Optical Orthogonal Codes: Their Bounds and New Optimal Constructions

Ryoh Fuji-Hara and Ying Miao
Institute of Policy and Planning Sciences
University of Tsukuba
Tsukuba 305-8573, Japan
fujihara@sk.tsukuba.ac.jp and miao@sk.tsukuba.ac.jp

Abstract

A $(v, k, \lambda_a, \lambda_c)$ optical orthogonal code $\mathcal{C}$ is a family of $(0, 1)$-sequences of length v and weight k satisfying the following two correlation properties: $(1)\sum_{0 \le t \le v-1} x_t x_{t+i} \le \lambda_a$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1})$ and any integer $i \not\equiv 0 \bmod v$; and $(2)\sum_{0 \le t \le v-1} x_t y_{t+i} \le \lambda_b$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1})$, $\mathbf{y} = (y_0, y_1, \ldots, y_{v-1})$ with $\mathbf{x} \ne \mathbf{y}$, and any integer i, where subscripts are taken modulo v. The study of optical orthogonal codes is motivated by an application in optical code-division multiple-access communication systems. In this article, upper bounds on the size of an optical orthogonal code are discussed. Several new constructions for optimal $(v, k, 1, 1)$ optical orthogonal codes are described by means of optimal cyclic packing families. Many new optimal optical orthogonal codes with weight $k \ge 4$ and correlation constraints $\lambda_a = \lambda_c = 1$ are thus produced.

1 Introduction

Let $v, k, \lambda_a, \lambda_c$ be positive integers. A $(v, k, \lambda_a, \lambda_c)$ *optical orthogonal code*, or briefly $(v, k, \lambda_a, \lambda_c)$-OOC, $\mathcal{C}$, is a family of $(0, 1)$-sequences of *length* v and *weight* k satisfying the following two properties:

(1) (*The auto-correlation property*)
$\sum_{0 \le t \le v-1} x_t x_{t+i} \le \lambda_a$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$ and any integer $i \not\equiv 0 \bmod v$;

(2) (*The cross-correlation property*)
$\sum_{0 \le t \le v-1} x_t y_{t+i} \le \lambda_c$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$, $\mathbf{y} = (y_0, y_1, \ldots, y_{v-1}) \in \mathcal{C}$ with $\mathbf{x} \ne \mathbf{y}$, and any integer i.

The subscripts here are reduced modulo v so that only periodic correlations are considered. The numbers λ_a and λ_c are referred to as *auto-* and *cross-correlation constraints* of the optical orthogonal code respectively.

A convenient way of viewing optical orthogonal codes, especially when k is much smaller than v, is from a set-theoretic perspective. A $(v, k, \lambda_a, \lambda_c)$-OOC $\mathcal{C}$ can be considered as a collection of k-sets of integers modulo v, in which each k-set corresponds to a codeword and the numbers in each k-set specify the nonzero bits of the codeword. One can reformulate the correlation properties in this set-theoretic frame-work as follows:

(3) (*The auto-correlation property*)
$|(X+s_1)\cap(X+s_2)| \le \lambda_a$ for any $X \in \mathcal{C}$ and any integers $s_1 \not\equiv s_2 \bmod v$;

(4) (*The cross-correlation property*)
$|(X+s_1)\cap(X+s_2)| \le \lambda_c$ for any $X, Y \in \mathcal{C}$ with $X \neq Y$, and any integers s_1 and s_2.

Note that $X + s = \{x + s \bmod v : x \in X\}$ represents a cyclic shift of a codeword X of amount s.

The study of optical orthogonal codes has been motivated by an application in optical code-division multiple-access communication systems. Optical orthogonal codes also find applications in mobile radio, frequency-hopping spread-spectrum communications, radar, sonar signal design, constructing protocol-sequence sets for the M-active-out-of T users collision channel without feedback, etc. For detailed discussions, the interested reader is referred to [11, 18, 24, 30, 31, 32, 34].

Research on optical orthogonal codes has concentrated on the case when $\lambda = \lambda_a = \lambda_c$, in which the notation of the code is abbriviated to (v, k, λ)-OOC, see, for example, [2, 12, 35]. However, it does not mean that a $(v, k, \lambda_a, \lambda_c)$-OOC with $\lambda_a \neq \lambda_b$ is not of interest, although we can regard such an OOC as a (v, k, λ)-OOC with $\lambda = \max(\lambda_a, \lambda_c)$.

In this article, we will not outline the known applications of optical orthogonal codes, nor try to exploit their potential applications; instead, we will focus our attention on their combinatorial constructions. A simple upper bound on the maximum possible size of a $(v, k, \lambda_a, \lambda_c)$-OOC with $\lambda_a \neq \lambda_b$ will be derived, which might be tighter than the Johnson bound when λ_a is much larger than λ_c. When $\lambda_a = \lambda_b = \lambda$, the Johnson bound could be applied, and an OOC achieving this bound is in fact equivalent to a combinatorial structure called optimal cyclic packing family. As a consequence, in order to construct such (v, k, λ)-OOCs, we need only to construct the corresponding optimal cyclic packing families. Several combinatorial structures such as $V(m, t)$ vectors, nested cyclic packings, perfect Mendelsohn difference families, are utilized to construct optimal cyclic 2-packing families, or equivalently, "good" (v, k, λ)-OOCs with $\lambda = 1$, which are optimal from the point of view of correct detection by the receiver. Many new optimal optical orthogonal codes with weight $k \ge 4$ and correlation constraints $\lambda_a = \lambda_c = 1$ are produced by this approach. More new optimal optical orthogonal codes can also be obtained if we use our new optimal optical orthogonal codes as ingredients in various recursive constructions in, for example, [35].

2 A Simple Upper Bounds on Code Size

For a given set of positive integers v, k, λ_a and λ_c, the largest possible size of a $(v, k, \lambda_a, \lambda_c)$-OOC is denoted by $\Phi(v, k, \lambda_a, \lambda_c)$. An optical orthogonal code achieving this maximum size is said to be *optimal.* The determination of the exact values of $\Phi(v, k, \lambda_a, \lambda_c)$ and the specific construction of optimal optical orthogonal codes are of interest. However, since it is difficult to determine the exact value of $\Phi(v, k, \lambda_a, \lambda_c)$ in general, upper and lower bounds on $\Phi(v, k, \lambda_a, \lambda_c)$ are also of interest. Some of these bounds have been already found in, for example, [11, 12]. In this section, we try to derive a simple upper bound on $\Phi(v, k, \lambda_a, \lambda_c)$.

Let $\mathcal{C}$ be a $(v, k, \lambda_a, \lambda_c)$-OOC with $|\mathcal{C}| = M$ where $M = \Phi(v, k, \lambda_a, \lambda_c)$. Now let $C = (c_{ij})$ be the $vM \times v$ matrix whose rows are codewords and their cyclic shifts. Each rows of C contains k 1's.

Calculate the sum of the scalar products of pair of rows of C in two ways:

$$\textstyle\sum_{1\le i\le vM}\sum_{1\le j\le vM, j\ne i}\sum_{1\le n\le v} c_{in}c_{jn}. \tag{5}$$

By the definition of a $(v, k, \lambda_a, \lambda_c)$-OOC, for each row of C, say i, there are $v-1$ rows j (those in the same orbit) such that $\sum_{1\le n\le v} c_{in}c_{jn} \le \lambda_a$, and there are $(M-1)v$ rows (those in different orbits) such that $\sum_{1\le n\le v} c_{in}c_{jn} \le \lambda_c$. Therefore the sum (5) does not exceed $\sum_{1\le i\le vM}[(v-1)\lambda_a + (M-1)v\lambda_c] = vM[(v-1)\lambda_a + (M-1)v\lambda_c]$. On the other hand, this sum is equal to $\sum_{1\le n\le v}\sum_{1\le i\le vM}\sum_{1\le j\le vM, j\ne i} c_{in}c_{jn}$. If k_n denotes the number of 1's in the nth column of C, then this column contributes $k_n(k_n-1)$ to this sum. Thus

$$\sum_{1\le n\le v} k_n(k_n-1) \le vM[(v-1)\lambda_a + (M-1)v\lambda_c].$$

But clearly $k_n = kM$ for each $n \in \{1, 2, \ldots, v\}$. So we have that

$$vkM(kM-1) \le vM[(v-1)\lambda_a + (M-1)v\lambda_c],$$

which implies

$$M(k^2 - v\lambda_c) \le v(\lambda_a - \lambda_c) + k - \lambda_a.$$

If $k^2 - v\lambda_c > 0$, then

$$M \le \frac{v(\lambda_a - \lambda_c) + k - \lambda_a}{k^2 - v\lambda_c}.$$

Theorem 2.1

$$\Phi(v, k, \lambda_a, \lambda_c) \le \lfloor \frac{v(\lambda_a - \lambda_c) + k - \lambda_a}{k^2 - v\lambda_c} \rfloor$$

provided that the denominator $k^2 - v\lambda_c$ is positive.

This upper bound is of no interest when $\lambda_a = \lambda_c = \lambda$. Let $\Phi(v, k, \lambda)$ be the shorthand notation of $\Phi(v, k, \lambda_a, \lambda_c)$ when $\lambda_a = \lambda_c = \lambda$. Chung and Kumar [12] showed that $\Phi(v, k, \lambda) \le 1$ if $k^2 > v\lambda$ and $\Phi(v, k, \lambda) = 0$ if $k(k-1) > (v-1)\lambda$. However, when λ_a is much greater than λ_c, this bound might be tighter than the well-known Johnson bound described below.

Taking every sequence in a (v, k, λ)-OOC, $\mathcal{C}$, and all its cyclic shifts as codewords, we get a constant-weight binary error-correcting code of length v and weight k. The correlation properties of the optical orthogonal code guarantee that the minimum Hamming distance of the derived constant-weight code is $2(k-\lambda)$ provided that there exists at least one sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$ such that $\sum_{0\le t\le v-1} x_t x_{t+i_1} = 1$ for some integer $i_1 \not\equiv 0 \bmod v$, or there exist at least two distinct sequences $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$ and $\mathbf{y} = (y_0, y_1, \ldots, y_{v-1}) \in \mathcal{C}$ such that $\sum_{0\le t\le v-1} x_t y_{t+i_2} = 1$ for some integer i_2. Since the number $|\mathcal{C}|v$ of its codewords is upper bounded by the Johnson bound $A(v, 2(k-\lambda), k)$ [20], where $A(n, d, w)$ denotes the maximum size of a constant-weight binary error-correcting code of length n, weight w and minimum Hamming distance d, we have

$$\begin{aligned} |\mathcal{C}| &\le \frac{1}{v} A(v, 2(k-\lambda), k) \\ &\le \frac{1}{k} A(v-1, 2(k-\lambda), k-1) \\ &\le \frac{1}{k} \lfloor \frac{v-1}{k-1} \lfloor \frac{v-2}{k-2} \lfloor \cdots \lfloor \frac{v-\lambda}{k-\lambda} \rfloor \cdots \rfloor \rfloor \rfloor, \end{aligned}$$

where $\lfloor x \rfloor$ denotes the largest integer not exceeding x.

Theorem 2.2 *(Johnson bound)*

$$\Phi(v, k, \lambda) \le \lfloor \frac{1}{k} \lfloor \frac{v-1}{k-1} \lfloor \frac{v-2}{k-2} \lfloor \cdots \lfloor \frac{v-\lambda}{k-\lambda} \rfloor \cdots \rfloor \rfloor \rfloor \rfloor.$$

When $\lambda_a \neq \lambda_c$, we can set $\lambda = \max(\lambda_a, \lambda_c)$ and apply the above Johnson bound. However, for the case when λ_a is much greater than λ_c, some detailed information on the structure of such OOC has been ignored in the Johnson bound, and we would not be surprised if we find that the Johnson bound is weaker than the upper bound we obtained in Theorem 2.1 in such a case. For example, the upper bound for a $(23, 7, 3, 1)$-OOC given by Theorem 2.2 is 11, while that given by Theorem 2.1 is only 1.

3 Optimal Optical Orthogonal Codes and Optimal Cyclic Packing Families

Optimal optical orthogonal codes are closely related to some combinatorial structures. For example, Yin [35] showed that an optimal $(v, k, 1)$-OOC is equivalent to a combinatorial configuration called optimal cyclic 2-packing family. In this section, we define some terminology in combinatorial design theory, and describe the relationship bwtween (v, k, λ) optical orthogonal codes and cyclic t-packing families.

Let $v \ge k \ge t \ge 2$ be positive integers. A t-(v, k, λ) *packing design* is a pair $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a v-set of elements (*points*) and $\mathcal{B}$ is a collection of k-subsets of $\mathcal{V}$ (*blocks*), such that every t-subset of points occurs in at most λ blocks in $\mathcal{B}$. If $\lambda > 1$, then $\mathcal{B}$ is allowed to contain repeated blocks. The *packing number* $D_\lambda(v, k, t)$ is the maximum number of blocks in any t-(v, k, λ) packing design. It is clear that $D_\lambda(v, k, 0) = \lambda$ and $D_\lambda(v, k, 1) = \lfloor \frac{v\lambda}{k} \rfloor$.

Suppose that $(\mathcal{V},\mathcal{B})$ is a t-(v,k,λ) packing design. Deleting one point x_0 from $\mathcal{V}$, we can obtain a $(t-1)$-$(v-1,k-1,\lambda)$ packing design $(\mathcal{V}-\{x_0\},\mathcal{B}_0)$, where $\mathcal{B}_0=\{B-\{x_0\}: x_0\in B, B\in\mathcal{B}\}$. Counting the number of the flags $\sum_{x\in\mathcal{V},B\in\mathcal{B},x\in B}|(x,B)|$ in two ways, we have

$$kD_\lambda(v,k,t)\leq vD\lambda(v-1,k-1,t-1),$$

which implies the following well-known result due to Schonheim [33].

Theorem 3.1 *(Schonheim bound)*

$$D_\lambda(v,k,t)\leq\lfloor\frac{v}{k}\lfloor\frac{v-1}{k-1}\lfloor\frac{v-2}{k-2}\lfloor\ldots\lfloor\frac{(v-t+1)\lambda}{k-t+1}\rfloor\ldots\rfloor\rfloor\rfloor\rfloor.$$

For a t-(v,k,λ) packing design $(\mathcal{V},\mathcal{B})$, let σ be a permutation on $\mathcal{V}$. For any block $B=\{b_1,\ldots,b_k\}$, define $B^\sigma=\{b_1^\sigma,\ldots,b_k^\sigma\}$. If $\mathcal{B}^\sigma=\{B^\sigma: B\in\mathcal{B}\}=\mathcal{B}$, then σ is called an *automorphism* of the t-(v,k,λ) packing design. The set of all such permutations forms a group under composition called the *full automorphism group* of the packing design. Any of its subgroups is called an *automorphism group* of the packing design. A t-(v,k,λ) packing design admitting a cyclic and point-regular automorphism group is called a *cyclic t-(v,k,λ) packing design*. For a cyclic t-(v,k,λ) packing design $(\mathcal{V},\mathcal{B})$, the point set $\mathcal{V}$ can be identified with Z_v, the residue ring of the integers modulo v. In this case, the packing design has an automorphism $\sigma: i\longrightarrow i+1\text{mod } v$.

For a cyclic t-(v,k,λ) packing design $(Z_v,\mathcal{B})$, let $B=\{b_1,\ldots,b_k\}$ be a block in $\mathcal{B}$. The *block orbit* containing B is defined to be the set of the following distinct blocks

$$B^{\sigma^i}=B+i=\{b_1+i,\ldots,b_k+i\}\text{ mod } v$$

for $i\in Z_v$. If a block orbit has v distinct blocks, i.e. its stabilizer $G_B=\{0\}$, then this block orbit is said to be *full*, otherwise *short*. Choose an arbitarily fixed block from each block orbit and then call it a *base block*.

Now consider a cyclic t-(v,k,λ) packing design $(\mathcal{V},\mathcal{B})$ containning only full block orbits, that is, for any base block $B\in\mathcal{B}$, the stabilizer $G_B=\{0\}$. Set $\mathcal{F}$ to be the family of all base blocks of such a t-(v,k,λ) packing design. Then the pair $(Z_v,\mathcal{F})$ is called a *cyclic t-(v,k,λ) packing family*.

We use $CD_\lambda(v,k,t)$ to denote the maximum number of base blocks in any cyclic t-(v,k,λ) packing family. Then clearly we have

$$CD_\lambda(v,k,t)\leq\frac{1}{v}D_\lambda(v,k,\lambda)\leq\frac{1}{k}D_\lambda(v-1,k-1,t-1).$$

Theorem 3.2

$$CD_\lambda(v,k,t)\leq\lfloor\frac{1}{k}\lfloor\frac{v-1}{k-1}\lfloor\frac{v-2}{k-2}\lfloor\ldots\lfloor\frac{(v-t+1)\lambda}{k-t+1}\rfloor\ldots\rfloor\rfloor\rfloor\rfloor.$$

Cyclic t-(v,k,λ) packing family with $\lfloor\frac{1}{k}\lfloor\frac{v-1}{k-1}\lfloor\frac{v-2}{k-2}\lfloor\ldots\lfloor\frac{(v-t+1)\lambda}{k-t+1}\rfloor\ldots\rfloor\rfloor\rfloor\rfloor$ base blocks is called *optimal.*

Given an optimal cyclic $(\lambda{+}1)$-$(v,k,1)$ packing family with $\lfloor\frac{1}{k}\lfloor\frac{v-1}{k-1}\lfloor\frac{v-2}{k-2}\lfloor\ldots\lfloor\frac{v-\lambda}{k-\lambda}\rfloor\ldots\rfloor\rfloor\rfloor\rfloor$ base blocks, we can construct a $(0,1)$-sequence of length v and of weight k from each base block whose nonzero bit positions are exactly indexed by the base block. It is easy to see that the derived $(0,1)$-sequences constitute a (v,k,λ)-OOC which is in fact optimal.

Conversely, let $\mathcal{C}$ be an optimal (v,k,λ)-OOC with $\lfloor\frac{1}{k}\lfloor\frac{v-1}{k-1}\lfloor\frac{v-2}{k-2}\lfloor\ldots\lfloor\frac{v-\lambda}{k-\lambda}\rfloor\ldots\rfloor\rfloor\rfloor\rfloor$ codewords. For each codeword, we construct a k-subset of Z_v by taking the index set of its nonzero bit positions. This creates a family $\mathcal{F}$ of $\lfloor\frac{1}{k}\lfloor\frac{v-1}{k-1}\lfloor\frac{v-2}{k-2}\lfloor\ldots\lfloor\frac{v-\lambda}{k-\lambda}\rfloor\ldots\rfloor\rfloor\rfloor\rfloor$ k-subsets of Z_v. The correlation properties of the OOC gurantee that $|(X+s_1)\cap(Y+s_2)|\leq\lambda$ for any integers $s_1,s_2\in Z_v$ and any $X,Y\in\mathcal{F}$ except when $X=Y$ and $s_1\equiv s_2 \bmod v$. Thus we can take $\mathcal{F}$ as the family of the base blocks to form an optimal cyclic $(\lambda+1)$-$(v,k,1)$ packing family with the automorphism $\sigma: i\longrightarrow i+1 \bmod v$, which is in fact optimal.

Theorem 3.3 *An optimal (v,k,λ)-OOC is equivalent to an optimal cyclic $(\lambda{+}1)$-$(v,k,1)$ packing family, provided that $\lambda<k$ holds.*

By virtue of Theorem 3.3, in order to construct optimal (v,k,λ)-OOCs, we need only to construct their corresponding optimal cyclic $(\lambda+1)$-$(v,k,1)$ packing families. But in general, the construction of optimal cyclic t-$(v,k,1)$ packing families is not an easy task. Fortunately, when $t=2$, there is a feasible approach to settle this problem.

Let $\mathcal{F}=\{B_1,B_2,\ldots,B_t\}$ be a collection of k-subsets of Z_v with $B_i=\{b_{i1},b_{i2},\ldots,b_{ik}\}$, $1\leq i\leq t$. For any $i, 1\leq i\leq t$, the *differences in* B_i are

$$\Delta B_i=\{b_{ij}-b_{is}: 1\leq j,s\leq k, j\neq s\},$$

while the *differences in* $\mathcal{F}$ are defined to be

$$\begin{aligned}\Delta\mathcal{F} &= \bigcup\nolimits_{1\leq i\leq t}\Delta B_i\\ &= \{b_{ij}-b_{is}: 1\leq i\leq t, 1\leq j,s\leq k, j\neq s\}.\end{aligned}$$

If the setwise stabilizer G_{B_i} of each B_i, $1\leq i\leq t$, is the identity $\{0\}$, and $\Delta\mathcal{F}$ covers $Z_v-L-\{0\}$ exactly once, where L, the *difference leave* of $\mathcal{F}$, is a subset of nonzero elements of Z_v, then the pair $(Z_v,\mathcal{F})$ is in fact a cyclic 2-$(v,k,1)$ packing family. If the difference leave L can be partitioned into *leaves* $L_1,L_2,\ldots,L_n$ such that each leaf L_i along with the element zero forms a subgroup of Z_v of order g_i, then this cyclic 2-$(v,k,1)$ packing family is said to be $(g_1,g_2,\ldots,g_n)$*-regular.* When $n=1$, we simply say g*-regular.* The members of $\mathcal{F}$ are the base blocks of the cyclic packing family.

Counting the differences in two ways, we can easily know that there are exactly $\frac{v-|L|-1}{k(k-1)}$ base blocks in a $(v,k,1)$-CP with difference leave L. As an immediate consequence, we have the following result.

Theorem 3.4 *A necessary condition for the existence of a cyclic 2-$(v,k,1)$ packing family with difference leave L is that $v-|L|-1\equiv 0$ mod $k(k-1)$.*

By a simple counting arguement, we get a criteria for a cyclic 2-$(v,k,1)$ packing family with difference leave L to be optimal.

Theorem 3.5 *A cyclic* 2-$(v,k,1)$ *packing family with difference leave L is optimal if the cardinality of L satisfies* $0 \leq |L| < k(k-1)$.

Two special cases of cyclic 2-packing families need to be mentioned. The first one is a 1-regular cyclic 2-$(v,k,1)$ packing family, that is, a cyclic 2-$(v,k,1)$ packing family with the empty set as its difference leave. In this case, the cyclic 2-packing family is commonly called a $(v,k,1)$ *cyclic difference family*, or briefly, a $(v,k,1)$-CDF (see, for example, [1]). The second one is a k-regular cyclic 2-$(v,k,1)$ packing family in which the difference leave is $(v/k)Z_k$, the unique subgroup of Z_v with order k. These special cyclic 2-packing families are clearly optimal.

By means of an optimal cyclic 2-packing family, an optimal $(v,3,1)$-OCC was shown in [2] to exist except for $v = 6t+2$ where $t \equiv 2,3 \bmod 4$, in which an optimal $(v,3,1)$-OOC does not exist. When $k \geq 4$, despite the vast amount of energy spent (see, for exacmple, [11, 30, 31, 32, 35]), the existence problem for an optimal $(v,k,1)$-OOC remains unsettled.

Here we list some examples of known 1- and k-regular cyclic 2-$(v,k,1)$ packing familis with $k \geq 4$. They can be used as ingredients in this article to yield more optimal cyclic 2-packing families with $k \geq 4$ and $\lambda = 1$, or equivalently, more optimal optical orthogonal codes with weight $k \geq 4$ and $\lambda = 1$. Note that this list of series of examples is not comprehensive at all, and is used only to illustrate our constructions and their corresponding existence results.

Lemma 3.6 *[15] Let $v = p_1 p_2 \cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to* 1 *modulo* 12*. Then there exists a* 1*-regular cyclic* 2-$(v,4,1)$ *packing family.*

Lemma 3.7 *[15] Let $v = p_1 p_2 \cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to* 1 *modulo* 20*. Then there exists a* 1*-regular cyclic* 2-$(v,5,1)$ *packing family.*

Lemma 3.8 *[15] Let $v = p_1 p_2 \cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to* 1 *modulo* 30 *but not equal to* 61*. Then there exists a* 1*-regular cyclic* 2-$(v,6,1)$ *packing family.*

Lemma 3.9 *[10] Let $p \equiv 1 \bmod k(k-1)$ be an odd prime number, and let $m = k(k-1)/2$. Then there exists a* 1*-regular cyclic* 2-$(p,k,1)$ *packing family whenever $p > D(k) = (E + \sqrt{E^2 + 4f})^2/4$, where*

(1) when $k = 2a+1$, $E = 2[((a^2-3a+4)a^a - \frac{1}{2}(a-1)^3 a^{a-1} + (4a-3)(a-1)^{a-1})m^a + (k-4)a^{a+1}(m-1)m^{a-1}] - 5a^a + 1$ and $F = [d_k + 2(k-5)a + 4]m^{a-1}a^a$, $d_k = 0$ if $k \leq 7$, or $d_k = m(a-3)$ otherwise;

(2) when $k = 2a$, $E = 2[((a-2)(a-1)a^a - \frac{1}{2}(a-1)^3a^{a-1} + (4a-3)(a-1)^{a-1})m^{a-1} + (k-3)(a-1)a^a(m-1)m^{a-2}] - a^a + 1$ and $F = [d_k + 2(k-3)(a-1)]m^{a-2}a^a$, $d_k = 0$ if $k \leq 6$, or $d_k = m(a-3)$ otherwise.

Lemma 3.10 *[35] Let $p \in \{5, 7, 11\}$. Let $v = p_1p_2 \cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to 1 modulo 12. Then there exists an optimal cyclic p-regular 2-$(pv, 4, 1)$ packing family.*

Lemma 3.11 *[35] Let $p \in \{5, 7, 11, 13, 17, 19\}$. Let $v = p_1p_2 \cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to 1 modulo 20. Then there exists an optimal cyclic p-regular 2-$(pv, 5, 1)$ packing family.*

Lemma 3.12 *[35] Let $p \in \{7, 11, 13, 17, 19, 23, 29\}$. Let $v = p_1p_2 \cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to 1 modulo 30 but not equal to 61. Then there exists an optimal cyclic p-regular 2-$(pv, 6, 1)$ packing family.*

Lemma 3.13 *[35] Let p_k be a prime number such that $k \leq p_k < k(k-1)$. Let $p \equiv 1 \bmod k(k-1)$ be an odd prime number. Then there exists an optimal cyclic p_k-regular 2-$(p_kp, k, 1)$ packing family whenever $p > D(k)$, where $D(k)$ was defined in Lemma 3.9.*

We wish to point out that the results in Lemmas 3.6, 3.7 and 3.8 are based on the existence of $(q, k, 1)$ difference families with q a prime and $k = 4, 5$, which has been completely settled in [4, 5, 6, 7]. Also note that the results in Lemmas 3.10– 3.13 are based on the existence of difference families described in Lemmas 3.6– 3.9.

4 $V(m, t)$ Vectors

As shown in Theorem 3.3, in order to construct optimal optical orthogonal codes with $\lambda = 1$, we need only to construct optimal cyclic 2-packing families with $\lambda = 1$. In this section, we will describe a construction for optimal cyclic 2-packing families with $\lambda = 1$ from $V(m, t)$ vectors.

For any two positive integers u and v, if $\gcd(u, v) = 1$, then it is clear that $Z_v \times Z_v \simeq Z_{uv}$. So we can use $Z_v \times Z_v$, instead of Z_{uv}, as the set of points. Sometimes, if there is no confusion arises, we will identify $Z_v \times Z_v$ with Z_{uv}. Note that for a set S, $n{\cdot}S$ will denote the set $\{ns : s \in S\}$.

Let $q = mt + 1$ be a prime power and let C_m^0 be a multiplicative subgroup of $GF(q) - \{0\}$ of order t and index m. Let the cosets of this subgroup be $C_m^0, C_m^1, \ldots, C_m^{m-1}$. These are called the *cyclotomic classes* of $GF(q)$ of index m. They evidently partition $GF(q) - \{0\}$. The cyclotomic classess $\{C_m^0, C_m^1, \ldots, C_m^{m-1}\}$ will be denoted by $\mathcal{C}_m$.

Given a set of m distinct elements in $GF(q)$, if they belong to m distinct cyclotomic classes $C_m^0, C_m^1, \ldots, C_m^{m-1}$, then we say that this set of m elements form a *system of* *distinct representatives of the cyclotomic classes* $C_m^0, C_m^1, \ldots, C_m^{m-1}$, and it is denoted by SDRC($\mathcal{C}_m$).

For $q = mt + 1$ a prime power, Mullin et al. [27] defined a $V(m,t)$ to be a vector $(b_1, b_2, \ldots, b_{m+1})$ with elements from $GF(q)$ satisfying the property that for $k = 1, 2, \ldots, m+1$, the set

$$\{b_i - b_j : i \in \{1, 2, \ldots, m+1\} - \{k\}, i - j \equiv k \bmod (m+2) \text{ and } 1 \leq j \leq m+1\}$$

is a system of distinct representatives of the cyclotomic classes SDRC($\mathcal{C}_m$). The $V(m,t)$ vector is often written with a $\sim$ in the 0th position. For each k, we speak of the kth set of differences, denoted by D_k. These are the differences of elements that are k apart in the vector.

It has been shown in [25] that a $V(m,t)$ exists in $GF(mt+1)$ only if m and t are not both even. For $m = 2, 3, 4, 5, 6$ and 7, the spectrum for $V(m,t)$ has been determined in [8, 17, 23, 25, 29].

Lemma 4.1 *All $V(m,t)$ exist whenever $m = 2, 3, 4, 5, 6, 7, t \geq m-1$ and $mt+1$ is a prime number except when both m and t are even.*

There are systematic tables of $V(m,t)$ vectors in [3]. These were extended in [13] to produce systematic tables for $m = 8, 9, 10$ and $mt+1$, a prime, less than 5000, which can be summarized as follows:

Lemma 4.2 *All $V(m,t)$ exist whenever $m = 8, 9, 10, t \geq m-1$ and $mt+1$ is a prime less than* 5000*, except when $m = 9$ and $t = 8$, or when both m and t are even.*

For general m, Chen and Zhu [9] showed the following existence result.

Lemma 4.3 *Let $q = mt+1$ be a prime power. If m and t are not both even, then there exists a $V(m,t)$ in $GF(q)$ whenever $q > B(m) = (E + \sqrt{E^2 + 4F})^2/4$, where $E = (u-1)(m-1)m^u - m^{u-1} + 1$, $F = (u-1)m^u$ and $u = \lfloor (m+1)/2 \rfloor$.*

In particular, they [9] determined the spectrum for $V(m,t)$ with $m = 8$.

Lemma 4.4 *Let $q = 8t+1$ be a prime power with $t > 7$ odd. Then there exists a $V(8,t)$ in $GF(q)$ with possible exceptions $q = 11^2, 13^2, 29^2, 3^6, 3^{10}$.*

$V(m,t)$ vectors were first introduced by Mullin et al. [27] to simplify a construction for mutually orthogonal latin squares. They are also proved to be useful in the construction of perfect Mendelsohn designs (see [26]). Here we provide one more application of these vectors in the construction of optical orthogonal codes. Remember that for any subset $B = \{(b_i, i) : b_i \in Z_m, i \in Z_n\} \subset Z_m \times Z_n$, $\Delta_k B$ denotes the set of differences $\{b_{i_2} - b_{i_1} : i_2 - i_1 \equiv k \bmod n\}$.

Theorem 4.5 *Let $p = mt + 1$ be a prime number. If there exists a $V(m, t)$, then there exists a cyclic $(m + 2, mt + 1)$-regular 2-$((mt + 1)(m + 2), m + 1, 1)$ packing family with difference leave $\{0\} \times (Z_{m+2} - \{0\}) \cup (Z_{mt+1} - \{0\}) \times \{0\}$.*

Proof Let $Z_{mt+1} \times Z_{m+2}$ be the set of points, and $(b_1, b_2, \ldots, b_{m+1})$ be the vector $V(m, t)$. Consider the following $(m + 1)$-subset of $Z_{mt+1} \times Z_{m+2}$:

$$B = \{(b_1, 1), (b_2, 2), \ldots, (b_{m+1}, m + 1)\}.$$

Then

$$\begin{aligned} \Delta_k B &= \{b_i - b_j : i \in \{1, 2, \ldots, m + 1\} - \{k\}, i - j \equiv k \bmod (m + 2) \\ &\quad \text{and } 1 \le j \le m + 1\} \\ &= D_k. \end{aligned}$$

Since $(b_1, b_2, \ldots, b_{m+1})$ is a $V(m, t)$ vector, by its definition, $\Delta_k B$ forms an SDRC($\mathcal{C}_m$) for any $k, 1 \le k \le m + 1$.

For any element $c \in GF(p)$, we define $c{\cdot}B$ to be the set

$$c{\cdot}B = \{(cb_1, 1), (cb_2, 2), \ldots, (cb_{m+1}, m + 1)\}.$$

Now set $\mathcal{F} = \{c{\cdot}B : c \in C_m^0\}$. Then it is easy to see that

$$\begin{aligned} \Delta\mathcal{F} &= \textstyle\bigcup_{A\in\mathcal{F}} \Delta A \\ &= \textstyle\bigcup_{c\in C_m^0} c{\cdot}\Delta B \\ &= \textstyle\bigcup_{c\in C_m^0} c{\cdot}(\bigcup_{1\le k\le m+1} \{k\} \times \Delta_k B) \\ &= \textstyle\bigcup_{1\le k\le m+1} \{k\} \times (\bigcup_{c\in C_m^0} c{\cdot}\Delta_k B) \\ &= Z_{mt+1} \times Z_{m+2} - \{0\} \times (Z_{m+2} - \{0\}) - (Z_{mt+1} - \{0\}) \times \{0\} - \{(0, 0)\}. \end{aligned}$$

Therefore $\mathcal{F}$ is a cyclic $(m+2, mt+1)$-regular 2-$((mt+1)(m+2), m+1, 1)$ packing family with difference leave $\{0\} \times (Z_{m+2} - \{0\}) \cup (Z_{mt+1} - \{0\}) \times \{0\}$. □

According to Theorem 3.5, the resultant cyclic $(m+2, mt+1)$-regular 2-$((mt+1)(m+2), m + 1, 1)$ packing family is optimal if and only if

$$(m + 2 - 1) + (mt + 1 - 1) < (m + 1)m,$$

which requires that t be a positive integer less than or equal to $m - 1$. However, if there exists a cyclic 2-$(mt + 1, m + 1, 1)$ packing family with difference leave L, then we can embed this ingredient cyclic packing family into the cyclic packing family constructed in Theorem 4.5.

Theorem 4.6 *Let $p = mt + 1$ be a prime number. If there exist a $V(m, t)$ and a cyclci 2-$(mt + 1, m + 1, 1)$ packing family with difference leave L, then there exists a cyclic 2-$((mt+1)(m+2), m+1, 1)$ packing family with difference leave $\{0\}\times(Z_{m+2}-\{0\})\cup L\times\{0\}$. Moreover, if $|L| < m^2 - 1$, the resultant cyclic 2-$((mt+1)(m+2), m+1, 1)$ packing family is optimal.*

Proof Let $\mathcal{B}$ be the cyclic 2-$(mt+1, m+1, 1)$ packing family with difference leave L. Then $\mathcal{F} \cup \{B \times \{0\} : B \in \mathcal{B}\}$ is the desired cyclic packikng family with difference leave $\{0\} \times (Z_{m+2} - \{0\}) \cup L \times \{0\}$. In order that the resultant cyclic packing family to be optimal, by Theorem 3.5, we need only that $0 < |L| + m + 1 < (m+1)m$, which means that $0 \leq |L| < m^2 - 1$. □

We give an example to illustrate our construction.

Example 4.7 Let $p = 13, m = 3, s = 1$. 2 is a primitive element of $GF(13)$, and $C_3^0 = \{1, 8, 12, 5\}$, $C_3^1 = \{2, 3, 11, 10\}$, $C_3^2 = \{4, 6, 9, 7\}$. Clearly, $(0, 1, 3, 9)$ is a $V(3, 4)$ vector, and $\{0, 1, 4, 6\}$ is the base block of a $(13, 4, 1)$-CDF. Then

$B_1 = \{(0,1), (1,2), (3,3), (9,4)\}$,
$B_2 = \{(0,1), (8,2), (11,3), (7,4)\}$,
$B_3 = \{(0,1), (12,2), (10,3), (4,4)\}$,
$B_4 = \{(0,1), (5,2), (2,3), (6,4)\}$

are the base blocks of a cyclic $(5, 13)$-regular 2-$(65, 4, 1)$ packing family with difference leave $(Z_5 - \{0\}) \times \{0\} \cup \{0\} \times (Z_{13} - \{0\})$. Adding

$B_5 = \{(0,0), (1,0), (4,0), (6,0)\}$

to the collection of base blocks, we get an optimal cyclic 5-regular 2-$(65, 4, 1)$ packing family with difference leave $Z_5 - \{0\}$. □

Here are some special cases of Theorem 4.6.

Theorem 4.8 *Let $p = (m+1)mt+1$ be a prime number. If there exist a $V(m, (m+1)t)$ and a $((m+1)mt+1, m+1, 1)$-CDF, then there exists an optimal cyclic $(m+2)$-regular 2-$((m+1)mt+1)(m+2), m+1, 1)$ packing family.*

Corollary 4.9 *If $p = 12t + 1$ is a prime number, then there exists an optimal cyclic 5-regular 2-$(5p, 4, 1)$ packing family.*

Proof Apply Theorem 4.8 with Lemmas 3.6 and 4.1. □

Corollary 4.10 *Let t be an odd integer. If $p = 20t + 1$ is a prime number, then there exists an optimal cyclic 6-regular 2-$(6p, 5, 1)$ packing family.*

Proof Apply Theorem 4.8 with Lemmas 3.7 and 4.1. □

Corollary 4.11 *If $p = 30t + 1$ is a prime number $\neq 61$, then there exists an optimal cyclic 7-regular 2-$(7p, 6, 1)$ packing family.*

Proof Apply Theorem 4.8 with Lemmas 3.8 and 4.1. □

For general k, Theorem 4.8 can also yield optimal cyclic $(k+1)$-regular 2-$((k+1)p, k, 1)$ packing family, where $p = k(k-1)t + 1$ is a prime number.

Corollary 4.12 *Let $p = k(k-1)t+1$ be a prime number where $k-1$ and kt are not both even. If $p > max\{B(k-1), D(k)\}$, where $B(k-1)$ and $D(k)$ were defined in Lemmas 4.3 and 3.9 respectively, then there exists an optimal cyclic $(k+1)$-regular 2-$((k+1)p, k, 1)$ packing family.*

Proof Apply Theorem 4.8 with Lemmas 3.9 and 4.3. □

5 Nested Cyclic 2-Packing Families

The concepts of nested designs were introduced by Preece [28] and Federer [16] in different ways for some statistical applications. These designs were further discussed by Kageyama and Miao [21], in which the two concepts were unified and generalized. They have applications in the constructions of several types of codes. Recently Yin [35] generalized this notion to nested 2-packing families, and by using nested optimal cyclic 2-packing families, he did produce a handful of optimal OOCs with $k = 4$ and $\lambda = 1$.

Let $(Z_v, \mathcal{B})$ be a cyclic 2-(v, k, λ) packing family. If each of its base blocks has a distinct subblock of size k' so that the collection of these subblocks constitute a cyclic 2-(v, k', λ') packing family having the automorphism $\psi : i \longrightarrow i + 1 \bmod v$, then this cyclic 2-packing family is called a *nested* cyclic 2-(v, k, λ) p-acking family of *form* (k', λ').

Theorem 5.1 *[35] Let v be an odd integer. If a nested optimal cyclic 2-$(v, 4, 2)$ packing family of form $(3, 1)$ exists, then so does an optimal cyclic 2-$(2v, 4, 1)$ packing family.*

What Yin had actually done in [35] is to find an optimal cyclic $(v, 3, 1)$ packing family with v odd in which the $\lfloor (v-1)/6 \rfloor$ base blocks can be chosen so that for any nonzero integer x of Z_v, at most one of x and its complement $v - x$ occurs in the base blocks and no base block can contain the element 0. This is equivalent to find a nested optimal cyclic 2-$(v, 4, 2)$ packing family of form $(3, 1)$ by adding zero to each of its base blocks. For convenience, Yin [35] called the collection of the base blocks so chosen as a *perfect base* of the nested optimal cyclic 2-$(v, 4, 2)$ packing family of form $(3, 1)$. He conjectured that for every odd v, there exists an optimal cyclic 2-$(v, 3, 1)$ packing family with a perfect base, and verified this conjecture for all odd v up to 50.

In this section, we present a recursive construction for optimal cyclic 2-$(v, 3, 1)$ packing families with a perfect base. By virtue of Theorem 5.1, this would allow us to produce more optimal cyclic 2-packing families with $k = 4$ and $\lambda = 1$.

Let $D = (d_{ij})$ be a $t \times \lambda u$ matrix with entries from Z_u. If every element of Z_u occurs exactly λ times among the differences $d_{i_1 j} - d_{i_2 j}, j = 1, \ldots, \lambda u$, for any $i_1 \neq i_2$, where $1 \leq i_1, i_2 \leq t$, then D is called a (u, t, λ) *difference matrix*, or briefly, (u, t, λ)-DM.

Theorem 5.2 *Let u and v be two odd integers such that $u \equiv 1$ mod 6. Suppose that the following exist:*

(1) a $(u, 3, 1)$-CDF with a perfect base;

(2) an optimal cyclic 2-$(v, 3, 1)$ packing family with a perfect base in which L is its difference leave; and

(3) a $(v, 4, 1)$-DM.

Then there exists an optimal cyclic 2-$(uv, 3, 1)$ packing family with a perfect base in which $u{\cdot}L = \{u\ell : \ell \in L\}$ is its difference leave. Furthermore, if the optimal cyclic 2-$(v, 3, 1)$ packing family is $(g_1, \ldots, g_n)$-regular, then so is the resultant cyclic 2-$(uv, 3, 1)$ packing family.

Proof Let $\mathcal{D}$ be a $(u, 3, 1)$-CDF with a perfect base $\{D_i : i = 1, 2, \ldots, s\}$, where $D_i = \{d_{i1}, d_{i2}, d_{i3}\}$ and $s = (u - 1)/6$. Let $\mathcal{F}$ be an optimal cyclic 2-$(v, 3, 1)$ packing family with a perfect base $\{F_h : h = 1, 2, \ldots, t\}$, where $F_h = \{f_{h1}, f_{h2}, f_{h3}\}$ and $t = \lfloor (v - 1)/6 \rfloor$. Without loss of generality, we may also assume that in the $(v, 4, 1)$-DM $A = (a_{ij})$, $0 \leq i \leq 3, 1 \leq j \leq v$, all a_{0j} are zero. Then every element of Z_v appears exactly once in every row, except the first one, of the $(v, 4, 1)$-DM.

Now for each $D_i \in \mathcal{D}$, we define v new base blocks

$$E_{ij} = \{d_{i1} + a_{1j}u, d_{i2} + a_{2j}u, d_{i3} + a_{3j}u\},\ 1 \leq j \leq v,$$

and for each $F_h \in \mathcal{F}$, we define one new base block

$$F_h^{'} = u{\cdot}F_h = \{uf_{i1}, uf_{i2}, uf_{i3}\}.$$

Let $\mathcal{E} = \{E_{ij} : 1 \leq i \leq s, 1 \leq j \leq v\}$, $\mathcal{F}^{'} = \{F_h^{'} : 1 \leq h \leq t\}$, and $\mathcal{E}^{'} = \mathcal{E} \cup \mathcal{F}^{'}$. Then it can be readily checked that $\mathcal{E}^{'}$ is the desired optimal cyclic 2-$(uv, 3, 1)$ packing family with a perfect base in which $u{\cdot}L = \{u\ell : \ell \in L\}$ is its difference leave.

In fact, we have that

$$\begin{aligned}
\Delta\mathcal{E}^{'} &= \Delta(\mathcal{E} \cup \mathcal{F}^{'}) \\
&= \Delta\mathcal{E} \cup \Delta\mathcal{F}^{'} \\
&= \textstyle\bigcup_{1\leq i\leq s, 1\leq j\leq v} \Delta E_{ij} \cup \bigcup_{1\leq h\leq t} \Delta F_h^{'} \\
&= (Z_{uv} - u{\cdot}Z_v) \cup (u{\cdot}Z_v - u{\cdot}L - \{0\}) \\
&= Z_{uv} - u{\cdot}L - \{0\}.
\end{aligned}$$

If the optimal cyclic 2-$(v, 3, 1)$ packing family is $(g_1, \ldots, g_n)$-regular, then clearly the resultant cyclic 2-$(uv, 3, 1)$ packing family is also $(g_1, \ldots, g_n)$-regular.

We can also prove that $\mathcal{E}^{'}$ is in fact a perfect base.

If

$$d_{i_1m_1} + a_{m_1j_1}u \equiv d_{i_2m_2} + a_{m_2j_2}u \text{ mod } uv,$$

then

$$d_{i_1m_1} - d_{i_2m_2} \equiv 0 \text{ mod } u,$$

which implies that $i_1 = i_2$ and $m_1 = m_2$ since $\mathcal{D}$ is a perfect base of the $(u, 3, 1)$-CDF. In this case, we have that

$$a_{m_1j_1} - a_{m_2j_2} \equiv 0 \text{ mod } v,$$

which implies that $j_1 = j_2$ since there is no element of Z_v can appear twice in any row, except the first one, of the difference matrix.

If

$$d_{i_1m_1} + a_{m_1j_1}u \equiv -d_{i_2m_2} - a_{m_2j_2}u \text{ mod } uv,$$

then

$$(d_{i_1m_1} + d_{i_2m_2}) + (a_{m_1j_1} + a_{m_2j_2})u \equiv 0 \text{ mod } uv,$$

which implies that $d_{i_1m_1} + d_{i_2m_2} \equiv 0 \text{ mod } u$. This is impossible since $\mathcal{D}$ is a perfect base of the $(u, 3, 1)$-CDF.

If

$$d_{im_1} + a_{m_1j}u \equiv \pm f_{hm_2}u \text{ mod } uv,$$

then

$$d_{im_1} \equiv 0 \text{ mod } u,$$

which is impossible since $\mathcal{D}$ is a perfect base of the $(u, 3, 1)$-CDF.

Finally if

$$f_{h_1m_1}u \equiv \pm f_{h_2m_2}u \text{ mod } uv,$$

then

$$f_{h_1m_1} \equiv \pm f_{h_2m_2} \text{ mod } v,$$

which is impossible since $\mathcal{F}$ is a perfect base of the $(v, 3, 1)$-CDF.

The proof is then completed. □

By applying Theorem 5.1 with Theorem 5.2, we can obtain the following result.

Corollary 5.3 *Let u and v be two odd integers such that $u \equiv 1$ mod 6. Suppose that the following exist:*

(1) a $(u, 3, 1)$-CDF with a perfect base;

(2) an optimal cyclic 2-$(v, 3, 1)$ packing family with a perfect base; and

(3) a $(v, 4, 1)$-DM.

Then there exists an optimal cyclic 2-$(2uv, 4, 1)$ packing family.

One series of $(u, 3, 1)$-CDFs with a perfect base can be constructed in the following way. Let ε be a unit of order 3 in Z_{6t+1} such that $\{1-\varepsilon, 1-\varepsilon^2\}$ is a set of units of Z_{6t+1}. Consider the relation $\sim$ defined in $Z_{6t+1} - \{0\}$ by

$$x \sim y \text{ if and only if } y = \varepsilon^s x \text{ for some } s \in \{0, 1, 2\}.$$

It is easy to see that $\sim$ is an equivalence relation whose equivalence classes are the cosets $\langle\varepsilon\rangle\cdot r = \{r, \varepsilon r, \varepsilon^2 r\}$ of the multiplicative subgroup $\langle\varepsilon\rangle$ of order 3 for $r \in Z_{6t+1} - \{0\}$. Since $\{1-\varepsilon, 1-\varepsilon^2\}$ is a set of uints, each of these equivalence classes has actually size 3. Hence a complete system of distinct representatives for the equivalence classes of $\sim$ has cardinality $2t$. Let X be such a system. If there exists a set X_0 such that $X = \pm X_0$, then each of $X_0\cdot\langle\varepsilon\rangle$ and $-X_0\cdot\langle\varepsilon\rangle$ forms a $(6t+1, 3, 1)$-CDF with a perfect base. The differences arising from $\langle\varepsilon\rangle$, $\Delta\langle\varepsilon\rangle$, is $\pm\langle\varepsilon\rangle\cdot(1-\varepsilon)$. Then $\Delta(X_0\cdot\langle\varepsilon\rangle) = X_0\cdot\Delta\langle\varepsilon\rangle = X_0\cdot\pm\langle\varepsilon\rangle\cdot(1-\varepsilon) = \pm X_0\cdot\langle\varepsilon\rangle\cdot(1-\varepsilon) = X\cdot\langle\varepsilon\rangle\cdot(1-\varepsilon) = (Z_{6t+1} - \{0\})\cdot(1-\varepsilon) = Z_{6t+1} - \{0\}$, and $\Delta(-X_0\cdot\langle\varepsilon\rangle) = -\Delta(X_0\cdot\langle\varepsilon\rangle) = Z_{6t+1} - \{0\}$.

Lemma 5.4 *Let ε be a unit of order 3 in Z_{6t+1} such that $\{1-\varepsilon, 1-\varepsilon^2\}$ is a set of units of Z_{6t+1}. Let X be a complete system of distinct representatives for the equivalence classes of $\sim$ defined above. Then there exists a set X_0 such that $X = \pm X_0$.*

Proof For any $x \in X$ we claim that $x\cdot\langle\varepsilon\rangle \cap (-x\cdot\langle\varepsilon\rangle) = \emptyset$. Otherwise there would exist $x_0 \in X$ and $s \in \{0, 1, 2\}$ such that $-x_0 = x_0\varepsilon^s$. Since ε is a unit of order 3, $-x_0\varepsilon^3 = x_0\varepsilon^s$, which means $-x_0 = x_0\varepsilon^{3-s}$. So we know that $x_0\varepsilon^{3-s} = x_0\varepsilon^s$, which implies $x_0(\varepsilon^{3-2s} - 1) = 0$. If $3 - 2s \not\equiv 0 \bmod 3$, then by our hypothesis, $\varepsilon^{3-2s} - 1$ is a unit, and then $x_0 = 0$, which is impossible. So we must have $3-2s \equiv 0 \bmod 3$, that is, $s \equiv 0 \bmod 3$, and thus $s = 0$. This means $-x_0 = x_0$, which is impossible too since $6t+1$ is odd.

Therefore we can separate X into two t-subsets X_0 and $-X_0$ so that $x \in X_0$ if and only if $-x \in -X_0$. □

As a summary, we have the following result.

Theorem 5.5 *Let ε be a unit of order 3 in Z_{6t+1} such that $\{1-\varepsilon, 1-\varepsilon^2\}$ is a set of units of Z_{6t+1}. Then there exists a $(6t+1, 3, 1)$-CDF with a perfect base.*

For example, we have the following series of cyclic difference families with a perfect base.

Lemma 5.6 *There exists a $(p, 3, 1)$-CDF with a perfect base whenever $p \equiv 1$ mod 6 is a prime number.*

Proof Let θ be a primitive element of GF$(p) = Z_p$, while $p = 6t+1$ is a prime number. Then it is easy to see that θ^{2t} is a unit of order 3 of Z_{6t+1} such that $\{1-\theta^{2t}, 1-\theta^{4t}\}$ is a set of units of Z_{6t+1}. □

In Theorem 5.2, the existence of a difference matrix is assumed. Difference matrices have been investigated extensively, see for example, [14]. Here are two examples.

Lemma 5.7 *[15] Let v and k be positive integers such that $gcd(v,(k-1)!) = 1$. Let $d_{ij} \equiv ij \bmod v$ for $i = 0, 1, \ldots, k-1$ and $j = 0, 1, \ldots, v-1$. Then $D = (d_{ij})$ is a $(v,k,1)$-DM. In particular, If v is an odd prime number, then there exists a $(v,k,1)$-DM for any integer k $(\leq v)$.*

Lemma 5.8 *[19] Let k be a prime power. If there exists a $(v,k,1)$-CDF with $v \equiv 1 \bmod k(k-1)$, then there exists a $(v,k,1)$-DM.*

We can produce many more optimal cyclic difference packings with $k = 4$ and $\lambda = 1$. Below we provide one example to illustrate this construction.

Example 5.9 Take $u = 7$ and $v = 11$. $\{1, 2, 4\}$ is a perfect base for a $(7,3,1)$-CDF and an optimal cyclic 2-$(11,3,1)$ packing family respectively.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 2 & 4 & 6 & 8 & 10 & 1 & 3 & 5 & 7 & 9 \\ 0 & 3 & 6 & 9 & 1 & 4 & 7 & 10 & 2 & 5 & 8 \end{pmatrix}$$

is a $(11,4,1)$-DM in which every entry in the first row is 0. Then

$$\begin{aligned} \{\{1,2,4\}, &\quad \{8,16,25\}, \\ \{15,30,46\}, &\quad \{22,44,67\}, \\ \{29,58,11\}, &\quad \{36,72,32\}, \\ \{43,9,53\}, &\quad \{50,23,74\}, \\ \{57,37,18\}, &\quad \{64,51,39\}, \\ \{71,65,60\}, &\quad \{7,14,28\}\} \end{aligned}$$

gives an optimal cyclic 2-$(77,3,1)$ packing family with a perfect base, while

$$\begin{aligned} \{\{(1,0),(2,0),(4,0),(0,1)\}, &\quad \{(8,0),(16,0),(25,0),(0,1)\}, \\ \{(15,0),(30,0),(46,0),(0,1)\}, &\quad \{(22,0),(44,0),(67,0),(0,1)\}, \\ \{(29,0),(58,0),(11,0),(0,1)\}, &\quad \{(36,0),(72,0),(32,0),(0,1)\}, \\ \{(43,0),(9,0),(53,0),(0,1)\}, &\quad \{(50,0),(23,0),(74,0),(0,1)\}, \\ \{(57,0),(37,0),(18,0),(0,1)\}, &\quad \{(64,0),(51,0),(39,0),(0,1)\}, \\ \{(71,0),(65,0),(60,0),(0,1)\}, &\quad \{(7,0),(14,0),(28,0),(0,1)\}\} \end{aligned}$$

gives an optimal cyclic 2-$(154,4,1)$ packing family.

6 Cyclic Perfect Mendelsohn Difference Families

In this section, we make use of cyclic perfect Mendelsohn difference families to construct cyclic 2-packing families.

Given a cyclically ordered k-tuple $(a_0, \ldots, a_{k-1})$ in Z_v with orders $a_0 < a_1 < \ldots < a_{k-1} < a_0$, the pair a_i, a_{i+t} is said to be *t-apart* in $(a_0, \ldots, a_{k-1})$, where the subscripts are taken modulo k. A (v, k, λ) *cyclic perfect Mendelsohn difference family*, or briefly a (v, k, λ)-CPMDF, is a collection $\mathcal{F} = \{B_i : i \in I\}$ of cyclically ordered k-tuples of Z_v such that any element of $Z_v - \{0\}$ can be expressed in precisely λ ways as the t-apart difference of two distinct elements lying in the same member of $\mathcal{F}$ for any t such that $1 \leq t \leq k-1$. The members of $\mathcal{F}$ are called the *base blocks* of the cyclic perfect Mendelsohn difference family. The number of base blocks of a (v, k, λ)-CPMDF is equal to $\lambda(v-1)/k$, and hence a necessary condition for the existence of a (v, k, λ)-CPMDF is that $\lambda(v-1) \equiv 0 \mod k$ holds.

Theorem 6.1 *Let v be a positive integer relatively prime to k. If there exist a (v, k, λ)-CP with difference leave L and a (v, k, λ)-CPMDF, then there exists a cyclic 2-(kv, k, λ) packing family with difference leave $\{0\} \times L \cup (Z_k - \{0\}) \times \{0\}$. Moreover, if the ingredient cyclic 2-(v, k, λ) packing family is $(g_1, \ldots, g_n)$-regular, then the resultant cyclic 2-(kv, k, λ) packing family is $(k, g_1, \ldots, g_n)$-regular.*

Proof Let $\mathcal{D} = \{D_i : i \in I\}$ with $D_i = \{d_{i0}, \ldots, d_{i,k-1}\}$ and $\mathcal{E}$ =$\{E_j : j \in J\}$ with $E_j = (e_{j0}, \ldots, e_{j,k-1})$ be a cyclic 2-(v, k, λ) packing family with difference leave L and a (v, k, λ)-CPMDF respectively. We define

$$\mathcal{F} = \{\{0\} \times D_i : i \in I\} \cup \{\{(s, e_{js}) : 0 \leq s \leq k-1\} : j \in J\}.$$

It can be readily checked that $\mathcal{F}$ is a cyclic 2-(kv, k, λ) packing family over $Z_k \times Z_v$ with different leave $\{0\} \times L \cup (Z_k - \{0\}) \times \{0\}$.

Since $\mathcal{D}$ is a cyclic 2-(v, k, λ) packing family with difference leave L, it is obvious that the differences from $\{0\} \times D_i$'s cover $\{0\} \times (Z_v - L - \{0\})$ exactly λ times. Now let (t, y) be a fixed element of $Z_k \times Z_v - \{0\} \times (Z_v - \{0\}) - (Z_k - \{0\}) \times \{0\} - \{(0, 0)\}$. By the definition of $\mathcal{E}$, there are exactly λ pairs $(s, j) \in \{0, 1, \ldots, k-1\} \times J$ such that $e_{j,s+t} - e_{js} = y$, where the subscripts are all taken modulo k. This implies that $(s+t, e_{j,s+t}) - (s, e_{js}) = (t, e_{j,s+t} - e_{js})$ $= (t, y)$. So every $(t, y) \in Z_k \times Z_v - \{0\} \times (Z_v - \{0\}) - (Z_k - \{0\}) \times \{0\} - \{(0, 0)\}$ is representable as λ differences from $\{\{(s, e_{js}) : 0 \leq s \leq k-1\} : j \in J\}$. Moreover, such representations can not be more than λ times, because the number of differences from $\{\{(s, e_{js}) : 0 \leq s \leq k-1\} : j \in J\}$ is $k(k-1)|J| = \lambda(k-1)(v-1)$, as $k|J| = \lambda(v-1)$ from the definition of a cyclic perfect Mendelsohn difference family. But $(k-1)(v-1)$ is the cardinality of $Z_k \times Z_v - \{0\} \times (Z_v - \{0\}) - (Z_k - \{0\}) \times \{0\} - \{(0, 0)\}$. So we can conclude that the differences from $\mathcal{F}$ cover $Z_k \times Z_v - \{0\} \times L - (Z_k - \{0\}) \times \{0\} - \{(0, 0)\}$ exactly λ times, and hence $\mathcal{F}$ is a cyclic 2-(kv, k, λ) packing family with difference leave $\{0\} \times L \cup (Z_k - \{0\}) \times \{0\}$, since $\gcd(k, v) = 1$ by the hypothesis. The second assertion is trivially true then. □

By Theorem 3.5, we can obtain the following result.

Theorem 6.2 *If there exist a cyclic* 2-$(v,k,1)$ *packing family with difference leave* L *such that* $0 \le |L| < (k-1)^2$*, and a* $(v,k,1)$*-CPMDF, then there exists an optimal cyclic* 2-$(kv,k,1)$ *packing family. Moreover, if the ingredient cyclic* 2-$(v,k,1)$ *packing family is* $(g_1,\ldots,g_n)$*-regular, then the resultant optimal cyclic* 2-$(kv,k,1)$ *packing family is* $(k,g_1,\ldots,g_n)$*-regular.*

Proof Note that in a $(v,k,1)$-CPMDF, $v \equiv 1 \bmod k$, which implies that $\gcd(v,k)=1$. Then apply Theorems 6.1 and 3.5. □

Many infinite series of $(v,k,1)$-CPMDFs can be found in [22]. Here we give one series as examples.

Lemma 6.3 *Let* $v=\prod_{i\in I} p_i^{n_i}$ *be the prime power factorization of* v *such that* $p_i \ge k$ *for all* $i \in I$*. Let* $f_i = gcd(k,p_i-1)$ *for all* $i\in I$*, and* $f = gcd(f_i : i \in I)$*. If* $f=k$*, then there exists a* $(v,k,1)$*-CPMDF.*

Theorems 6.1 and 6.2 together with the existence results on cyclic packing families and cyclic perfect Mendelsohn difference families can yield many new infinite series of optimal cyclic packing families. Here are a few examples.

Corollary 6.4 *If* $p=12t+1$ *is a prime number, then there exists an optimal cyclic* $(4,5)$*-regular packing family.*

Proof Apply Theorems 6.1 and 6.2 with Corollary 4.9 and Lemma 6.3. □

Corollary 6.5 *Let* $v=p_1p_2\cdots p_r$ *be the prime factorization of* v *where* $p_1,p_2,\ldots,p_r$ *are all prime numbers congruent to* 1 *modulo* 12*. Then there exists an optimal cyclic* 4*-regular* 2-$(4v,4,1)$ *packing family.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.6 and 6.3. □

Corollary 6.6 *Let* $v=p_1p_2\cdots p_r$ *be the prime factorization of* v *where* $p_1,p_2,\ldots,p_r$ *are all prime numbers congruent to* 1 *modulo* 12*. Then there exists an optimal cyclic* $(4,5)$*-regular* 2-$(20v,4,1)$ *packing family.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.10 and 6.3. □

Corollary 6.7 *Let* $v=p_1p_2\cdots p_r$ *be the prime factorization of* v *where* $p_1,p_2,\ldots,p_r$ *are all prime numbers congruent to* 1 *modulo* 20*. Then there exists an optimal cyclic* 5*-regular* 2-$(5v,5,1)$ *packing family.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.7 and 6.3. □

Corollary 6.8 *Let $v = p_1p_2\cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to 1 modulo 20. Then there exists an optimal cyclic $(5, 11)$-regular 2-$(55v, 5, 1)$ packing family.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.11 and 6.3. □

Corollary 6.9 *If $p = 30t+1$ is a prime number $\neq 61$, then there exists an optimal cyclic $(6, 7)$-regular 2-$(42p, 6, 1)$ packing family.*

Proof Apply Theorems 6.1 and 6.2 with Corollary 4.11 and Lemma 6.3. □

Corollary 6.10 *Let $v = p_1p_2\cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to 1 modulo 30 but not equal to 61. Then there exists an optimal cyclic 6-regular 2-$(6v, 6, 1)$ packing family.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.8 and 6.3. □

Corollary 6.11 *Let $p \in \{7, 13, 19\}$. Let $v = p_1p_2\cdots p_r$ be the prime factorization of v where $p_1, p_2, \ldots, p_r$ are all prime numbers congruent to 1 modulo 30 but not equal to 61. Then there exists an optimal cyclic $(6, p)$-regular 2-$(6pv, 6, 1)$ packing family.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.12 and 6.3. □

Corollary 6.12 *Let $p \equiv 1$ mod $k(k-1)$ be an odd prime number. Then there exists an optimal cyclic k-regular 2-$(kp, k, 1)$ packing family whenever $p > D(k)$, where $D(k)$ was defined in Lemma 3.9.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.9 and 6.3. □

Corollary 6.13 *Let p_k be a prime number such that $k \leq p_k < (k-1)^2 + 1$ and $p_k \equiv 1$ mod k. Let $p \equiv 1$ mod $k(k-1)$ be an odd prime number. Then there exists an optimal cyclic (k, p_k)-regular 2-$(kp_kp, k, 1)$ packing family whenever $p > D(k)$, where $D(k)$ was defined in Lemma 3.9.*

Proof Apply Theorems 6.1 and 6.2 with Lemmas 3.13 and 6.3. □

Corollary 6.14 *Let $k+1$ be a prime number. Let $p = k(k-1)t + 1$ be a prime number where $k-1$ and kt are not both even. If $p > max\{B(k-1), D(k)\}$, where $B(k-1)$ and $D(k)$ were defined in Lemmas 4.3 and 3.9 respectively, then there exists an optimal cyclic $(k, k+1)$-regular 2-$(k(k+1)p, k, 1)$ packing family.*

Proof Apply Theorems 6.1 and 6.2 with Corollary 4.12 and Lemma 6.3. □

7 Concluding Remarks

In this article, we established an equivalence between optimal optical orhtogonal codes and optimal cyclic t-packing families. This relation allows us to construct optimal optical orthogonal codes by way of optimal cyclic t-packing families. This approach was showed to be quite accessible when t is 2 in this article. However, the construction for optimal cyclic t-packing families is apparently a difficult task in general. Determining the spectrum of optimal cyclic t-$(v,k,1)$ packing families is becoming an interesting and challenging problem in design theory and coding theory.

References

[1] R. J. R. Abel, *Difference families,* in: C. J. Colbourn and J. H. Dinitz, eds., *CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996, 270–287.

[2] E. F. Brickell and V. K. Wei, *Optical orthogonal codes and cyclic block designs,* Congr. Numer. **58** (1987), 175–192.

[3] A. E. Brouwer and G. H. J. van Rees, *More mutually orthogonal latin squares,* Discrete Math. **39** (1982), 263–281.

[4] M. Buratti, *Constructions for $(q,k,1)$ difference families with q a prime power and $k=4,5$,* Discrete Math. **138** (1995), 169–175.

[5] M. Buratti, *Improving two theorems of Bose on difference families,* J. Combin. Des. **3** (1995), 15–24.

[6] K. Chen and L. Zhu, *Existence of $(q,6,1)$ difference families with q a prime power,* Des. Codes. Crypto. *15* (1998), 167–173.

[7] K. Chen and L. Zhu, *Existence of $(q,k,1)$ difference families with q a prime power and $k=4,5$,* J. Combin. Des. **7** (1999), 21–30.

[8] K. Chen, G. H. J. van Rees and L. Zhu, *$V(m,t)$ and its variants,* J. Statist. Plann. Inference, to appear.

[9] K. Chen and L. Zhu, *Existence of $V(m,t)$ vectors,* J. Statist. Plann. Inference, to appear.

[10] K. Chen and L. Zhu, *Improving Wilson's bound on difference families,* preprint.

[11] F. R. K. Chung, J. A. Salehi and V. K. Wei, *Optical orthogonal codes: design, analysis, and applications,* IEEE Trans. Info. Theory **35** (1989), 595–604. Correction: IEEE Trans. Info. Theory **38** (1992), 1429.

[12] H. Chung and P. V. Kumar, *Optical orthogonal codes—new bounds and an optimal construction,* IEEE Trans. Inform. theory **36** (1990), 866-873.

[13] C. J. Colbourn, *Some direct constructions for incomplete transversal designs,* J. Statist. Plann. Inference, to appear.

[14] C. J. Colbourn and W. de Launey, *Difference matrices,* in: C. J. Colbourn and J. H. Dinitz, eds., *CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996, 287–297.

[15] M. J. Colbourn and C. J. Colbourn, *Recursive constructions for cyclic block designs,* J. Statist. Plann. Inference **10** (1984), 97–103.

[16] W. T. Federer, *Construction of class of experimental designs using transversals in Latin squares and Hedayat's sum composition method,* in: T. A. Bancroft, ed., *Statistical Papers in Honor of George W. Snedecor*, The Iowa State University Press, Ames, Iowa, 1972, 91–114.

[17] G. Ge, *All* $V(3,t)$*'s exist for* $3t+1$ *a prime power,* J. Combin. Math. Combin. Computing, to appear.

[18] S. W. Golomb, *Digital Communication with Space Application,* Prentice Hall, Englewood Cliff, N. J., Penisula Publishing, Los Altos, Ca. 1982.

[19] J. Jimbo and S. Kuriki, *On a composition of cyclic* 2*-designs,* Discrete Math. **46** (1983), 249–255.

[20] S. M. Johnson, *A new upper bound for error-correcting codes,* IEEE Trans. Inform. Theory **8** (1962), 203–207.

[21] S. Kageyama and Y. Miao, *Nested designs with block size five and subblock size two,* J. Statist. Plann. Inference. **64** (1997), 125–139.

[22] C. Lam and Y. Miao, $(C_k \oplus G, k, \lambda)$ *difference families,* preprint.

[23] C. H. A. Ling, Y. Lu, G. H. J. van Rees and L. Zhu, $V(m,t)$*'s for* $m = 4, 5, 6,$ J. Statist. Plann. Inference, to appear.

[24] J. L. Massey and P. Mathys, *The collision channel without feedback,* IEEE Trans. Inform. Theory **31** (1985), 192-204.

[25] Y. Miao and S. Yang, *Concerning the vector* $V(m,t)$*,* J. Statist. Plann. Inference **51** (1996), 223–227.

[26] Y. Miao and L. Zhu, *Perfect Mendelsohn designs with block size six,* Discrete Math. **143** (1995), 189–207

[27] R. C. Mullin, P. J. Schellenberg, D. R. Stinson and S. A. Vanstone, *Some results on the existence of squares,* Ann. Discrete Math. **6** (1980), 257–274.

[28] D. A. Preece, *Nested balanced incomplete block designs,* Biometrika **54** (1967), 479–486.

[29] G. H. J. van Rees, *All $V(m,t)$'s exist for $3t+1$ a prime,* J. Combin. Des. **3** (1995), 339–403.

[30] J. A. Salehi, *Code division multiple-access techniques in optical fibre networks – part I: Fundamental principles,* IEEE Trans. Info. Theory **37** (1989), 824–833.

[31] J. A. Salehi, *Emerging optical code-division multiple access communications systems,* IEEE Networks **3–2** (1989), 31–39.

[32] J. A. Salehi and C. A. Brackett, *Code division multiple access techniques in optical fiber networks,* IEEE Trans. Commun. **37** (1989), 824–842.

[33] J. Schonheim, *On maximal systems of k-tuples,* Studia Sci. Math. Hungar. **1** (1966), 363–368.

[34] M. P. Vecchi and J. A. Salehi, *Neuromorphic networks based on sparse optical orthogonal codes,* Neural Information Processing Systems–Natural and Synthetic, Amer. Inst. Physics, 1988, 814–823.

[35] J. Yin, *Some combinatorial constructions for optical orthogonal codes,* Discrete Math. **185** (1998), 201–219.