i,j} = 0$ otherwise. Hence, M represents the set of positions where the blunt ends are placed.

Let $M(n, w, \lambda)$ denote the largest possible size of an (n, w, λ)-GOC. A code with the largest size is said to be *optimal*. Doty and Winslow [5] derived the following upper bound for $M(n, w, \lambda)$.

Theorem 1 [5]: Let

$$\begin{aligned} &U_{\mathrm{GOC}}(n, w, \lambda) \\ &\quad \triangleq \frac{1}{\binom{w}{\lambda+1}} \left[\binom{n^2-1}{\lambda} + \sum_{x_0=1}^{n-1} \sum_{y_0=1}^{n-1} \binom{n^2 - x_0 - y_0 - 1}{\lambda - 1} \right] \\ &\quad = (1 + o(1)) \frac{(\lambda+1)^2 n^{2\lambda}}{w(w-1)(w-2)\cdots(w-\lambda)}. \end{aligned} \tag{1}$$

Then $M(n, w, \lambda) \leq U_{\mathrm{GOC}}(n, w, \lambda)$.

In the above theorem, for two functions f and g, we write $f = o(g)$ to mean that $\lim_{n\to\infty} f(n)/g(n) = 0$. As we are interested in the asymptotic behaviour of the upper bounds, we also adopt other Bachmann-Landau notations. We write $f = O(g)$ if $\limsup_{n\to\infty} \frac{|f(n)|}{g(n)} < C$ for some positive constant C. We write $f = \Omega(g)$ if $g = O(f)$, and we write $f = \Theta(g)$ if $f = O(g)$ and $f(n) = \Omega(g)$.

Let N be a positive integer, let $1 \leq \lambda \leq w \leq N$ and let $\mathbb{Z}_N$ denote the integers modulo N. Given a subset $C \subseteq \mathbb{Z}_N$ and an element $v \in \mathbb{Z}_N$, the *translation of C by v* is defined to be $C + v = \{c + v : c \in C\}$. The *periodic auto-correlation* of C is defined as $\max_{v \in \mathbb{Z}_N \setminus \{0\}} |C \cap (C + v)|$. For two subsets $C, C' \subseteq \mathbb{Z}_N$, the *periodic cross-correlation* of C and C' is defined as $\max_{v \in \mathbb{Z}_N} |C \cap (C' + v)|$. A collection $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$ of w-subsets of $\mathbb{Z}_N$ is an (N, w, λ)-*optical orthogonal code* (OOC) if the following conditions are satisfied:

(i) the periodic auto-correlation of C is $\leq \lambda$, for all $C \in \mathcal{C}$, and

(ii) the periodic cross-correlation of C and C' is $\leq \lambda$, for all $C, C' \in \mathcal{C}$ with $C \neq C'$.

Note that, for translations in the definition of OOCs, addition is performed over the *cyclic group* $\mathbb{Z}_N$, instead of over the integers as in the definition of GOCs.

Chung *et al.* [6] showed that the size of an (N, w, λ)-OOC is bounded above by $U_{\mathrm{OOC}}(N, w, \lambda)$, where

$$U_{\mathrm{OOC}}(N, w, \lambda) \triangleq \frac{(N-1)(N-2)\cdots(N-\lambda)}{w(w-1)(w-2)\cdots(w-\lambda)}. \tag{2}$$

Observe that an (n^2, w, λ)-OOC is an (n, w, λ)-GOC, by regarding each one-dimensional (1D) codeword of length n^2 as the concatenation of the n rows of a two-dimensional (2D) codeword. Comparing (1) and (2), with $N = n^2$, we note that the size of an (n, w, λ)-GOC could possibly exceed the upper bound $U_{\mathrm{OOC}}(n^2, w, \lambda)$. However, no such classes of GOCs are known. While Doty and Winslow [5] constructed a class of (p, p, λ)-GOCs of size $p^{\lambda-1} - p^{\lambda-2}$, for all primes p, and have compared this code size with some known lower bounds for OOCs, this code size does not beat the bound $U_{\mathrm{OOC}}(p^2, p, \lambda) = p^{\lambda-1} + O(p^{\lambda-2})$.

A. Our Contributions

The main contributions of this paper are:

- For suitably large w, an upper bound for $M(n, w, \lambda)$, which is asymptotically equal to (2), with $N = n^2$ (Section III).
- For $t \leq p$ and $p - \lfloor p/t \rfloor \leq \lambda \leq p$, a class of (p, p, λ)-GOCs of size $tp^{\lambda-1}-t$, which exceeds the OOC upper bound $p^{\lambda-1} + O(p^{\lambda-2})$ (Section IV-A).
- A recursive construction for GOCs, which can increase n while keeping w and λ fixed (Section IV-B). We also show that, if the input codes are close to optimal, so are the output codes. Examples of GOCs with size exceeding (2) are obtained.
- For $\lambda = 1$, an upper bound for $M(n, w, 1)$, which shows the upper bound $U_{\mathrm{GOC}}(n, w, 1) = \frac{4n(n-1)}{w(w-1)}$ cannot be attained when $w \geq 6$ (Section V-A). Some optimal $(n, w, 1)$-GOCs with $w \leq 5$ which achieve $U_{\mathrm{GOC}}(n, w, 1) = \frac{4n(n-1)}{w(w-1)}$ (Section V-B). We also determine the exact value of $M(n, 3, 1)$ for $n \notin \{19, 21, 24\}$ in Section V-C.

The techniques used are from combinatorial design theory.

III. An Asymptotic Upper Bound

In this section, we use a method of Erdõs *et al.* [7] to obtain an asymptotic upper bound on the size of (n, w, λ)-GOC when w is large. For $\mathbf{a} = (a_1, a_2) \in \mathbb{Z}^2$ and positive integer R, let $W_{\mathbf{a},R}$ be an $R \times R$ *window starting at* $\mathbf{a}$, that is, $W_{\mathbf{a},R} = [a_1, a_1+R-1]\times[a_2, a_2+R-1]$. For $S \subseteq [n]^2$, the *observation of S through the window $W_{\mathbf{a},R}$* is

$$W_{\mathbf{a},R}(S) = \{\mathbf{v} - \mathbf{a} : \mathbf{v} \in S \cap W_{\mathbf{a},R}\}.$$

Note that every observation, by definition, lies within $[R]^2$. The major difference of the proof technique used here with that for (1) in [5] is that we consider the local aperiodic correlations within $[R]^2$, rather than the aperiodic correlations within $[n]^2$, see Fig. 2.

Theorem 2: Let w and λ be functions in n. If $w = \Omega(\lambda^4\, n^c)$ for some positive constant c, then

$$M(n, w, \lambda) \leq (1 + o(1))\frac{n^{2\lambda}}{w^{\lambda+1}}.$$

Therefore,

$$\lim_{n\to\infty} M(n, w(n), \lambda(n))/U_{\mathrm{OOC}}(n^2, w(n), \lambda(n)) \leq 1.$$

Proof: Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be an (n, w, λ)-GOC. The number of $R \times R$ windows with nonempty intersection with $[n]^2$ is $(n+R-1)^2$, so the number of observations of macrobonds in $\mathcal{M}$ through these windows is $N = m(n + R - 1)^2$. Note that there may be repetitions. But since $\mathcal{M}$ is a GOC, that only happens for observations with weight less than $\lambda+1$. As each element of $[n]^2$ is observed through R^2 windows, the average number of elements per observation, over these N observations, is $A = R^2 mw/N$.

On the other hand, suppose the ith observation is of size w_i. Then it has precisely $\binom{w_i}{\lambda+1}$ subsets of size $\lambda + 1$. Therefore, there are in total $\sum_{i=1}^{N}\binom{w_i}{\lambda+1}$ subsets of size exactly $\lambda + 1$, induced by these N observations.

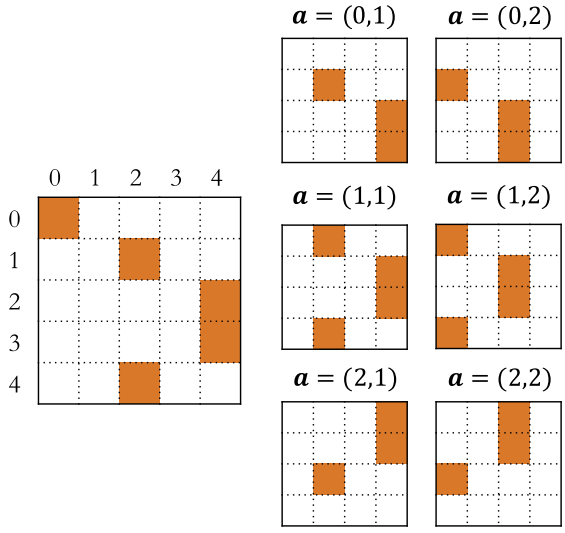

Fig. 2. The codeword $\{(0, 0), (1, 2), (2, 4), (3, 4), (4, 2)\}$ has aperiodic auto-correlation two. We list all the 4×4 windows with the weight of the observation at least three. All the 3-subsets induced on these windows are pairwise distinct. For example, in the window $W_{(0,1),4}$ the 3-subset is $\{(1, 1), (2, 3), (3, 3)\}$, while in $W_{(0,2),4}$ the 3-subset is $\{(1, 0), (2, 2), (3, 2)\}$. We have two observations of weight four and four observations of weight three. In total, there are twelve distinct 3-subsets of $[4]^2$, and this number is indeed at most $\binom{4^2}{3}$.

Now, since $\mathcal{M}$ is an (n, w, λ)-GOC, we have $|W_{\mathbf{a},R}(M_i) \cap W_{\mathbf{b},R}(M_j)| \leq \lambda$ for any two distinct observations $W_{\mathbf{a},R}(M_i)$ and $W_{\mathbf{b},R}(M_j)$, with $\mathbf{a} \neq \mathbf{b}$ or $i \neq j$. Therefore, all the $(\lambda + 1)$-subsets, induced from the observations, are pairwise distinct. The number of possible $(\lambda + 1)$-subsets in an $R \times R$ window is $\binom{R^2}{\lambda+1}$. Since all observations lie within the $R \times R$ window $[R]^2$, we have

$$\sum_{i=1}^{N}\binom{w_i}{\lambda+1} \leq \binom{R^2}{\lambda+1}.$$

Note that $A = \frac{\sum_{i=1}^{N} w_i}{N}$. It follows from the convexity of the function $\binom{x}{\lambda+1}$ in variable x and Jensen's inequality that

$$\binom{A}{\lambda+1} \leq \frac{1}{N}\sum_{i=1}^{N}\binom{w_i}{\lambda+1} \leq \frac{1}{N}\binom{R^2}{\lambda+1}.$$

In other words, $NA(A-1)\cdots(A-\lambda) \leq R^{2\lambda+2}$, or, $mw(A-1)\cdots(A-\lambda) \leq R^{2\lambda}$.

Choose $R = n^{1-c/4}$. Since $w = \Omega(\lambda^4\, n^c)$, we have $A = R^2 w/(n + R - 1)^2 = \Omega(\lambda^4 n^{c/2})$. It follows that for n large enough, we have

$$(A-1)(A-2)\cdots(A-\lambda) \geq A^{\lambda} - \lambda^2\, A^{\lambda-1}.$$

Hence, $mw(A^{\lambda} - \lambda^2\, A^{\lambda-1}) \leq R^{2\lambda}$, and

$$\begin{aligned} m &\leq \frac{R^{2\lambda}}{wA^{\lambda}} + \frac{m\lambda^2}{A} = \frac{(n + R - 1)^{2\lambda}}{w^{\lambda+1}} + \frac{m\lambda^2}{A}, \\ &= \frac{n^{2\lambda}}{w^{\lambda+1}} + o\left(\frac{n^{2\lambda}}{w^{\lambda+1}}\right) + \frac{m\lambda^2}{A} \\ &= \frac{n^{2\lambda}}{w^{\lambda+1}} + o\left(\frac{n^{2\lambda}}{w^{\lambda+1}}\right). \end{aligned}$$

The last equation holds as $m = O(\lambda^2 n^{2\lambda}/w^{\lambda+1})$ and so $m\lambda^2/A = o(n^{2\lambda}/w^{\lambda+1})$. □

It follows that both OOCs and GOCs share the same asymptotic upper bound when $w = \Omega(\lambda^4 n^c)$, for any constant $c > 0$.

IV. Constructions of GOCs Using Cyclic GOCs

We revisit another class of low-correlation codes that had been studied in the context of optical code-division multiple access (CDMA) networks. These codes form an important ingredient in the constructions of the two families GOCs in later two subsections.

Let $\mathcal{M}$ be a family of w-subsets of $\mathbb{Z}_m \times \mathbb{Z}_n$. For $M \in \mathcal{M}$, the *periodic auto-correlation* of M is given by the value $\max_{\mathbf{v}\in(\mathbb{Z}_m\times\mathbb{Z}_n)\setminus\{(0,0)\}} |M \cap (M+\mathbf{v})|$. For distinct $M, M' \in \mathcal{M}$, the *periodic cross-correlation* of M and M' is defined as $\max_{\mathbf{v}\in\mathbb{Z}_m\times\mathbb{Z}_n} |M \cap (M'+\mathbf{v})|$. (Note that the translations are computed over the group $\mathbb{Z}_m \times \mathbb{Z}_n$.) Such a family $\mathcal{M}$ is called an (m, n, w, λ)-*optical orthogonal signature pattern code* (OOSPC) if, for $M, M' \in \mathcal{M}$ with $M \neq M'$, we have:

(i) the periodic auto-correlation of M is $\leq \lambda$, and
(ii) the periodic cross-correlation of M and M' is $\leq \lambda$.

Optical orthogonal signature pattern codes were studied in the context of optical CDMA networks [8]–[12] . When m and n are relatively prime, using Chinese remainder theorem, it is easy to see that an (m, n, w, λ)-OOSPC is equivalent to an (mn, w, λ)-OOC [12]. Moreno *et al.* [13] presented three constructions for OOSPCs to obtain the corresponding OOCs. When m and n are not relatively prime, Yang and Kwong [12] gave three constructions for OOSPCs with periodic cross-correlation 1; some infinite classes of (m, n, w, λ)-OOSPCs with $w \in \{3, 4\}$ and $\lambda \in \{1, 2\}$ have been obtained in [14]–[18]. Recently, inspired by the algebraic constructions for 2D OOCs based on polynomials and rational functions over finite fields [19] and the recursive construction for 1D OOC based on r-simple matrices [20], Ji *et al.* [21] presented direct and recursive constructions for OOSPCs with arbitrary periodic correlations.

In this paper, we restrict ourselves to the case where $m = n$. Each codeword may then be visualized as a square array. When a translation is applied to such a codeword, entries in the codeword that move off one edge of the array reappear in the array from the opposite edge (due to the modulo n operation), unlike in the case of a GOC, where the symbols simply move out of the array. Therefore, identifying $\mathbb{Z}_n^2$ with $[n]^2$ as sets in the obvious way, it is easy to see the periodic auto-correlation (resp. periodic cross-correlation) in the OOSPC definition is always no less than the aperiodic auto-correlation (resp. aperiodic cross-correlation) in the GOC definition. It follows that an (n, n, w, λ)-OOSPC is also an (n, w, λ)-GOC. For these reasons, we shall refer to an (n, n, w, λ)-OOSPC as an (n, w, λ)-*cyclic geometric orthogonal code* (CGOC). These codes are used in Section IV-A to construct GOCs whose size exceeds (2), with $N = n^2$.

Although an (n^2, w, λ)-OOC is an (n, w, λ)-GOC and the translations in both OOCs and CGOCs are done modulo n, there are differences in their properties. Consider, for example, the codeword (011100000) in Fig. 3. As a 1D codeword of length nine, it has periodic auto-correlation two. However, when interpreted as the corresponding 2D codeword $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, its periodic auto-correlation is one.

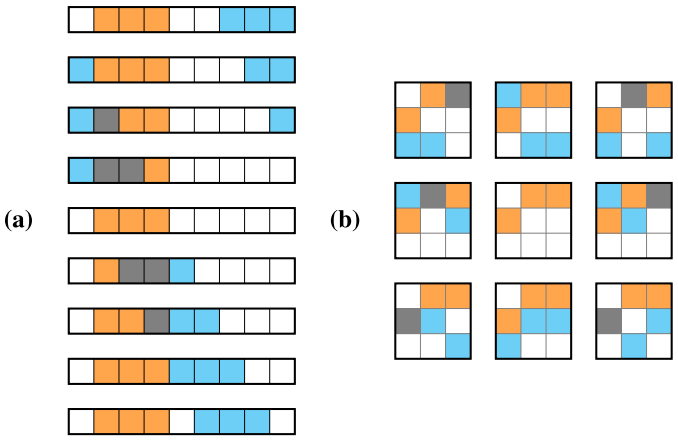

Fig. 3. **(a)** The 1D codeword (011100000) is marked in orange, all its possible translations are marked in blue and the overlaps are marked in grey. **(b)** The corresponding 2D codeword and all its possible translations. The overlaps are marked in grey.

Let $C(n, w, \lambda)$ denote the largest possible size of an (n, w, λ)-CGOC. Since CGOCs may be regarded as binary constant weight codes (by identifying subsets of $\mathbb{Z}_n^2$ with $n \times n$ $(0, 1)$-matrices), by using the Johnson bound [22] for constant weight codes, we have the following upper bound on $C(n, w, \lambda)$.

Theorem 3 (Johnson-Type Bound): Let

$$U_{\mathrm{CGOC}}(n, w, \lambda) \triangleq \frac{(n^2-1)(n^2-2)\cdots(n^2-\lambda)}{w(w-1)(w-2)\cdots(w-\lambda)}.$$

Then $C(n, w, \lambda) \leq U_{\mathrm{CGOC}}(n, w, \lambda)$.

Although $U_{\mathrm{CGOC}}(n, w, \lambda) = U_{\mathrm{OOC}}(n^2, w, \lambda)$, CGOCs have the potential to yield GOCs whose size exceeds (2), since the periodic correlation in the CGOC definition may be larger than the aperiodic correlation in GOC definition and there is room to add more codewords.The following two results on CGOCs are used later in Corollary 8 and Theorem 11, respectively to give infinite classes of GOCs.

Theorem 4 [21]:Let $p \geq 3$ be a prime and λ an integer with $2 \leq \lambda \leq p$, then there is a (p, p, λ)-CGOC of size $p^{\lambda-1} - 1$.

Theorem 5 [21]: Let $\mathcal{C}$ be an (n, w, λ)-CGOC with $w > \lambda$. Let N be a positive integer such that the minimal prime factor of N is not less that $w-1$, then there is an (nN, w, λ)-CGOC of size $N^{2\lambda}|\mathcal{C}|$.

A. Direct Construction of GOCs From CGOCs

Recall that an (n, w, λ)-CGOC is also an (n, w, λ)-GOC. The following result therefore follows immediately from Theorem 4.

Corollary 6: Let $p \geq 3$ be a prime and λ an integer with $2 \leq \lambda \leq p$. Then there is a (p, p, λ)-GOC of size $p^{\lambda-1} - 1$.

When $\lambda = O\left(p^{1/4-\epsilon}\right)$ for some $\epsilon > 0$, the condition in Theorem 2 is satisfied. In other words, $M(p, p, \lambda) \leq p^{\lambda-1}+o(p^{\lambda-1})$, so the codes in Corollary 6 are asymptotically optimal. However, when $\lambda = \Omega(p^{1/4})$, the condition in Theorem 2 does not hold. Indeed, for some values of λ satisfying $\lambda = \Theta(p)$, we construct, in this section, some GOCs with sizes $tp^{\lambda-1} - O(1)$, where t may be chosen to be greater than one.

In what follows, we canonically identify the elements in $[n]$ with those in $\mathbb{Z}_n$. Given $M \subseteq [n]^2$ and $\mathbf{v} = (v_a, v_b) \in [n]^2$, let the *translation of M by $\mathbf{v}$ modulo n* be $M + \mathbf{v} \pmod n \triangleq \{(m_a+v_a \bmod n, m_b+v_b \bmod n) : (m_a, m_b) \in M\}$. As before, we refer to $M + \mathbf{v} \pmod n$ as a *periodic translate of M*.

Suppose that $\mathcal{M}$ is an (n, w, λ)-CGOC and M is a codeword belonging to $\mathcal{M}$. Then all periodic translates of M are excluded from $\mathcal{M}$ as the periodic correlation of M and its periodic translate M' is always w. However, the aperiodic cross-correlation of M and M' may be smaller than w and our strategy is to augment $\mathcal{M}$ with such periodic translates to obtain a GOC of larger size.

We focus our strategy on a certain class of CGOCs. In particular, suppose that M is a w-subset of $[n]^2$ such that $|M\cap(\{i\}\times\mathbb{Z}_n)| \leq 1$ for each $i \in \mathbb{Z}_n$. In other words, regarding M as an $n \times n$ $(0, 1)$-matrix, there is at most one 1 in each row of M.

Let $1 \leq t \leq w$ and set $\gamma = \lfloor w/t \rfloor$. We partition the rows of M into $t + 1$ contiguous parts $[v_{j-1}, v_j - 1]$ for $j = 1, \ldots, t+1$ (here, $v_0 = 0$ and $v_{t+1} = n$) such that each of the first t parts contains exactly γ 1's. In other words, the size $M \cap ([v_{j-1}, v_j - 1] \times [n])$ is exactly γ.

We then define the following t matrices $\mathrm{tr}(M, i) = M - (v_i, 0) \pmod n$ for $i \in [1, t]$. Observe that $\mathrm{tr}(M, i)$ is a periodic translate of M. Furthermore, for $i \in [1, t]$, the aperiodic translate $M+(n-v_i, 0)$ has exactly $i\gamma$ 1's in $[n]^2$, i.e. $\left|[n]^2 \cap (M + (n - v_i, 0))\right| = i\gamma$.

Example 7: Let $n = w = 7$ and consider a codeword $M = \{(0, 0), (1, 1), (2, 2), (3, 4), (4, 1), (5, 5), (6, 6)\}$ depicted in Fig. 4. Then the periodic auto-correlation of M is four.

Consider $t = 2$ and so, $\gamma = 3$. Hence, the rows are partitioned to the three parts $[0, 2]$, $[3, 5]$, *and* $[6, 6]$.

Then the two periodic translates we are interested in are:

$$\mathrm{tr}(M, 1) = \{(4, 0), (5, 1), (6, 2), (0, 4), (1, 1), (2, 5), (3, 6)\},$$
$$\mathrm{tr}(M, 2) = \{(1, 0), (2, 1), (3, 2), (4, 4), (5, 1), (6, 5), (0, 6)\}.$$

By construction, $\mathrm{tr}(M, 1)$ *and* $\mathrm{tr}(M, 2)$ *each has aperiodic auto-correlation four. Furthermore, it is easy to check that* $\mathrm{tr}(M, 1)$ *and* $\mathrm{tr}(M, 2)$ *have aperiodic cross-correlation four, even though their periodic cross-correlation is seven.*

With this definition of $\mathrm{tr}(M, i)$, we provide our first construction of GOCs using CGOCs.

Construction 1: Suppose that there exists an (n, w, λ)-CGOC $\mathcal{M}$ such that, for each $M \in \mathcal{M}$ and each $i \in \mathbb{Z}_n$, we have $|M \cap (\{i\} \times \mathbb{Z}_n)| \leq 1$. For any positive integer t with $t \leq w$, let

$$\mathcal{F} = \{\mathrm{tr}(M, i) : M \in \mathcal{M}, i \in [1, t]\}.$$

If $w - \lfloor w/t \rfloor \leq \lambda$, then $\mathcal{F}$ is an (n, w, λ)-GOC of size $t|\mathcal{M}|$.

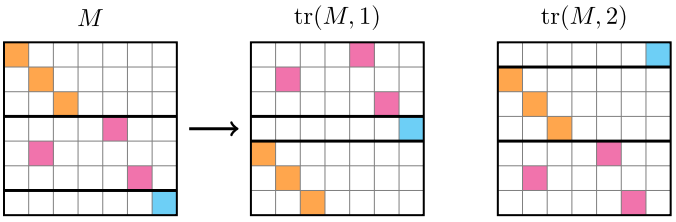

Fig. 4. The codewords M, $\mathrm{tr}(M, 1)$, and $\mathrm{tr}(M, 2)$ in Example 7.

Proof: Since $\mathcal{M}$ is an (n, w, λ)-CGOC, it is easy to check that $\{\mathrm{tr}(M, i) : M \in \mathcal{M}\}$ is also an (n, w, λ)-CGOC for $i \in [1, t]$. It then remains to show that the aperiodic cross-correlation of $\mathrm{tr}(M, i)$ and $\mathrm{tr}(M', j)$ with $i \neq j$ is at most λ.

Let v_i and v'_j be the integers such that $\mathrm{tr}(M, i) = M-(v_i, 0) \pmod n$ and $\mathrm{tr}(M', j) = M' - (v'_j, 0) \pmod n$. When $M \neq M'$, then for all $\mathbf{u} \in \mathbb{Z}^2$, we have that

$$\begin{aligned}
&|\mathrm{tr}(M, i) \cap (\mathrm{tr}(M', j) + \mathbf{u})| \\
&= |(M - (v_i, 0) \pmod n) \cap (M' - (v'_j, 0) + \pmod n) + \mathbf{u}| \\
&\leq |(M - (v_i, 0) \pmod n) \cap (M' - (v'_j, 0) + \mathbf{u} \pmod n)| \\
&= |M \cap (M' + (v_i - v'_j, 0) + \mathbf{u} \pmod n)| \\
&\leq \lambda.
\end{aligned}$$

The last inequality holds due to the periodic cross-correlation property of $\mathcal{M}$ as CGOC. Similarly, when $M = M'$ and $\mathbf{u} \not\equiv (v_j - v_i, 0) \pmod n$, similar calculations yield that the aperiodic cross-correlation of $\mathrm{tr}(M, i)$ and $\mathrm{tr}(M, j)$ is at most λ.

It remains to consider the case $M = M'$ and $\mathbf{u} \equiv (v_j - v_i, 0) \pmod n$. Denote $M_\ell = M\cap([v_{\ell-1}, v_\ell - 1]\times[n])$ for $\ell \in [1, t]$. Then the collection $\{M_1, M_2, \ldots, M_{t+1}\}$ forms a partition of M with $|M_\ell| = \gamma$ for $\ell \neq t+1$ and $|M_{t+1}| \leq \gamma$. Furthermore,

$$\begin{aligned}
\mathrm{tr}(M, i) &= M - (v_i, 0) \pmod n \\
&= \left(\bigcup_{\ell=1}^{i} M_\ell + (n - v_i, 0))\right) \cup \left(\bigcup_{\ell=i+1}^{t+1} M_\ell - (v_i, 0)\right).
\end{aligned}$$

Hence, for $\mathrm{tr}(M, i)$ and $\mathrm{tr}(M, j)$ with $i < j$, and $\mathbf{u} = (v_j - v_i, 0) + (pn, qn)$ with $p, q \in \mathbb{Z}$, we have the following cases.

(i) When $(p, q) = (0, 0)$, we have

$$\begin{aligned}
&\mathrm{tr}(M, j) + \mathbf{u} \\
&= \left(\bigcup_{\ell=1}^{j} M_\ell + (n - v_i, 0))\right) \cup \left(\bigcup_{\ell=j+1}^{t+1} M_\ell - (v_i, 0)\right),
\end{aligned}$$

and so,

$$\begin{aligned}
&|\mathrm{tr}(M, i) \cap (\mathrm{tr}(M, j) + \mathbf{u})| \\
&= \sum_{\ell=1}^{i} |M_\ell| + \sum_{\ell=j+1}^{t+1} |M_\ell| = w - (j - i)\gamma \leq w - \gamma \leq \lambda.
\end{aligned}$$

(ii) When $(p, q) = (-1, 0)$, we have

$$\begin{aligned}
&\mathrm{tr}(M, j) + \mathbf{u} \\
&= \left(\bigcup_{\ell=1}^{j} M_\ell + (-v_i, 0))\right) \cup \left(\bigcup_{\ell=j+1}^{t+1} M_\ell + (-n - v_i, 0)\right),
\end{aligned}$$

TABLE I
COMPARISON OF $L_C(n,\lambda,t)$ WITH THE LOWER BOUND $L_1(n,\lambda)$ IN [5, TABLE 1]

n	λ	$L_1(n,\lambda)$	t	$L_C(n,\lambda,t)$
5	3	20	2	48
5	4	100	5	496
7	4	294	2	684
7	5	2,058	3	7,200
7	6	14,406	7	117,642
11	6	146,410	2	322,100

and so,

$$|\mathrm{tr}(M,i)\cap(\mathrm{tr}(M,j)+\mathbf{u})| = \sum_{\ell=i+1}^{j}|M_\ell| \le (j-i)\gamma \le (t-1)\gamma \le w-\gamma \le \lambda.$$

(iii) When $(p,q)\notin\{(0,0),(-1,0)\}$, then $(\mathrm{tr}(M,j)+\mathbf{u})\cap[n]^2=\varnothing$ and then $|\mathrm{tr}(M,i)\cap(\mathrm{tr}(M,j)+\mathbf{u})|=0$.

Therefore, the cross-correlation of $\mathrm{tr}(M,i)$ and $\mathrm{tr}(M',j)$ is always at most λ. □

It can be verified that the CGOCs in Theorem 4 satisfy the condition of Construction 1. We may therefore apply Construction 1 to obtain the following class of (p,p,λ)-GOCs, whose size exceeds the OOC upper bound $p^{\lambda-1}+O(p^{\lambda-2})$.

Corollary 8: Let $p\ge 3$ be a prime. Let λ and t be two positive integers with $t\le p$ and $p-\lfloor p/t\rfloor\le\lambda\le p$. Then there is a (p,p,λ)-GOC of size $tp^{\lambda-1}-t$.

Let $L_C(n,\lambda,t)=tn^{\lambda-1}-t$ and we compare $L_C(n,\lambda,t)$ with the lower bound of [5, Table 1].

To end this subsection, we discuss the complexity of Construction 1. As mentioned above, given a codeword M in a CGOC $\mathcal{M}$ satisfying the conditions of the construction, we form t matrices $\mathrm{tr}(M,1),\mathrm{tr}(M,2),\ldots,\mathrm{tr}(M,t)$ by partitioning the rows of M into $t+1$ parts and shifting them cyclically. Therefore, we can construct these t matrices in time $O(tn)$.

It remains to determine the complexity of constructing the CGOC $\mathcal{M}$. To so, we specialize our analysis on Doty and Winslow's construction for CGOCs [5]. They consider the polynomials $f(x)=a_\lambda x^\lambda+a_{\lambda-1}x^{\lambda-1}+\cdots+a_1x+a_0$, where the coefficients $a_i\in\mathbb{F}_p$ for $i\in[0,\lambda]$ obey $a_{\lambda-1}=a_0=0$ and $a_\lambda\neq 0$. The codewords are given by $M_f=\{(x,f(x): x\in\mathbb{F}_p)\}$. It is easy to check that each codeword has exactly one 1 in each row and Doty and Winslow showed that these codewords form a (p,p,λ)-CGOC of size $p^{\lambda-1}-p^{\lambda-2}$. We may therefore apply Construction 1 with this CGOC and obtain a (p,p,λ)-GOC of size $tp^{\lambda-1}-tp^{\lambda-2}$. Since to form each codeword in the CGOC requires $O(\lambda p)$ time and there are $O(p^{\lambda-1})$ codewords, Doty and Winslow's CGOC may be constructed in $O(\lambda p^\lambda)$ time and the GOC resulting from Construction 1 may be constructed in $O((\lambda+t)p^\lambda)$.

B. Recursive Construction of GOCs

In this section, we introduce a recursive approach to construct (n,w,λ)-GOCs of large size. We have the following interpretation for GOCs.

Proposition 9: Let $\mathcal{M}=\{M_1,M_2,\ldots,M_m\}$ be a family of w-subsets of $[n]^2$. $\mathcal{M}$ is an (n,w,λ)-GOC if and only if

(i) for each $M_i\in\mathcal{M}$, any nonzero $\mathbf{v}\in\mathbb{Z}^2$ can be represented as a difference $\mathbf{m}-\mathbf{m}'$ with $\mathbf{m},\mathbf{m}'\in M_i$ at most λ times, and

(ii) for each pair of $M_i,M_j\in\mathcal{M}$ with $i\neq j$, any $\mathbf{v}\in\mathbb{Z}^2$ can be represented as a difference $\mathbf{m}-\mathbf{m}'$ with $\mathbf{m}\in M_i$ and $\mathbf{m}'\in M_j$ at most λ times.

In addition to CGOCs, permutation codes constitute another key ingredient in our method.

Let S_n be the set of permutations on the set $\{1,2\ldots,n\}$. Write a permutation $\boldsymbol{\pi}\in S_n$ in the form $\boldsymbol{\pi}=(\pi_1,\pi_2,\ldots,\pi_n)$. The *Hamming distance* between two permutations $\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\ldots,\sigma_n)$ and $\boldsymbol{\pi}=(\pi_1,\pi_2,\ldots,\pi_n)$ in S_n is defined to be $d_H(\boldsymbol{\sigma},\boldsymbol{\pi})=|\{i:\sigma_i\neq\pi_i\}|$.

For $1\le d\le n$, we say that $\emptyset\neq\mathcal{C}\subseteq S_n$ is an (n,d)-*permutation code* if $d_H(\boldsymbol{\sigma},\boldsymbol{\pi})\ge d$ for every two distinct permutations $\boldsymbol{\sigma},\boldsymbol{\pi}\in\mathcal{C}$. Let the largest possible size of an (n,d)-permutation code be denoted by $P(n,d)$. Bounds on $P(n,d)$ and the exact values of $P(n,d)$ under some specific parameters have been studied in [23]. In particular, we have $P(n,d)\le n!/(d-1)!$.

We now present a recursive construction for GOCs.

Construction 2: Let $\mathcal{A}=\{A_1,A_2,\ldots,A_{m_1}\}$ be an (n_1,w,λ)-CGOC, let $\mathcal{C}=\{C_1,C_2,\ldots,C_{m_2}\}$ be an (n_2,w,λ)-GOC, and let $\mathcal{P}=\{\boldsymbol{\pi}_1,\boldsymbol{\pi}_2,\ldots,\boldsymbol{\pi}_{m_0}\}$ be a $(w,w-\lambda)$-permutation code.

For each $A_i=\{(a_{i1},b_{i1}),(a_{i2},b_{i2}),\ldots,(a_{iw},b_{iw})\}\in\mathcal{A}$, $C_j=\{(c_{j1},d_{j1}),(c_{j2},d_{j2}),\ldots,(c_{jw},d_{jw})\}\in\mathcal{C}$ and $\boldsymbol{\pi}_k\in\mathcal{P}$, construct a new codeword F_{ijk} as follows:

$$F_{ijk}=\{(a_{i\ell}+n_1\ c_{j\boldsymbol{\pi}_k(\ell)},b_{i\ell}+n_1\ d_{j\boldsymbol{\pi}_k(\ell)}):1\le\ell\le w\}.$$

Let

$$\mathcal{F}=\{F_{ijk}:1\le i\le m_1,1\le j\le m_2,1\le k\le m_0\}.$$

Then $\mathcal{F}$ is an (n_1n_2,w,λ)-GOC of size $m_0\ m_1\ m_2$.

Proof: We first show that the aperiodic auto-correlation of any F_{ijk} is $\le\lambda$. Since the periodic auto-correlation of $\mathcal{A}$ as CGOC is $\le\lambda$, any $(x,y)\in\mathbb{Z}_{n_1}^2\backslash\{(0,0)\}$ can be represented as

$$(a_{i\alpha}-a_{i\beta}\pmod{n_1},b_{i\alpha}-b_{i\beta}\pmod{n_1})$$

with $1\le\alpha,\beta\le w$ and $\alpha\neq\beta$ at most λ ways. Now, for any codeword $F_{ijk}\in\mathcal{F}$, any difference

$$(a_{i\alpha}+n_1\ c_{j\boldsymbol{\pi}_k(\alpha)}-a_{i\beta}-n_1\ c_{j\boldsymbol{\pi}_k(\beta)},b_{i\alpha}+n_1\ d_{j\boldsymbol{\pi}_k(\alpha)}-b_{i\beta}-n_1\ d_{j\boldsymbol{\pi}_k(\beta)})$$

can occur at most λ times, as this difference is congruent to $(a_{i\alpha}-a_{i\beta},b_{i\alpha}-b_{i\beta})$ modulo n_1, which occurs at most λ times. So $\mathcal{F}$ has low aperiodic auto-correlation.

To check the aperiodic cross-correlation property, we need to verify two cases.

(i) First we check the aperiodic cross-correlation between F_{ijk} and $F_{i'j'k'}$ with $i\neq i'$. This means that these two codewords are constructed based on different codewords in $\mathcal{A}$.

Since the periodic cross-correlation of $\mathcal{A}$ as CGOC is $\le\lambda$, any element (x,y) in $\mathbb{Z}_{n_1}^2$ can be represented as

$$(a_{i\alpha}-a_{i'\beta}\pmod{n_1},b_{i\alpha}-b_{i'\beta}\pmod{n_1})$$

with $1 \le \alpha, \beta \le w$ at most λ ways. Then any difference

$$(a_{i\alpha} + n_1\ c_{j\boldsymbol{\pi}_k(\alpha)} - a_{i'\beta} - n_1\ c_{j'\boldsymbol{\pi}_{k'}(\beta)},\ b_{i\alpha} + n_1\ d_{j\boldsymbol{\pi}_k(\alpha)} - b_{i'\beta} - n_1\ d_{j'\boldsymbol{\pi}_{k'}(\beta)})$$

can occur at most λ times, as this difference is congruent to $(a_{i\alpha} - a_{i'\beta}, b_{i\alpha} - b_{i'\beta})$ modulo n_1.

(ii) Now, we check the aperiodic cross-correlation between F_{ijk} and $F_{ij'k'}$. Consider the differences

$$(a_{i\alpha} + n_1\ c_{j\boldsymbol{\pi}_k(\alpha)} - a_{i\beta} - n_1\ c_{j'\boldsymbol{\pi}_{k'}(\beta)},\ b_{i\alpha} + n_1\ d_{j\boldsymbol{\pi}_k(\alpha)} - b_{i\beta} - n_1\ d_{j'\boldsymbol{\pi}_{k'}(\beta)}),$$

with $1 \le \alpha, \beta \le w$. All of these differences fall into two disjoint sets according to whether $\alpha = \beta$ or not.

a) If $\alpha \ne \beta$, the difference cannot be congruent to $(0, 0)$ modulo n_1. With the same argument as in the proof of the low aperiodic auto-correlation, we can show such difference cannot occur more than λ times.

b) If $\alpha = \beta$, the difference is equal to

$$n_1(c_{j\boldsymbol{\pi}_k(\alpha)} - c_{j'\boldsymbol{\pi}_{k'}(\alpha)}, d_{j\boldsymbol{\pi}_k(\alpha)} - d_{j'\boldsymbol{\pi}_{k'}(\alpha)}).$$

When $j \ne j'$, such difference cannot occur more than λ times due to the aperiodic cross-correlation of $\mathcal{C}$. When $j = j'$ and $k \ne k'$, there are at most λ pairs $(\boldsymbol{\pi}_k(\alpha), \boldsymbol{\pi}_{k'}(\alpha))$ with $\boldsymbol{\pi}_k(\alpha) = \boldsymbol{\pi}_{k'}(\alpha)$ as α ranges from 1 to w. Thus the zero difference $(0, 0)$ appears at most λ times. The case of the nonzero difference follows from the aperiodic auto-correlation property of $\mathcal{C}$.

Then we complete the proof. □

Example 10: Suppose $A = \{(0, 1), (0, 2), (1, 0)\}$ *is a codeword of a* $(3, 3, 1)$*-CGOC and* $C = \{\mathbf{(0, 1), (1, 0), (1, 1)}\}$ *is a codeword of a* $(3, 3, 1)$*-GOC. We construct a codeword* F_1 *as*

$$\begin{aligned} F_1 &= \{0 + 3 \cdot \mathbf{0}, 1 + 3 \cdot \mathbf{1}), (0 + 3 \cdot \mathbf{1}, 2 + 3 \cdot \mathbf{0}), \\ &\qquad (1 + 3 \cdot \mathbf{1}, 0 + 3 \cdot \mathbf{1})\} \\ &= \{(0, 4), (3, 2), (4, 3)\}. \end{aligned}$$

Then we switch the last two elements $(1, 0)$ *and* $(1, 1)$ *in* C *and construct another codeword* F_2 *as*

$$\begin{aligned} F_1 &= \{0 + 3 \cdot \mathbf{0}, 1 + 3 \cdot \mathbf{1}), (0 + 3 \cdot \mathbf{1}, 2 + 3 \cdot \mathbf{1}), \\ &\qquad (1 + 3 \cdot \mathbf{1}, 0 + 3 \cdot \mathbf{0})\} \\ &= \{(0, 4), (3, 5), (4, 0)\}. \end{aligned}$$

The family $\{F_1, F_2\}$ *is a* $(9, 3, 1)$*-GOC of size two.*

In Construction 2, suppose that

$$\begin{aligned} m_1 &= \alpha \frac{n_1^{2\lambda}}{w(w-1)\cdots(w-\lambda)}, \\ m_2 &= \beta \frac{n_2^{2\lambda}}{w(w-1)\cdots(w-\lambda)}, \text{ and} \\ m_0 &= \gamma\, w(w-1)\cdots(w-\lambda), \end{aligned}$$

where $\alpha, \gamma \le 1$ and $\beta \le (\lambda + 1)^2$. Then we can obtain an $(n_1 n_2, w, \lambda)$-GOC of size $\alpha\beta\gamma\,(n_1 n_2)^{2\lambda}/w(w-1)\cdots(w-\lambda)$. Recall that

$$U_{\mathrm{GOC}}(n_1 n_2, w, \lambda) = (\lambda + 1)^2 \frac{(n_1 n_2)^{2\lambda}}{w(w-1)\cdots(w-\lambda)} + o\left((n_1 n_2)^{2\lambda}\right).$$

TABLE II
COMPARISON OF THE COEFFICIENT c WITH U^*_{GOC} AND U^*_{OOC}

n_1	n_2	w	λ	U^*_{OOC}	U^*_{GOC}	c
4	3	4	2	864	7,776	2,112
5	4	4	2	6,666	60,000	23,688
7	6	4	2	129,654	1,166,886	644,160
4	4	5	2	1,092	9,830	2,520
5	5	5	2	6,510	58,593	17,640
7	6	5	2	51,861	466,754	155,520
7	5	6	2	12,505	112,546	16,200
7	6	6	2	25,930	233,377	36,720
3	4	5	3	24,883	398,133	37,440
5	5	5	3	2,034,505	32,552,083	6,748,800
7	6	5	3	45,741,931	731,870,899	198,374,400
7	4	6	3	1,338,584	21,417,346	1,651,680
7	6	6	3	15,247,310	243,956,966	30,636,000
4	6	6	4	155,882,380	3,822,059,520	322,560,000

Hence, if α and γ are close to 1 and β is close to $(\lambda + 1)^2$, the size of the resultant code is close to this upper bound. In other words, if the ingredients $\mathcal{A}$, $\mathcal{C}$, and $\mathcal{P}$ in Construction 2 are "close to optimal", then the new GOC $\mathcal{F}$ obtained is also "close to optimal."

When $w \le 6$ and $\lambda < w$, Chu *et al.* [23] showed that a $(w, w - \lambda)$-permutation code of size $w(w-1)\cdots(w-\lambda)$ exists. Therefore, we have the following result on the size of codes resulting from Construction 2 for $w \le 6$.

Theorem 11: Let $w \in \{3, 4, 5, 6\}$ *and let* N *be a positive integer whose minimal prime factor is not less than* $w - 1$. *Suppose that there exists an* (n_1, w, λ)*-CGOC of size* m_1 *and an* (n_2, w, λ)*-GOC of size* m_2. *Then there exists an* $(n_1 n_2 N, w, \lambda)$*-GOC of size* $cN^{2\lambda}$, *where* $c = m_1 m_2 w(w-1)\cdots(w-\lambda)$.

Proof: Applying Theorem 5 to the (n_1, w, λ)-CGOC gives an $(n_1 N, w, \lambda)$-CGOC of size $m_1 N^{2\lambda}$. Applying Construction 2 with this CGOC, together with the (n_2, w, λ)-GOC and the $(w, w - \lambda)$-permutation code from [23], then yields an $(n_1 n_2 N, w, \lambda)$-GOC with the desired size. □

We obtain some lower bounds on the sizes of (n_1, w, λ)-CGOCs and (n_2, w, λ)-GOCs for $w \le 6$ by computer search. Then, by applying Theorem 11, we obtain some $(n_1 n_2 N, w, \lambda)$-GOCs of size $cN^{2\lambda}$, with c listed in Table II. Recall that

$$\begin{aligned} U_{\mathrm{GOC}}(n_1 n_2 N, w, \lambda) &= \frac{(\lambda+1)^2 (n_1 n_2)^{2\lambda}}{w(w-1)\cdots(w-\lambda)} N^{2\lambda} + o(N^{2\lambda}), \\ U_{\mathrm{OOC}}((n_1 n_2 N)^2, w, \lambda) &= \frac{(n_1 n_2)^{2\lambda}}{w(w-1)\cdots(w-\lambda)} N^{2\lambda} + o(N^{2\lambda}). \end{aligned}$$

In Table II, the coefficients (of $N^{2\lambda}$)

$$\begin{aligned} U^*_{\mathrm{GOC}}(n_1 n_2, w, \lambda) &= \frac{(\lambda+1)^2 (n_1 n_2)^{2\lambda}}{w(w-1)\cdots(w-\lambda)} \text{ and} \\ U^*_{\mathrm{OOC}}((n_1 n_2)^2, w, \lambda) &= \frac{(n_1 n_2)^{2\lambda}}{w(w-1)\cdots(w-\lambda)}, \end{aligned}$$

are also listed (abbreviated as simply U^*_{OOC} and U^*_{GOC}) for comparison with c. We note that c is significantly greater than the corresponding U^*_{OOC} in all these cases. These are again examples of GOCs with size exceeding the OOC upper bound.

V. GOCs With Aperiodic Correlation One

In this section, we focus on the case $\lambda = 1$. We first present an improved upper bound on the size of the $(n, w, 1)$-GOC, which shows that Doty and Winslow's bound $U_{\mathrm{GOC}}(n, w, 1) = \frac{4n(n-1)}{w(w-1)}$ cannot be attained when $w \geq 6$. Then we constructed several infinite classes of optimal $(n, 3, 1)$-GOCs and $(n, 4, 1)$-GOCs, the sizes of which meet Doty and Winslow's bound $U_{\mathrm{GOC}}(n, w, 1)$. In the end, we further determine the maximum size of the $(n, 3, 1)$-GOC for almost all positive integers n.

A. An Upper Bound for GOCs With $\lambda = 1$

We first present an upper bound for GOCs with $\lambda = 1$, which improves Doty and Winslow's bound $U_{\mathrm{GOC}}(n, w, 1) = \frac{4n(n-1)}{w(w-1)}$. The technique comes from Kløve's work [24] on difference triangle sets.

Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a family of w-subsets of $[n]^2$. For each M_i, the *list of differences from* M_i is defined to be the multiset $\Delta M_i = \{(a_{ik} - a_{ij}, b_{ik} - b_{ij}) : 1 \leq j \neq k \leq w\}$ for $1 \leq i \leq m$, while the *list of differences from* $\mathcal{M}$ is defined to be the multiset union $\Delta\mathcal{M} = \cup_{i=1}^{m} \Delta M_i$. Let $D_n = [-(n-1), n-1]^2 \backslash \{(0, 0)\}$. We have the following characterization for GOCs with $\lambda = 1$, the proof of which is straightforward and we omit here.

Proposition 12: $\mathcal{M}$ is an $(n, w, 1)$-GOC if and only if the set $\Delta\mathcal{M}$ contains each element of D_n at most once.

Next, we provide an upper bound on the size of GOCs for the case $\lambda = 1$. Specialisation of the upper bounds leads to Corollaries 14 and 15.

Theorem 13: For all $1 \leq t \leq w - 1$, we have

$$M(n, w, 1) \leq \frac{2(t+1)n(n-1) - (w-t-1)}{t\left((w - \frac{t+1}{2})^2 + (\frac{t+1}{2})^2\right)}.$$

Proof: Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be an $(n, w, 1)$-GOC. We can rearrange the elements in each M_i in ascending order. That is, we may assume $M_i = \{(a_{i1}, b_{i1}), (a_{i2}, b_{i2}), \ldots, (a_{iw}, b_{iw})\}$ for all i, where $a_{ij} \leq a_{ik}$ if $1 \leq j < k \leq w$, and $b_{ij} < b_{ik}$ if $a_{ij} = a_{ik}$. Let

$$\alpha_{is} = \sum_{j=s+1}^{w} \left((2n-1)(a_{ij} - a_{i,j-s}) + (b_{ij} - b_{i,j-s})\right).$$

The terms $(2n-1)(a_{ij} - a_{i,j-s}) + (b_{ij} - b_{i,j-s})$ in the sum above are positive and no more than $2n(n-1)$, and according to Proposition 12 they should be pairwise distinct. Rearrange these terms, we get $\alpha_{is} = \alpha_{i,w-s}$. Hence for $1 \leq t \leq w - 1$, we have

$$\sum_{i=1}^{m}\sum_{s=1}^{t} \alpha_{is} = \sum_{i=1}^{m}\sum_{s=1}^{t} \alpha_{i,w-s}.$$

Note that each α_{is} is a sum of $w - s$ terms. The left hand side of the equality above is a sum of $mt(w - \frac{t+1}{2})$ terms, all positive, while the right hand side is a sum of $mt\frac{t+1}{2}$ terms, all integers no greater than $2n(n-1)$. Hence

$$\begin{aligned}\sum_{i=1}^{m}\sum_{s=1}^{t} \alpha_{is} &\geq 1 + 2 + 3 + \cdots + mt\left(w - \frac{t+1}{2}\right) \\ &= \frac{mt}{2}\left(w - \frac{t+1}{2}\right)\left(1 + mt\left(w - \frac{t+1}{2}\right)\right),\end{aligned}$$

$$\begin{aligned}\sum_{i=1}^{m}\sum_{s=1}^{t} \alpha_{i,w-s} &\leq 2n(n-1) - (2n(n-1) - 1) - \cdots \\ &\quad - \left(2n(n-1) - mt\frac{t+1}{2} + 1\right) \\ &= \frac{mt(t+1)}{4}\left(4n(n-1) - mt\frac{(t+1)}{2} + 1\right).\end{aligned}$$

Combining these two inequalities, we get the upper bound on m. □

If we choose $t = w - 1$, Theorem 13 gives the upper bound $U_{\mathrm{GOC}}(n, w, 1) = \frac{4n(n-1)}{w(w-1)}$. If we choose $t + 1 = \sqrt{w}$, then $(w^2 - w(t+1))\frac{t}{t+1} \geq w^2 - 2w\sqrt{w}$ and we get the following bound.

Corollary 14:

$$M(n, w, 1) \leq \frac{2n(n-1)}{w^2 - 2w\sqrt{w} + \frac{\sqrt{w}(\sqrt{w}-1)}{2}}.$$

When $w \geq 16$, we have $\binom{w}{2} < w^2 - 2w\sqrt{w} + \frac{\sqrt{w}(\sqrt{w}-1)}{2}$ and the bound above is better than (1). When $6 \leq w \leq 15$, Table III lists the best choice for t in Theorem 13 and shows that we can still get better bound than (1).

TABLE III
New Upper Bounds for $(n, w, 1)$-GOCs With $6 \leq w \leq 15$

w	$U_{\mathrm{GOC}}(n, w, 1)$	t	New upper bound
6	$\frac{2n(n-1)}{15}$	2	$\frac{2n(n-1)-1}{15}$
7	$\frac{2n(n-1)}{21}$	3	$\frac{8n(n-1)-3}{87}$
8	$\frac{n(n-1)}{14}$	3	$\frac{2n(n-1)-1}{30}$
9	$\frac{n(n-1)}{18}$	3	$\frac{8n(n-1)-5}{159}$
10	$\frac{2n(n-1)}{45}$	3	$\frac{4n(n-1)-3}{102}$
11	$\frac{2n(n-1)}{55}$	3	$\frac{8n(n-1)-7}{255}$
12	$\frac{n(n-1)}{33}$	3	$\frac{n(n-1)-1}{39}$
13	$\frac{n(n-1)}{39}$	3	$\frac{8n(n-1)-9}{375}$
14	$\frac{2n(n-1)}{91}$	3	$\frac{4n(n-1)-5}{222}$
15	$\frac{2n(n-1)}{105}$	4	$\frac{n(n-1)-1}{65}$

B. Constructions for Optimal GOCs With $\lambda = 1$

Corollary 15 shows that Doty and Winslow's upper bound $U_{\mathrm{GOC}}(n, w, 1) = \frac{4n(n-1)}{w(w-1)}$ cannot be achieved for $w \geq 6$. Now, we show that this upper bound can be met for $w \leq 5$ by presenting several classes of optimal $(n, w, 1)$-GOCs. Our constructions are based on some combinatorial structures, which we now introduce.

Let v be a positive integer. Let $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$, where $B_i = (b_{i1}, b_{i2}, \ldots, b_{ik})$, be a family of ordered k-tuple of $[v]$ called *blocks*. The *list of directed differences*

from B_i is defined to be the multiset $\Delta B_i = \{b_{ik} - b_{ij} : 1 \le j < k \le w\}$ for $1 \le i \le m$, while the *list of directed differences from* $\mathcal{B}$ is defined to be the multiset union $\Delta\mathcal{B} = \cup_{i=1}^{m} \Delta B_i$. If $\Delta\mathcal{B} = [1, (v-1)/2]$, then $\mathcal{B}$ is called a *perfect difference family*, or briefly, a $(v, k, 1)$-PDF. Note that, if $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$ is a $(v, k, 1)$-PDF, we must have $m = (v-1)/(k(k-1))$.

Perfect difference families were first introduced by Bermond *et al.* [25] in connection with a problem of spacing movable antennas in radioastronomy, and have also been used to construct optical orthogonal codes [26] and radar arrays [27]. Bermond *et al.* [25] proved that perfect difference families cannot exist for $k \ge 6$. For $k \le 5$, the existence results are summarised as follows.

Theorem 16 (Colbourn and Dinitz [28], Ge et al. [29]): When $k \ge 6$, a $(v, k, 1)$-PDF does not exist. There exists a $(v, k, 1)$-PDF for

1) $k = 3$, $v \equiv 1, 7 \pmod{24}$;
2) $k = 4$, $v = 12t + 1$, $t \le 1000$ *and* $t \ne 2, 3$;
3) $k = 5$, $v = 20t + 1$ *with* $t = 6, 8, 10$.

In our construction we employ a class of related combinatorial objects, the existence of which is equivalent to that of perfect difference families. An $(n, k, 1)$-*strictly perfect difference family* (SPDF) is a family $\mathcal{B}$ of ordered k-tuple of $[n]$ such that $\Delta\mathcal{B} = [1, n-1]$.

Lemma 17: An $(n, k, 1)$-SPDF exists if and only if a $(2n-1, k, 1)$-PDF exists.

Proof: According to the definition, every $(n, k, 1)$-SPDF is also a $(2n-1, k, 1)$-PDF. Now, we show the sufficiency. Let $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$ be a $(2n-1, k, 1)$-PDF, then $\Delta\mathcal{B} = [1, n-1]$. For each block $B_i = (b_{i1}, b_{i2}, \ldots, b_{ik})$ of this PDF, let $B_i' = (0, b_{i2} - b_{i1}, \ldots, b_{ik} - b_{i1})$, then $B_i' \subseteq \{0\} \cup \Delta\mathcal{B} = [n]$ and $\Delta B_i' = \Delta B_i$. Hence $\mathcal{B}' = \{B_1', B_2', \ldots, B_m'\}$ is an $(n, k, 1)$-SPDF. □

Another ingredient needed for our construction is the class of *strictly perfect difference matrices* (SPDMs). An SPDM(k, n) is a $k \times (2n-1)$ matrix with entries from $[n]$ such that, for all $1 \le s < t \le k$, the *list of differences* $D_{st} = \{d_{sj} - d_{tj} : 1 \le j \le 2n-1\} = [-(n-1), n-1]$.

Example 18: The following examples of SPDM$(3, n)$ with $n \in \{2, 3, 7, 9\}$ are useful for our code construction.

1. An SPDM$(3, 2)$:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

2. An SPDM$(3, 3)$:

$$\begin{pmatrix} 0 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 0 & 2 \\ 1 & 2 & 0 & 2 & 0 \end{pmatrix}$$

3. An SPDM$(3, 7)$:

$$\begin{pmatrix} 6 & 6 & 5 & 0 & 2 & 0 & 4 & 6 & 0 & 0 & 1 & 2 & 5 \\ 2 & 6 & 2 & 2 & 1 & 6 & 5 & 0 & 3 & 5 & 5 & 0 & 0 \\ 1 & 0 & 3 & 0 & 6 & 3 & 1 & 2 & 6 & 5 & 0 & 4 & 6 \end{pmatrix}$$

4. An SPDM$(3, 9)$:

$$\begin{pmatrix} 8 & 1 & 8 & 8 & 8 & 4 & 0 & 0 & 8 & 7 & 1 & 2 & 1 & 0 & 0 & 0 & 8 \\ 6 & 6 & 1 & 2 & 3 & 0 & 8 & 1 & 5 & 6 & 5 & 8 & 1 & 2 & 3 & 7 & 0 \\ 2 & 4 & 4 & 6 & 3 & 8 & 0 & 2 & 0 & 0 & 2 & 1 & 8 & 8 & 5 & 6 & 5 \end{pmatrix}$$

Construction 3: Suppose that there exist an $(n, w, 1)$-SPDF and an SPDM(w, n). Then an $(n, w, 1)$-GOC of size $\frac{4n(n-1)}{w(w-1)}$ exists.

Proof: Let $\mathcal{B} = \{B_1, B_2, \ldots, B_{2(n-1)/w(w-1)}\}$ be an $(n, w, 1)$-SPDF and $D = (d_{ij})$ be an SPDM(w, n). For each block B_i of $\mathcal{B}$ and each column j of D, construct a set $M_{ij} = \{(b_{ik}, d_{kj}) : 1 \le k \le w\}$. Denote the family of these sets as $\mathcal{M}$. In addition, we also construct a set $M_i' = \{(0, b_{ik}) : 1 \le k \le w\}$ for each B_i of $\mathcal{B}$ and denote the family of these sets as $\mathcal{M}'$.

It is easy to check that $\Delta(\mathcal{M} \cup \mathcal{M}') = D_n$. Thus $\mathcal{M} \cup \mathcal{M}'$ is the desired $(n, w, 1)$-GOC. □

This construction shows that SPDFs and SPDMs can be used to construct optimal GOCs. We show further that SPDMs can also be constructed from SPDFs.

An *orthogonal array* OA(m, n) is an $m \times n^2$ array A, with entries from a set X of n elements, such that, when restricted to any two rows of A, every ordered pair of elements from X occurs in exactly one column of the restricted array. An orthogonal array A is *idempotent* if it contains the n distinct $m \times 1$ vectors $\{(x, x, \ldots, x)^T : x \in X\}$ as columns.

Example 19: For a prime power q, let $\mathbb{F}_q$ be the field of order q. Let A be a $q \times q^2$ array, with rows labeled by $x \in \mathbb{F}_q$ and columns by $(i, j) \in \mathbb{F}_q^2$, whose entry in row x and column (i, j) is $ix + j$. It is easy to check that A is an idempotent OA(q, q).

Construction 4: Suppose that there exist both an $(n, k, 1)$-SPDF and an idempotent OA(w, k). *Then an SPDM(w, n) exists.*

Proof: Let $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$ be an $(n, k, 1)$-SPDF. From the hypothesis on the existence of an idempotent OA(w, k), we know that for each $B_i \in \mathcal{B}$, there exists an idempotent orthogonal array O_i with w rows and k^2 columns over the k elements of B_i. Remove the idempotent part of O_i to obtain a small 'incomplete' orthogonal array O_i' with n rows and $k(k-1)$ columns for each block. Concatenating all these small 'incomplete' orthogonal arrays O_i' together with the all-zero column $\mathbf{0} = (0, 0, \ldots, 0)^T$, we obtain a large orthogonal array

$$A = (\mathbf{0}\ O_1'\ O_2'\ \cdots\ O_m').$$

Note that all the differences from any two rows of each small 'incomplete' orthogonal array O_i' are exactly those directed differences from the corresponding block and the negatives of these directed differences. Hence, all the differences from any two rows of the large array A are exactly the set $[-(n-1), n-1]$. Thus A is the required SPDM(w, n). □

The existence of an $(n, w, 1)$-SPDF implies that $w \le 5$ [25]. By Example 19, an idempotent OA(w, w) exists for $2 \le w \le 5$. Construction 4 yields an SPDM(w, n). Then, by applying Construction 3, an optimal $(n, w, 1)$-GOC whose size attains Doty and Winslow's bound is obtained.

TABLE IV
SOME $(h, 3)$-REGULAR $(n, 3, 1)$-SPDPs

(n, h)	Blocks
$(15, 3)$	$(0, 5, 12)$ $(0, 4, 14)$ $(0, 2, 13)$ $(0, 1, 9)$
$(22, 7)$	$(8, 16, 21)$ $(1, 3, 20)$ $(2, 12, 13)$ $(0, 4, 20)$ $(0, 7, 21)$
$(31, 7)$	$(2, 3, 22)$ $(1, 25, 30)$ $(0, 11, 25)$ $(1, 8, 24)$ $(0, 22, 26)$ $(1, 9, 22)$ $(0, 2, 30)$ $(0, 10, 27)$
$(34, 7)$	$(0, 19, 32)$ $(1, 8, 30)$ $(4, 15, 25)$ $(0, 16, 30)$ $(0, 31, 33)$ $(3, 4, 30)$ $(6, 14, 31)$ $(2, 6, 26)$ $(0, 5, 28)$
$(43, 7)$	$(3, 40, 42)$ $(0, 30, 34)$ $(6, 17, 42)$ $(2, 15, 37)$ $(0, 14, 41)$ $(3, 11, 35)$ $(1, 20, 30)$ $(3, 34, 41)$ $(20, 40, 41)$ $(0, 26, 42)$ $(4, 9, 37)$ $(0, 17, 40)$
$(33, 9)$	$(9, 17, 31)$ $(4, 17, 24)$ $(1, 26, 31)$ $(1, 17, 27)$ $(0, 11, 28)$ $(2, 29, 31)$ $(0, 1, 32)$ $(0, 4, 23)$
$(36, 9)$	$(1, 5, 30)$ $(1, 28, 29)$ $(1, 21, 32)$ $(1, 18, 34)$ $(1, 20, 27)$ $(3, 11, 25)$ $(4, 14, 27)$ $(1, 33, 35)$ $(0, 5, 35)$
$(45, 9)$	$(2, 18, 41)$ $(2, 30, 43)$ $(5, 15, 37)$ $(2, 31, 38)$ $(0, 35, 37)$ $(0, 11, 42)$ $(3, 17, 43)$ $(23, 24, 43)$ $(0, 17, 44)$ $(1, 9, 34)$ $(6, 10, 40)$ $(0, 5, 43)$
$(48, 9)$	$(9, 10, 45)$ $(3, 14, 33)$ $(3, 16, 45)$ $(6, 31, 47)$ $(3, 17, 37)$ $(1, 45, 47)$ $(7, 15, 46)$ $(1, 18, 44)$ $(8, 35, 40)$ $(3, 36, 40)$ $(0, 40, 47)$ $(0, 10, 38)$ $(0, 22, 45)$
$(57, 9)$	$(17, 18, 49)$ $(9, 29, 56)$ $(8, 42, 50)$ $(7, 44, 55)$ $(7, 29, 48)$ $(3, 33, 47)$ $(5, 30, 56)$ $(9, 16, 44)$ $(7, 52, 56)$ $(4, 40, 50)$ $(1, 40, 56)$ $(3, 43, 56)$ $(2, 25, 54)$ $(0, 54, 56)$ $(13, 51, 56)$ $(0, 17, 50)$

Proposition 20: Suppose that there exists an $(n, w, 1)$-SPDF. Then an optimal $(n, w, 1)$-GOC of size $\frac{4n(n-1)}{w(w-1)}$ exists.

As a consequence of Theorem 16, Lemma 17 and Proposition 20, we have the following result.

Corollary 21: $M(n, w, 1) = \frac{4n(n-1)}{w(w-1)}$ when
(i) $w = 3$, $n \equiv 1, 4 \pmod{12}$; or
(ii) $w = 4$, $n \equiv 1 \pmod 6$, $n \leq 6001$ and $n \neq 13, 19$; or
(iii) $w = 5$, $n = 61, 81$ or 101.

C. Determining the Exact Value of $M(n, 3, 1)$

In this subsection, we determine the exact value of $M(n, 3, 1)$. The case $n \equiv 1, 4 \pmod{12}$ is already settled in Corollary 21. The case $n \equiv 2, 5 \pmod{12}$ and the remaining case $n \equiv 0, 3, 6, 7, 8, 9, 10, 11 \pmod{12}$ are tackled later in Lemma 24 and Lemma 27, after we improve the upper bound $2n(n-1)/3$ and generalize Construction 3.

We first show that the upper bound $2n(n-1)/3$ cannot be attained when $n \equiv 3, 6, 7, 10 \pmod{12}$.

Lemma 22: Let $n \equiv 3, 6, 7, 10 \pmod{12}$. Then

$$M(n, 3, 1) \leq \frac{2n(n-1)}{3} - 1.$$

Proof: Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be an $(n, 3, 1)$-GOC. We consider all the differences $(\delta, \gamma) \in \Delta\mathcal{M}$ with $\delta > 0$, or $\delta = 0$ and $\gamma > 0$. Assume that $M_i = \{(a_{i1}, b_{i1}), (a_{i2}, b_{i2}), (a_{i3}, b_{i3})\}$ with $a_{ij} \leq a_{ik}$ for $1 \leq j < k \leq 3$, and $b_{ij} < b_{ik}$ if $a_{ij} = b_{ik}$. Then the interesting differences in ΔM_i are $(a_{i2} - a_{i1}, b_{i2} - b_{i1})$, $(a_{i3} - a_{i1}, b_{i3} - b_{i1})$ and $(a_{i3} - a_{i2}, b_{i3} - b_{i2})$. The sum of the first coordinates of these differences in $\Delta\mathcal{M}$ is $\sum_{i=1}^{m} 2a_{i3} - 2a_{i1}$, which is even.

If the size of code $m = \frac{2n(n-1)}{3}$, according to Proposition 12, we have $\Delta\mathcal{M} = D_n$. Thus the sum of the first coordinates of the interesting differences is $\sum_{\delta=1}^{n-1} \delta(2n-1) = (2n-1)\, n(n-1)/2$, which is odd when $n \equiv 3, 6, 7, 10 \pmod{12}$. A contradiction. Then the conclusion holds. □

We now generalize Construction 3 by means of SPDFs and SPDMs with 'holes'. We first introduce several notions for its description.

Let $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$ be a collection of ordered k-subsets of $[v]$. If the list of directed differences $\Delta\mathcal{B}$ covers each element of the set $[1, v-1] \backslash L$ exactly once, for some $L \subseteq [v]$, then we call $\mathcal{B}$ a $(v, k, 1)$-*strictly perfect difference packing*, or $(v, K, 1)$-SPDP, with *leave* L. Furthermore, if $L = \{0, r, 2r, \ldots, (h-1)r\}$ for some positive integers r and h, then we call $\mathcal{B}$ (h, r)-*regular*. Obviously, when $L = \emptyset$, $\mathcal{B}$ is in fact a $(v, k, 1)$-SPDF.

Example 23: The families of blocks listed in Table IV are examples of $(h, 3)$-regular $(n, 3, 1)$-SPDPs with $(n, h) \in \{(15, 3), (22, 7), (31, 7), (34, 7), (43, 7), (33, 9), (36, 9), (45, 9), (48, 9), (57, 9)\}$.

Let $D = (D_{ij})$ be a $k \times 2(n-h)$ matrix with entries from $[n]$. D is called an *incomplete strictly perfect difference matrix* with a *regular hole* $H = \{-(h-1)r, \ldots, -r, 0, r, \ldots, (h-1)r\}$, denoted briefly by ISPDM$(k, n; h, r)$, if for all $1 \leq s < t \leq k$, the list of differences $D_{st} = \{d_{sj} - d_{tj} : 1 \leq j \leq 2(n-h)\} = [-(n-1), n-1] \backslash H$. The following construction for ISPDMs is an analogue of Construction 4.

Construction 5: Suppose that there exist an (h, r)-regular $(n, k, 1)$-SPDP and an idempotent OA(w, k). Then an ISPDM$(w, n; h, r)$ exists.

Construction 6: Suppose that the followings exist:
(i) an (h, r)-regular $(n, w, 1)$-SPDP;
(ii) an ISPDM$(w, n; h, r)$;
(iii) an SPDM(w, h);
Then there exists an $(n, w, 1)$-GOC of size $\frac{4(n-h)(n+h-1)}{w(w-1)}$. Furthermore, if an $(h, w, 1)$-GOC of size $\frac{4h(h-1)}{w(w-1)} - \delta$ exists, then there exists an $(n, w, 1)$-GOC of size $\frac{4n(n-1)}{w(w-1)} - \delta$.

Proof: Let $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$ be an (h, r)-regular $(n, w, 1)$-SPDP, where $m = \frac{2(n-h)}{w(w-1)}$. Let $D = (d_{ij})$ and $D' = (d'_{is})$ be an ISPDM$(w, n; h, r)$ and an SPDM(w, h), respectively. We construct the codewords as follows:

(i) for each block $B_i = (b_{i1}, b_{i2}, \ldots, b_{ik})$ of $\mathcal{B}$ and each column j of D, construct a set $M_{ij} = \{(b_{ik}, d_{kj}) : 1 \leq k \leq w\}$, and denote the family of these sets as $\mathcal{M}$;
(ii) for each block $B_i = (b_{i1}, b_{i2}, \ldots, b_{ik})$ of $\mathcal{B}$ and each column s of D', construct two sets $N_{is} = \{(b_{ik}, rd_{ks}) : 1 \leq k \leq w\}$ and $N^*_{is} = \{(rd_{ks}, b_{ik}) : 1 \leq k \leq w\}$, and denote the family of these sets as $\mathcal{N}$.

It is readily checked that all the differences in $\Delta(\mathcal{M} \cup \mathcal{N})$ are pairwise distinct and

$$\Delta(\mathcal{M} \cup \mathcal{N}) = D_n \backslash (rD_h),$$

TABLE V
CODEWORDS OF SMALL GOC$(n, 3, 1)$

n	Codewords				
3	$\{(0,0),(0,1),(1,0)\}$	$\{(0,0),(0,2),(2,0)\}$	$\{(0,1),(1,2),(2,0)\}$		
6	$\{(1,5),(2,0),(5,0)\}$	$\{(0,2),(1,3),(4,1)\}$	$\{(0,1),(4,4),(5,0)\}$	$\{(0,1),(1,5),(5,1)\}$	$\{(0,2),(3,1),(5,5)\}$
	$\{(0,3),(2,5),(4,3)\}$	$\{(0,0),(1,5),(3,2)\}$	$\{(0,5),(2,0),(5,3)\}$	$\{(0,1),(0,5),(4,2)\}$	$\{(0,3),(1,0),(1,5)\}$
	$\{(0,5),(3,0),(5,0)\}$	$\{(1,0),(3,3),(5,2)\}$	$\{(0,4),(2,0),(5,5)\}$	$\{(0,0),(0,2),(0,3)\}$	$\{(0,1),(3,5),(4,5)\}$
	$\{(0,0),(4,5),(5,4)\}$	$\{(0,0),(2,5),(5,2)\}$	$\{(0,3),(2,4),(5,0)\}$	$\{(0,4),(1,2),(5,0)\}$	
7	$\{(1,6),(4,6),(6,1)\}$	$\{(0,4),(3,6),(6,0)\}$	$\{(1,5),(4,6),(5,1)\}$	$\{(0,5),(4,0),(5,2)\}$	$\{(0,0),(3,6),(5,0)\}$
	$\{(0,5),(5,1),(6,2)\}$	$\{(1,3),(4,0),(5,6)\}$	$\{(0,6),(2,4),(6,1)\}$	$\{(0,3),(3,1),(6,6)\}$	$\{(1,0),(2,4),(3,3)\}$
	$\{(0,4),(2,6),(5,2)\}$	$\{(2,2),(5,6),(6,0)\}$	$\{(1,0),(2,3),(5,6)\}$	$\{(0,6),(4,0),(5,5)\}$	$\{(0,1),(6,3),(6,5)\}$
	$\{(0,0),(0,3),(5,6)\}$	$\{(0,1),(2,6),(4,5)\}$	$\{(1,0),(1,4),(2,0)\}$	$\{(0,4),(4,3),(6,3)\}$	$\{(1,1),(3,5),(5,2)\}$
	$\{(0,0),(0,6),(6,0)\}$	$\{(0,4),(1,1),(6,5)\}$	$\{(0,0),(6,5),(6,6)\}$	$\{(0,4),(4,6),(6,2)\}$	$\{(0,0),(4,0),(4,5)\}$
	$\{(1,2),(2,0),(4,1)\}$	$\{(0,0),(2,6),(5,1)\}$			
9	$\{(1,3),(4,8),(8,0)\}$	$\{(0,8),(5,4),(5,8)\}$	$\{(0,5),(5,8),(8,0)\}$	$\{(1,1),(1,8),(8,7)\}$	$\{(0,0),(0,3),(8,8)\}$
	$\{(0,1),(2,8),(8,5)\}$	$\{(2,8),(5,5),(6,1)\}$	$\{(3,2),(6,8),(7,0)\}$	$\{(2,3),(7,8),(8,2)\}$	$\{(2,1),(3,8),(8,2)\}$
	$\{(0,2),(3,4),(8,8)\}$	$\{(1,1),(5,1),(8,8)\}$	$\{(0,1),(2,4),(5,8)\}$	$\{(1,2),(6,3),(7,8)\}$	$\{(2,4),(5,5),(6,0)\}$
	$\{(1,6),(5,5),(8,1)\}$	$\{(0,0),(4,8),(7,1)\}$	$\{(1,1),(4,0),(8,6)\}$	$\{(2,8),(4,6),(8,3)\}$	$\{(0,0),(7,0),(7,8)\}$
	$\{(0,8),(1,8),(6,0)\}$	$\{(0,0),(7,2),(7,4)\}$	$\{(0,3),(2,7),(5,1)\}$	$\{(0,7),(2,4),(8,7)\}$	$\{(1,0),(3,8),(5,1)\}$
	$\{(2,7),(7,4),(8,1)\}$	$\{(0,7),(5,0),(8,8)\}$	$\{(1,0),(2,4),(6,8)\}$	$\{(0,4),(6,8),(8,0)\}$	$\{(2,1),(2,7),(4,3)\}$
	$\{(0,6),(4,0),(8,5)\}$	$\{(0,4),(4,7),(8,2)\}$	$\{(2,1),(7,0),(8,6)\}$	$\{(0,6),(6,4),(7,2)\}$	$\{(0,4),(6,6),(8,7)\}$
	$\{(1,8),(7,1),(8,0)\}$	$\{(0,0),(2,0),(8,7)\}$	$\{(2,0),(6,2),(6,7)\}$	$\{(0,6),(1,7),(8,0)\}$	$\{(1,8),(6,3),(8,2)\}$
	$\{(4,7),(5,0),(7,5)\}$	$\{(2,0),(5,0),(7,6)\}$	$\{(0,5),(3,0),(8,2)\}$	$\{(0,2),(6,2),(7,5)\}$	$\{(1,5),(7,1),(8,3)\}$
	$\{(4,5),(6,0),(7,8)\}$	$\{(0,0),(6,8),(8,2)\}$	$\{(0,7),(0,8),(8,0)\}$		
10	$\{(1,9),(6,2),(9,0)\}$	$\{(1,1),(7,9),(9,5)\}$	$\{(0,9),(5,9),(8,1)\}$	$\{(0,0),(7,9),(9,8)\}$	$\{(1,1),(5,7),(9,0)\}$
	$\{(0,0),(4,8),(9,4)\}$	$\{(0,0),(1,4),(2,2)\}$	$\{(0,9),(6,1),(6,7)\}$	$\{(0,2),(6,5),(7,4)\}$	$\{(1,0),(6,2),(8,7)\}$
	$\{(1,9),(3,1),(9,7)\}$	$\{(0,2),(4,7),(8,4)\}$	$\{(0,4),(0,9),(9,2)\}$	$\{(0,9),(2,9),(3,0)\}$	$\{(0,8),(6,1),(8,4)\}$
	$\{(1,0),(5,0),(6,9)\}$	$\{(0,9),(7,1),(8,2)\}$	$\{(0,5),(1,1),(9,1)\}$	$\{(1,5),(4,9),(8,0)\}$	$\{(0,3),(3,2),(6,8)\}$
	$\{(1,1),(2,8),(4,1)\}$	$\{(0,3),(0,5),(0,6)\}$	$\{(0,2),(0,9),(9,8)\}$	$\{(0,3),(6,2),(7,7)\}$	$\{(0,9),(1,2),(3,3)\}$
	$\{(0,0),(1,0),(9,9)\}$	$\{(0,0),(2,9),(4,4)\}$	$\{(0,3),(7,0),(9,8)\}$	$\{(0,9),(3,5),(6,0)\}$	$\{(2,4),(9,0),(9,9)\}$
	$\{(0,0),(5,8),(9,3)\}$	$\{(0,8),(6,4),(9,5)\}$	$\{(0,0),(5,7),(9,1)\}$	$\{(0,4),(2,1),(8,5)\}$	$\{(0,2),(3,5),(6,2)\}$
	$\{(0,9),(1,4),(8,3)\}$	$\{(0,1),(4,4),(9,8)\}$	$\{(0,4),(4,3),(9,6)\}$	$\{(0,7),(6,2),(9,7)\}$	$\{(2,9),(8,6),(9,0)\}$
	$\{(0,1),(1,9),(6,3)\}$	$\{(1,2),(2,8),(9,8)\}$	$\{(1,0),(8,8),(9,5)\}$	$\{(1,9),(3,0),(6,7)\}$	$\{(2,0),(6,9),(7,1)\}$
	$\{(0,6),(3,8),(8,3)\}$	$\{(0,9),(9,0),(9,4)\}$	$\{(0,2),(5,1),(7,5)\}$	$\{(1,0),(7,1),(9,8)\}$	$\{(0,5),(1,7),(8,0)\}$
	$\{(0,9),(7,7),(9,1)\}$	$\{(0,8),(4,0),(7,9)\}$	$\{(0,2),(2,8),(6,9)\}$	$\{(1,0),(7,9),(9,7)\}$	$\{(1,2),(5,9),(9,5)\}$
	$\{(1,2),(5,0),(8,8)\}$	$\{(0,4),(5,1),(5,9)\}$	$\{(0,6),(1,9),(6,0)\}$	$\{(0,6),(4,8),(9,0)\}$	
12	$\{(0,1),(5,10),(9,11)\}$	$\{(0,0),(10,3),(11,11)\}$	$\{(2,0),(5,10),(8,7)\}$	$\{(0,3),(4,1),(10,7)\}$	
	$\{(0,2),(8,11),(11,5)\}$	$\{(0,0),(7,5),(11,7)\}$	$\{(4,2),(8,11),(9,6)\}$	$\{(0,0),(0,10),(9,11)\}$	
	$\{(0,0),(2,2),(6,10)\}$	$\{(0,0),(6,5),(11,5)\}$	$\{(1,11),(9,0),(11,6)\}$	$\{(0,9),(6,7),(11,3)\}$	
	$\{(0,0),(9,4),(11,8)\}$	$\{(1,3),(2,8),(11,10)\}$	$\{(0,11),(5,0),(11,11)\}$	$\{(5,0),(5,4),(10,11)\}$	
	$\{(0,0),(1,11),(8,10)\}$	$\{(1,1),(9,0),(11,11)\}$	$\{(0,6),(7,0),(8,6)\}$	$\{(0,11),(4,10),(7,2)\}$	
	$\{(1,0),(8,8),(10,3)\}$	$\{(4,8),(9,1),(10,3)\}$	$\{(1,0),(1,11),(10,7)\}$	$\{(2,9),(11,3),(11,4)\}$	
	$\{(4,5),(4,8),(9,0)\}$	$\{(1,11),(7,2),(9,5)\}$	$\{(0,11),(4,5),(11,3)\}$	$\{(4,1),(7,2),(8,11)\}$	
	$\{(0,5),(1,8),(4,10)\}$	$\{(0,9),(1,3),(11,0)\}$	$\{(2,2),(4,0),(11,11)\}$	$\{(0,10),(9,2),(10,0)\}$	
	$\{(1,6),(2,10),(11,0)\}$	$\{(0,10),(4,6),(10,6)\}$	$\{(1,3),(1,10),(9,0)\}$	$\{(1,9),(3,0),(7,3)\}$	
	$\{(0,11),(1,1),(11,9)\}$	$\{(1,0),(8,10),(11,6)\}$	$\{(0,5),(1,1),(10,6)\}$	$\{(4,3),(8,10),(11,3)\}$	
	$\{(0,1),(1,0),(11,11)\}$	$\{(0,4),(7,10),(11,0)\}$	$\{(1,2),(6,8),(9,6)\}$	$\{(1,1),(3,9),(8,10)\}$	
	$\{(1,8),(11,1),(11,10)\}$	$\{(0,6),(4,10),(10,11)\}$	$\{(1,4),(1,9),(9,0)\}$	$\{(2,7),(5,7),(11,0)\}$	
	$\{(4,10),(6,11),(9,0)\}$	$\{(0,11),(6,1),(11,4)\}$	$\{(2,11),(4,8),(8,0)\}$	$\{(4,0),(9,10),(11,2)\}$	
	$\{(3,1),(5,10),(8,0)\}$	$\{(2,0),(4,10),(6,0)\}$	$\{(0,10),(6,2),(9,7)\}$	$\{(0,9),(8,2),(11,6)\}$	
	$\{(2,3),(8,11),(9,0)\}$	$\{(1,8),(2,0),(8,9)\}$	$\{(0,11),(2,0),(10,3)\}$	$\{(3,4),(9,1),(9,7)\}$	
	$\{(1,0),(7,4),(9,11)\}$	$\{(3,5),(10,1),(11,11)\}$	$\{(0,9),(2,3),(10,8)\}$	$\{(0,0),(0,8),(11,9)\}$	
	$\{(1,0),(4,9),(8,4)\}$	$\{(1,10),(6,8),(10,1)\}$	$\{(4,9),(5,9),(6,2)\}$	$\{(1,1),(6,9),(10,0)\}$	
	$\{(1,9),(7,11),(11,0)\}$	$\{(1,0),(1,2),(10,8)\}$	$\{(1,6),(6,0),(10,6)\}$	$\{(5,0),(9,11),(10,2)\}$	
	$\{(0,2),(3,10),(10,2)\}$	$\{(0,11),(5,2),(7,1)\}$	$\{(0,5),(8,0),(11,11)\}$	$\{(0,4),(3,11),(11,3)\}$	
	$\{(0,10),(1,11),(11,0)\}$	$\{(0,2),(8,9),(11,4)\}$	$\{(1,2),(6,7),(9,10)\}$	$\{(0,4),(6,0),(8,5)\}$	
	$\{(1,3),(7,2),(10,1)\}$	$\{(0,9),(1,6),(11,4)\}$	$\{(1,11),(3,11),(10,0)\}$	$\{(4,10),(9,7),(11,3)\}$	
	$\{(0,11),(3,2),(11,0)\}$	$\{(0,6),(7,1),(8,8)\}$	$\{(0,7),(4,4),(11,11)\}$	$\{(0,0),(3,6),(10,9)\}$	

where $rD_h = \{(r\delta, r\gamma) : (\delta, \gamma) \in D_h\}$. So $\mathcal{M} \cup \mathcal{N}$ is an $(n, w, 1)$-GOC of size $\frac{4(n-h)(n+h-1)}{w(w-1)}$.

If we have an $(h, w, 1)$-GOC $\mathcal{F}$, then for each $F = \{(a_i, b_i) : 1 \le i \le w\} \in \mathcal{F}$, construct a set $F' = \{(ra_i, rb_i) : 1 \le i \le w\}$. Denote the family of F' as $\mathcal{F}'$. Then $\Delta\mathcal{F}'$ contains each elements of rD_h at most once. Thus $\mathcal{M} \cup \mathcal{N} \cup \mathcal{F}'$ is the desired code. □

Lemma 24: Let $n \equiv 2, 5 \pmod{12}$. *Then* $M(n, 3, 1) = \lfloor \frac{2n(n-1)}{3} \rfloor$.

Proof: For $n = 2$, the optimal code consists of one codeword, and we can choose any 3-subset of $\{0, 1\}^2$ as its codeword.

For $n \equiv 2, 5 \pmod{12}$ and $n \ge 5$, according to Theorem 16 and Lemma 17, there exists an $(n-1, 3, 1)$-SPDF, whose list of directed differences is $\{1, 2, \ldots, n-2\}$. We can also regard it as a $(2, n-1)$-regular $(n, 3, 1)$-SPDP with leave $\{0, n-1\}$. Apply Construction 5 with this SPDP and an idempotent OA(3, 3) to obtain an ISPDM$(3, n; 2, n-1)$. Then apply Construction 6 with the $(2, n-1)$-regular $(n, 3, 1)$-SPDP, the ISPDM$(3, n; 2, n-1)$, the $(2, 3, 1)$-GOC constructed above, and an SPDM(3, 2) from Example 18. This yields an $(n, 3, 1)$-GOC of size $\frac{2n(n-1)-1}{3}$, as desired. □

In order to provide more ingredient $(n, 3, 1)$-SPDPs for Construction 6, we need the following notations.

A *Langford sequence of order n and defect d*, $n > d$, is a partition of $[1, 2n]$ into a collection of ordered pairs (a_i, b_i) such that $\{b_i - a_i : 1 \le i \le n\} = [d, d+n-1]$. A *hooked Langford sequence of order n and defect d* is a partition of $[1, 2n+1] \backslash \{2n\}$ into a collection of ordered

TABLE VI
THE REQUISITE (h, r)-REGULAR $(n, 3, 1)$-SPDPS IN LEMMA 27

n	(h, r)	n	(h, r)
$n \equiv 3, 6 \pmod{12}, n \geq 18$	$(h, r) = (3, 1)$	$n = 15$	$(h, r) = (3, 3)$
$n \equiv 7, 10 \pmod{12}, n \geq 46$	$(h, r) = (7, 1)$	$n \in \{22, 31, 34, 43\}$	$(h, r) = (7, 3)$
$n \equiv 0, 9 \pmod{12}, n \geq 60$	$(h, r) = (9, 1)$	$n \in \{33, 36, 45, 48, 57\}$	$(h, r) = (9, 3)$
$n \equiv 8, 11 \pmod{12}$	$(h, r) = (2, n-2)$		

pairs (a_i, b_i) such that $\{b_i - a_i : 1 \leq i \leq n\} = [d, d + n - 1]$. The existence problem of Langford sequences and hooked Langford sequences has been settled in [30].

Theorem 25 (Simpson [30]):

1) *A Langford sequence of order n and defect d exists if and only if (i) $n \geq 2d - 1$, and (ii) $n \equiv 0, 1 \pmod 4$ for d is odd, or $n \equiv 0, 3 \pmod 4$ for d is even.*
2) *A hooked Langford sequence of order n and defect d exists if and only if (i) $n(n - 2d + 1) + 2 \geq 0$, and (ii) $n \equiv 2, 3 \pmod 4$ for d is odd, or $n \equiv 1, 2 \pmod 4$ for d is even.*

Lemma 26: There exist (h, r)-regular $(n, 3, 1)$-SPDPs for:

(i) $n = 12t + 3$, $t \geq 2$, $h = 3$ and $r = 1$;
(ii) $n = 12t + 6$, $t \geq 1$, $h = 3$ and $r = 1$;
(iii) $n = 12t + 7$, $t \geq 4$, $h = 7$ and $r = 1$;
(iv) $n = 12t + 10$, $t \geq 3$, $h = 7$ and $r = 1$;
(v) $n = 12t + 9$, $t \geq 5$, $h = 9$ and $r = 1$;
(vi) $n = 12t + 12$, $t \geq 4$, $h = 9$ and $r = 1$;
(vii) $n = 12t + 8$, $t \geq 0$, $h = 2$ and $r = n - 2$;
(viii) $n = 12t + 11$, $t \geq 0$, $h = 2$ and $r = n - 2$.

Proof: For (i), $n = 12t + 3$ and $t \geq 2$, there exists a Langford sequence of order $4t$ and defect 3 by Theorem 25. Then we have a collection of ordered pairs (a_i, b_i) with $\cup_{i=1}^{4t}\{a_i, b_i\} = [1, 8t]$ and $\{b_i - a_i : 1 \leq i \leq 4t\} = [3, 4t + 2]$. For each $1 \leq i \leq 4t$, construct a block

$$B_i = (0, a_i + 4t + 2, b_i + 4t + 2).$$

Then $B_i \subseteq [12t + 3]$ and

$$\cup_{i=1}^{4t} \Delta B_i = \cup_{i=1}^{4t}\{a_i + 4t + 2, b_i + 4t + 2, b_i - a_i\} = [3, 12t + 2].$$

Thus the family of $B_1, B_2, \ldots, B_{4t}$ is the desired $(3, 1)$-regular $(12t + 3, 3, 1)$-SPDP.

For (ii)–(vi), we can proceed similarly. According to Theorem 25, there exists a Langford sequence of order m and defect h with $m = \frac{n-h}{3}$. Then we have a collection of ordered pairs (a_i, b_i) with $\cup_{i=1}^{m}\{a_i, b_i\} = [1, 2m]$ and $\{b_i - a_i : 1 \leq i \leq m\} = [h, h + m - 1]$. For each $1 \leq i \leq m$, construct a block

$$B_i = (0, a_i + m + h - 1, b_i + m + h - 1).$$

Then $B_i \subseteq [3m + h]$ and

$$\begin{aligned}\cup_{i=1}^{m} \Delta B_i &= \cup_{i=1}^{m}\{a_i + m + h - 1, b_i + m + h - 1, b_i - a_i\} \\ &= [h, 3m + h - 1].\end{aligned}$$

Thus the family of $B_1, B_2, \ldots, B_m$ is the desired $(h, 1)$-regular $(3m + h, 3, 1)$-SPDP.

For (vii) and $(viii)$, $n = 12t + 8$ or $12t + 11$, there exists a hooked Langford sequence of order m and defect 1 with $m = \frac{n-2}{3}$ by Theorem 25. Then we have a collection of ordered pairs (a_i, b_i) with $\cup_{i=1}^{m}\{a_i, b_i\} = [1, 2m + 1]\backslash\{2m\}$ and $\{b_i - a_i : 1 \leq i \leq m\} = [1, m]$. For each $1 \leq i \leq m$, construct a block

$$B_i = (0, a_i + m, b_i + m).$$

Then $B_i \subseteq [3m + 2]$ and

$$\cup_{i=1}^{m} \Delta B_i = \cup_{i=1}^{m}\{a_i + m, b_i + m, b_i - a_i\} = [1, 3m + 1]\backslash\{3m\}.$$

Thus the family of $B_1, B_2, \ldots, B_m$ is the desired $(2, 3m)$-regular $(3m + 2, 3, 1)$-SPDP. □

Lemma 27: $M(n, 3, 1) = \lfloor \frac{2n(n-1)}{3} \rfloor$ *for* $n \equiv 0, 8, 9, 11 \pmod{12}$ *and* $n \neq 21$ *or* 24; $M(n, 3, 1) = \frac{2n(n-1)}{3} - 1$ *for* $n \equiv 3, 6, 7, 10 \pmod{12}$ *and* $n \neq 19$.

Proof: For $n \in \{3, 6, 7, 9, 10, 12\}$, the optimal codes are listed in Table V.

For the remaining values of n, we start with an (h, r)-regular $(n, 3, 1)$-SPDP coming from Example 23 or Lemma 26 (the values of h and r are listed in Table VI). Apply Construction 5 with this SPDP and an idempotent OA$(3, 3)$ from Example 19 to obtain an ISPDM$(3, n; h, r)$. Then we apply Construction 6 with the (h, r)-regular $(n, 3, 1)$-SPDP, the ISPDM$(3, n; h, r)$ constructed above, the SPDM$(3, h)$ from Example 18, and the $(h, 3, 1)$-GOC from Table V. This yields the desired $(n, 3, 1)$-GOC. □

Combining Corollary 21 and Lemmas 24 and 27, we have the following result.

Theorem 28: Let n be a positive integer and $n \notin \{19, 21, 24\}$. Then we have

$$M(n, 3, 1) = \begin{cases} \lfloor \frac{2n(n-1)}{3} \rfloor, & \text{if } n \equiv 0, 1, 2, 4, 5, 8, 9, 11 \pmod{12}; \\ \frac{2n(n-1)}{3} - 1, & \text{if } n \equiv 3, 6, 7, 10 \pmod{12}. \end{cases}$$

REFERENCES

[1] Y. M. Chee, H. M. Kiah, S. Ling, and H. Wei, "Geometric orthogonal codes better than optical orthogonal codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 1396–1400.

[2] P. W. K. Rothemund, "Folding DNA to create nanoscale shapes and patterns," *Nature*, vol. 440, pp. 297–302, Mar. 2006.

[3] S. Woo and P. W. K. Rothemund, "Programmable molecular recognition based on the geometry of DNA nanostructures," *Nature Chem.*, vol. 3, no. 8, pp. 620–627, 2011.

[4] T. Gerling, K. F. Wagenbauer, A. M. Neuner, and H. Dietz, "Dynamic DNA devices and assemblies formed by shape-complementary, non–base pairing 3D components," *Science*, vol. 347, no. 6229, pp. 1446–1452, 2015.

[5] D. Doty and A. Winslow, "Design of geometric molecular bonds," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 3, no. 1, pp. 13–23, Mar. 2017.

[6] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis, and applications," *IEEE Trans. Inf. Theory*, vol. IT-35, no. 3, pp. 595–604, Mar. 1989.

[7] P. Erdõs, R. Graham, I. Z. Ruzsa, and H. Taylor, "Bounds for arrays of dots with distinct slopes on lengths," *Combinatorica*, vol. 12, no. 1, pp. 39–44, 1992.
[8] J. Hui, "Pattern code modulation and optical decoding-a novel code-division multiplexing technique for multifiber networks," *IEEE J. Sel. Areas Commun.*, vol. SAC-3, no. 6, pp. 916–927, Nov. 1985.
[9] E. Park, A. J. Mendez, and E. M. Garmire, "Temporal/spatial optical CDMA networks-design, demonstration, and comparison with temporal networks," *IEEE Photon. Technol. Lett.*, vol. 4, no. 10, pp. 1160–1162, Oct. 1992.
[10] K. Kitayama, "Novel spatial spread spectrum based fiber optic CDMA networks for image transmission," *IEEE J. Sel. Areas Commun.*, vol. 12, no. 4, pp. 762–772, May 1994.
[11] A. A. Hassan, J. E. Hershey, and G. J. Saulnier, "Spatial optical CDMA," in *Perspectives in Spread Spectrum*. Boston, MA, USA: Springer, 1998, pp. 107–125.
[12] G.-C. Yang and W. C. Kwong, "Two-dimensional spatial signature patterns," *IEEE Trans. Commun.*, vol. 44, no. 2, pp. 184–191, Feb. 1996.
[13] O. Moreno, Z. Zhang, P. Y. Kumar, and V. A. Zinoviev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 448–455, Mar. 1995.
[14] M. Sawa, "Optical orthogonal signature pattern codes with maximum collision parameter 2 and weight 4," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3613–3620, Jul. 2010.
[15] M. Sawa and S. Kageyama, "Optimal optical orthogonal signature pattern codes of weight 3," *Biometrical Lett.*, vol. 46, no. 2, pp. 89–102, 2009.
[16] R. Pan and Y. Chang, "$(m, n, 3, 1)$ optical orthogonal signature pattern codes with maximum possible size," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 1139–1148, Feb. 2015.
[17] J. Chen, L. Ji, and Y. Li, "Combinatorial constructions of optimal $(m, n, 4, 2)$ optical orthogonal signature pattern codes," preprint. [Online]. Available: https://doi.org/10.1007/s10623-017-0409-6
[18] J. Chen, L. Ji, and Y. Li, "New optical orthogonal signature pattern codes with maximum collision parameter 2 and weight 4," *Designs, Codes Cryptography*, vol. 85, no. 2, pp. 299–318, 2017.
[19] R. Omrani, G. Garg, P. V. Kumar, P. Elia, and P. Bhambhani, "Large families of asymptotically optimal two-dimensional optical orthogonal codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1163–1185, Feb. 2012.
[20] W. Chu and S. W. Golomb, "A new recursive construction for optical orthogonal codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3072–3076, Nov. 2003.
[21] L. Ji, B. Ding, X. Wang, and G. Ge, "Asymptotically optimal optical orthogonal signature pattern codes," preprint. [Online]. Available: https://doi.org/10.1109/TIT.2017.2787593
[22] S. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inf. Theory*, vol. 8, no. 3, pp. 203–207, Apr. 1962.
[23] W. Chu, C. J. Colbourn, and P. Dukes, "Constructions for permutation codes in powerline communications," *Designs, Codes Cryptography*, vol. 32, no. 1, pp. 51–64, May 2004.
[24] T. Klove, "Bounds on the size of optimal difference triangle sets," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 2, pp. 355–361, Mar. 1988.
[25] J.-C. Bermond, A. Kotzig, and J. Turgeon, "On a combinatorial problem of antennas in radioastronomy," in *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I* (Colloq. Math. Soc. János Bolyai), vol. 18. Amsterdam, The Netherlands: North-Holland, 1978, pp. 135–149.
[26] R. J. R. Abel and M. Buratti, "Some progress on $(\upsilon, 4, 1)$ difference families and optical orthogonal codes," *J. Combinat. Theory. Ser. A*, vol. 106, no. 1, pp. 59–75, 2004.
[27] G. Ge, A. C. H. Ling, and Y. Miao, "A systematic construction for radar arrays," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 410–414, 2008.
[28] C. J. Colbourn and J. H. Dinitz, Eds., *The CRC Handbook of Combinatorial Designs* (Series on Discrete Mathematics and its Applications). Boca Raton, FL, USA: CRC Press, 1996.
[29] G. Ge, Y. Miao, and X. Sun, "Perfect difference families, perfect difference matrices, and related combinatorial structures," *J. Combinat. Designs*, vol. 18, no. 6, pp. 415–449, 2010.
[30] J. E. Simpson, "Langford sequences: Perfect and Hooked," *Discrete Math.*, vol. 44, no. 1, pp. 97–104, 1983.

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 Nanyang Technological University (NTU), 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, NTU, Singapore. His research interests include combinatorial design theory, coding theory, and enumerative combinatorics.

San Ling received the B.A. degree in mathematics from the University of Cambridge and the Ph.D. degree in mathematics from the University of California, Berkeley.

Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, in the Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include: arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography and sequences.

Hengjia Wei received the Ph.D. degree in Applied Mathematics from Zhejiang University, Hangzhou, Zhejiang, P. R. China in 2014. From 2014 to 2015 he was a Postdoctoral Fellow at the Capital Normal University. Currently he is a Research Fellow at the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. His research interests include combinatorial design theory, coding theory and their intersections.