A General Construction for Optimal Cyclic Packing Designs

Jianxing Yin

Department of Mathematics, Suzhou University, Suzhou 215006, People’s Republic of China

Communicated by the Managing Editors

Received October 9, 2000; published online December 19, 2001

Cyclic packing designs of pairs have various applications in communications. In this paper, the concept of a \((g_1, g_2, \ldots, g_r; u)\)-regular cyclic packing design is defined, and used to establish a quite general recursive construction concerning cyclic packing designs. As corollaries, we are able to unify many known constructions for cyclic designs. As an application, we obtain infinite series of new optimal cyclic packing designs which can be utilized directly to produce new optimal optical orthogonal codes.

Key Words: cyclic packing; general construction.

1. INTRODUCTION AND TERMINOLOGY

Typically, a packing design of pairs (or packing, in brief) of order \(v\) with block size \(k\), denoted by \(P(k, \lambda; v)\), is a pair \((X, B)\) where \(X\) is a \(v\)-set (of points), and \(B\) is a collection of \(k\)-subsets (called blocks) of \(X\) such that any pair of distinct points from \(X\) occurs in at most \(\lambda\) of the blocks. A natural generalization of this notion is obtained by allowing blocks to have different sizes. More specifically, let \(K\) be a subset of positive integers. A packing of order \(v\) with block sizes from \(K\), \(P(K, \lambda; v)\), is defined as a pair \((X, B)\) where \(X\) is a \(v\)-set (point set) and \(B\) is a collection of subsets (blocks) of \(X\) which satisfy the following two properties:

1. if \(B \in \mathcal{B}\), then \(|B| \in K\);
2. every pair of distinct points of \(X\) appears in at most \(\lambda\) blocks of \(\mathcal{B}\).

In the particular case where every pair of distinct points of \(X\) appears in exactly \(\lambda\) blocks of \(\mathcal{B}\), the packing is exact, which is nothing else than a pairwise balanced design (PBD), \(B(K, \lambda; v)\). A \(B(\{k\}, \lambda; v)\) is known as a balanced incomplete block design (BIBD).

Research supported by NSFC Grant 10071056. E-mail: jxyin@suda.edu.cn.
An automorphism of a $P(K, \lambda; v)$ ($X, \mathcal{A}$) is a bijection $h: X \to X$ such that $B \in \mathcal{A}$ if and only if $h(B) = \{h(b): b \in B\} \in \mathcal{A}$. A $P(K, \lambda; v)$ is said to be cyclic if it admits an automorphism that is a permutation consisting of a single cycle of length $v$.

For more general packing problem and related results, the interested reader may refer to Mills and Mullin’s survey [14], which contains 110 references. We only consider the case $\lambda = 1$ in this paper. As the terminology suggests, if ($X, \mathcal{A}$) is a cyclic $P(K, 1; v)$, then the point set $X$ can be identified with $\mathbb{Z}_v$, the residue ring of integers modulo $v$. The cyclic automorphism is then just the bijection mapping $h: i \mapsto i + 1 \mod v$. For a cyclic $P(K, 1; v)$ $(\mathbb{Z}_v, \mathcal{A})$, let $B = \{b_1, \ldots, b_k\}$ be a block in $\mathcal{A}$. The block orbit containing $B$ is defined to be the set of the following distinct blocks:

$$h'(B) = B + i = \{b_1 + i, \ldots, b_k + i\} \mod v,$$

for $i \in \mathbb{Z}_v$. If a block orbit has $v$ distinct blocks, i.e., its setwise stabilizer is the identity $\{0\}$, then this block orbit is said to be full, otherwise short. An arbitrary set of representatives for these orbits of $\mathcal{A}$ is called base blocks of the packing.

It is important to note that a cyclic $P(K, 1; v)$ including the exact case may have short block orbits. Following [18], we use notation $CP(K, 1; v)$ to denote a cyclic $P(K, 1; v)$ without short block orbits throughout what follows. A straightforward fact is that a $CP(K, 1; v)$ is uniquely determined by its base blocks. Given an arbitrary set of base blocks of a $CP(K, 1; v)$, one can obtain the packing by successively adding 1 to each base blocks modulo $v$. So, a quite convenient way of viewing a $CP(K, 1; v)$ is from the difference family perspective. To be precise, a $CP(K, 1; v)$ can be defined equivalently as a family of subsets (called base blocks) of $\mathbb{Z}_v$, $\mathcal{A}$, each of cardinality from $K$, such that the list of the differences arisen from $\mathcal{A}$,

$$A \mathcal{A} = \{a - b: a, b \in B, a \neq b, B \in \mathcal{A}\},$$

cover each nonzero integer in $\mathbb{Z}_v$ at most once.

Consider a $CP(K, 1; v)$, $\mathcal{A}$. Let $H_1, H_2, \ldots, H_r$ and $H$ be $(r + 1)$ mutually distinct additive subgroups of $\mathbb{Z}_v$ whose orders are $g_1, g_2, \ldots, g_r$ and $u$ respectively, such that $H_i \cap H_j = H$ for any integers $i$ and $j$ satisfying $1 \leq i < j \leq r$. If the difference leave of $\mathcal{A}$, $(\mathbb{Z}_v \setminus A \mathcal{A})$, along with zero, form the union of $H_i$($i = 1, 2, \ldots, r$), as sets, then we call $\mathcal{A}$ $(g_1, g_2, \ldots, g_r; u)$-regular. When $u = 1$, we drop the letter $u$ and write $(g_1, g_2, \ldots, g_r)$-regular for $(g_1, g_2, \ldots, g_r; u)$-regular, as in [8]. For the special case where $r = 1$, this notion can be found in [18].
Example 1.1. A \((10, 6, 4; 2)\)-regular \(\text{CP}(\{3, 5\}, 1; 60)\) is given by the following base blocks:

\[
\begin{align*}
\{0, 8, 21\} & \quad \{0, 9, 23\} \\
\{0, 11, 28\} & \quad \{0, 16, 41\} \\
\{0, 4, 5, 7, 38\}
\end{align*}
\]

Here, \(H_1 = \{0, 6, ..., 54\}\), \(H_2 = \{0, 10, 20, 30, 40, 50\}\), \(H_3 = \{0, 15, 30, 45\}\), and \(H = \{0, 30\}\).

Let us now return to the case where \(K = \{k\}\). In this case, we always omit the braces, and write \(P(k, 1; v)\) and \(\text{CP}(k, 1; v)\) for \(P(\{k\}, 1; v)\) and \(\text{CP}(\{k\}, 1; v)\) respectively. It is easy to see that the number of base blocks in a \(\text{CP}(k, 1; v)\) is upper bounded by \(\frac{v-1}{2}k(k-1)\). A \(\text{CP}(k, 1; v)\) is said to be optimal, if it contains \(\frac{v-1}{2}k(k-1)\) base blocks. Closely related to an optimal \(\text{CP}(k, 1; v)\) is an optimal \((v, k, 1)\) optical orthogonal code (briefly \((v, k, 1)\)-OOC) which we give a brief description below.

A \((v, k, 1)\)-OOC, \(\mathcal{C}\), is a family of \((0, 1)\) -sequences (called codewords) of length \(v\) and weight \(k\) satisfying the following two properties:

1. \(\sum_{0 \leq i < v-1} x_i x_{i+i} \leq 1\) for any \(x = (x_0, x_1, ..., x_{v-1}) \in \mathcal{C}\) and any integer \(i \neq 0 \pmod{v}\) (the auto-correlation property);
2. \(\sum_{0 \leq i < v-1} x_i y_{i+i} \leq 1\) for any \(x = (x_0, x_1, ..., x_{v-1}) \in \mathcal{C}\), \(y = (y_0, y_1, ..., y_{v-1}) \in \mathcal{C}\) with \(x \neq y\), and any integer \(i\) (the cross-correlation property).

Here, all subscripts are reduced modulo \(v\). A \((v, k, 1)\)-OOC is optimal if it contains \(\frac{v-1}{2}k(k-1)\) codewords.

The study of optical orthogonal codes was first motivated by an application in a fiber optic code-division multiple access channel which requires binary sequences with good correlation properties. Recent work has also been done on using optical orthogonal codes for multimedia transmission in fiber-optic LANs and in multirate fiber-optic CDMA systems. For related details, the interested reader may refer to [4, 7, 12, 13, 15–17]. For a more combinatorial background literature, see Bird and Keedwell [1].

It is known that

**Theorem 1.2 [18].** An optimal \((v, k, 1)\)-OOC is equivalent to an optimal \(\text{CP}(k, 1; v)\).

Cyclic packings have many other applications in communications. In this paper, we will not attempt to give a sufficient introduction in this aspect; instead we will describe a quite general recursive construction concerning optimal cyclic packings. As corollaries, we are able to unify many known
constructions for cyclic designs. As an application, we obtain infinite series of new optimal CP(k, 1; v)s, equivalently new optimal optical orthogonal codes.

Before finishing this section, we wish to point out that a g-regular CP(k, 1; v), according to its definition, can exist only if \( v \equiv g \pmod{k(k−1)} \), which is not necessarily optimal. However, when \( 1 \leq g \leq k(k−1) \), then a g-regular CP(k, 1; v) is also optimal. For completeness, we admit \( 1 \leq v \leq k(k−1) \) in a CP(k, 1; v), and the degenerate CP(k, 1; v) containing zero base blocks will be considered to be optimal and v-regular in the sequel.

2. THE CONSTRUCTION

We begin with the definition of a semi-cyclic group divisible design (SCGDD).

Let \( g \) and \( n \) be positive integers, and \( K \) a subset of positive integers. Let \( \mathcal{F} \) be a collection of subsets (called base blocks) of sizes from \( K \) in \( I_n \times Z_g \), where \( I_n = \{1, 2, ..., n\} \). For any two distinct integers \( i \) and \( j \) of \( I_n \), we define

\[
A_{ij}B = \{ b - a : (i, a), (j, b) \in B \text{ and } (i, a) \neq (j, b) \}, \quad B \in \mathcal{F};
\]

\[
A_{ij}\mathcal{F} = \sum_{B \in \mathcal{F}} A_{ij}B.
\]

Here the operation in \( A_{ij}B \) is performed in \( Z_g \). The differences in \( A_{ij}\mathcal{F} \) are often named \((i, j)\) mixed differences from \( \mathcal{F} \) (see [9]). We call \( \mathcal{F} \) a \( K\)-SCGDD of type \( g^n \) if, for any two distinct integers \( i \) and \( j \) of \( I_n \),

\[
A_{ij}\mathcal{F} = Z_g.
\]

As before, a \( \{k\}\)-SCGDD will be abbreviated to a \( k\)-SCGDD.

Consider a \( k\)-SCGDD of type \( g^k \). By a simple calculation we can know that such an SCGDD contains exactly \( g \) base blocks. Label these \( g \) base blocks by the integers of \( Z_g \), and then arrange them into a \( k \times g \) matrix \( D = (d_{ij}) \) in such a way that the cell \((i, c)\) is assigned to the second coordinate of the point \((i, c)\) in the \( j \)th base block for \( 1 \leq i \leq k \) and \( 0 \leq j \leq g−1 \). The interesting thing to note is that this matrix satisfies the following two properties:

1. each of its entries is an integer from \( Z_g \);
2. for any two distinct rows \( s \) and \( t \) the list \( \{d_{ij} - d_{ij} : 0 \leq j \leq v-1\} \) is equal to \( Z_g \).
Such a matrix is referred to as a cyclic difference matrix and denoted by 
(k, g)-CDM. Given a (k, g)-CDM, we can also form a k-SCGDD of type 
g^k by reversing the above process.

We remark that difference matrices have attracted tremendous attention 
in design theory (see, for example, [6]). Regarding their existence we 
mention the following two results. For more information, the interested 
reader may refer to [6].

**Lemma 2.1** [5]. Let m be a positive integer which is relatively prime to 
(k−1)!. Then a (k, m)-CDM exists.

**Lemma 2.2** [11]. Suppose that k is a prime power and a cyclic BIBD
B(k, 1; v) with v ≡ 1 (mod k(k−1)) exists, then a (k, v)-CDM also exists.

Our general construction will be mainly based on the following important 
lemma, which serves to create a new regular CP(K, 1; v) from known 
one.

**Lemma 2.3.** Let K_1 and K_2 be two subsets of positive integers (not necessarily disjoint). Let t and r be integers satisfying 0 ≤ t ≤ r − 1. Suppose that the following exist:

1. a (g_1, g_2, ..., g_r; u)-regular CP(K_1, 1; v);
2. a K_2-SCGDD of type m^h for every h ∈ K_1;
3. an mu-regular CP(K_2, 1; mg_j) for 1 ≤ j ≤ t when t ≥ 1

Then there exists a (mg_{t+1}, mg_{t+2}, ..., mg_r; mu)-regular CP(K_2, 1; mv).

**Proof.** Let $\mathcal{A}$ be the collection of base blocks of a given (g_1, g_2, ..., g_r; u)-regular CP(K_1, 1; v) whose difference leave along with zero is the union of additive subgroups $H_j$ of $\mathbb{Z}$, (j = 1, 2, ..., r), in which $H_i \cap H_j = H$ for 1 ≤ i < j ≤ r. By definition, $H_j$ has order $g_j$, and hence must be generated by the integer $v/g_j$, (1 ≤ j ≤ r). Similarly, $H$ must be generated by the integer $v/u$. So, the least common multiple of $v/g_i$ and $v/g_j$, (1 ≤ i < j ≤ r) is $v$. For each base block $B = \{b_1, b_2, ..., b_h\}$ of $\mathcal{A}$, by hypothesis, we have $h \in K_1$ and a K_2-SCGDD of type $m^h$, $\mathcal{F}$, over $I_h \times \mathbb{Z}_m$. We can then construct a collection $\mathcal{A}(B)$ of subsets of $\mathbb{Z}$ whose sizes from $K_2$,

$$\{b_{i_1} + x_1 \cdot v, b_{i_2} + x_2 \cdot v, ..., b_{i_k} + x_k \cdot v\},$$

where $\{(i_1, x_1), (i_2, x_2), ..., (i_k, x_k)\}$ runs over all base blocks in $\mathcal{F}$ and the sums are all reduced modulo mv. Since, for any two distinct integers $i$ and $j$
of \( I_i \), the list of \((i, j)\) mixed differences from \( \mathcal{A} \) is equal to \( Z_m \), the list of differences from \( \mathcal{A}(B) \) is then
\[
\Delta \mathcal{A}(B) = \{ (b_j - b_i) + v \cdot Z_m : b_i, b_j \in B \text{ and } b_i \neq b_j \}.
\]

In this way, as \( B \) ranges over all base blocks from \( \mathcal{A} \), we obtain a collection \( \mathcal{D} = \bigcup_{B \in \mathcal{A}} \mathcal{A}(B) \) of subsets of \( Z_m \), each of which has size from \( K_2 \).

The list of differences from \( \mathcal{D} \) is
\[
\Delta \mathcal{D} = \{ d + v \cdot Z_m : d \in \Delta \mathcal{A} \}.
\]

It is obvious that every integer in \( Z_m \) can be written uniquely as \( a + bv \) with \( 0 \leq a \leq v - 1 \) and \( 0 \leq b \leq m - 1 \). This implies that
\[
Z_m \setminus \Delta \mathcal{D} = \{ d + v \cdot Z_m : d \in Z_m \setminus \Delta \mathcal{A} \}.
\]

Now, for \( 1 \leq j \leq r \), let
\[
\overline{H}_j = \{ d + v \cdot Z_m : d \in H_j \},
\]
which is the additive subgroup generated by integer \( v/g_j \) in \( Z_m \). Let
\[
\overline{H} = \{ d + v \cdot Z_m : d \in H \}
\]
which is the additive subgroup generated by integer \( z \) in \( Z_m \). Then we have
\[
Z_m \setminus \Delta \mathcal{D} = \bigcup_{1 \leq j \leq r} \overline{H}_j,
\]
since \( Z_m \setminus \Delta \mathcal{A} = \bigcup_{1 \leq j \leq r} H_j \). Meanwhile, we have \( \overline{H}_j \cap \overline{H}_j = \overline{H} \), since the least common multiple of \( v/g_i \) and \( v/g_j \) is \( v/u \) for \( 1 \leq i < j \leq r \). Therefore, \( \mathcal{D} \) is the collection of base blocks of a \((mg_1, mg_2, ..., mg_r; mu)\)-regular \text{CP}(\( K_2, 1 ; m v \)) over \( Z_m \). Its difference leave along with zero is the union of \( \overline{H}_j \) \( (j = 1, 2, ..., r) \). The result for \( t = 0 \) then follows.

For the case where \( t \geq 1 \), we first note the fact from algebra that any cyclic finite group contains one and only one subgroup of order \( f \) for every positive divisor \( f \) of its order. Further, for any integer \( j(1 \leq j \leq r) \), \( \overline{H}_j = (v/g_j) \cdot Z_{mg_j} \) is isomorphic to \( Z_{mg_j} \). So, by hypothesis, we can construct an \( mu \)-regular \text{CP}(\( K_2, 1 ; mg_j \)) over \( \overline{H}_j, \mathcal{A}(H_j) \), so that its difference leave along with zero form the additive subgroup \( \overline{H} \) for \( 1 \leq j \leq t \). Thus we obtain another collection \( \mathcal{E} = \bigcup_{1 \leq j \leq t} \mathcal{A}(H_j) \) of subsets of \( Z_m \), each of which has size from \( K_2 \). The list of differences from \( \mathcal{E} \) is
\[
\Delta \mathcal{E} = \bigcup_{1 \leq j \leq t} (\overline{H}_j \setminus \overline{H}),
\]
and hence

$$Z_m \setminus A(\mathcal{D} \cup \mathcal{C}) = \bigcup_{r+1 \leq j \leq r} \mathcal{H}_j.$$ 

Thus, a \((mg_{s+1}, mg_{s+2}, \ldots, mg_{r}; mu)\)-regular CP\((K_s, 1; mu)\) is formed by taking all subsets in \((\mathcal{D} \cup \mathcal{C})\) as base blocks. The proof is then complete. \(\square\)

Taking \(t = r - 1\) and \(K_s = \{k\}\) in Lemma 2.3 we obtain the following.

**Lemma 2.4.** Suppose that the following exist:

1. a \((g_1, g_2, \ldots, g_r; u)\)-regular CP\((K, 1; v)\):
2. a \(k\)-SCGDD of type \(m^h\) for every \(h \in K\):
3. an \(mu\)-regular CP\((k, 1; mg_j)\) for \(1 \leq j \leq r - 1\).

Then there exists an \(mg_r\)-regular CP\((k, 1; mv)\).

We also require the following lemma.

**Lemma 2.5.** Suppose that both a \(g\)-regular CP\((k, 1; v)\) and an optimal CP\((k, 1; g)\) exist. Then an optimal CP\((k, 1; v)\) also exists. Moreover, if the given CP\((k, 1; g)\) is \((g_1, g_2, \ldots, g_r; u)\)-regular, then so is the derived CP\((k, 1; v)\).

**Proof.** Let \(\mathcal{A}\) be the collection of base blocks of the given \(g\)-regular CP\((k, 1; v)\) whose difference leave along with zero form additive subgroup \(H\) of \(Z_v\). To complete an optimal CP\((k, 1; v)\), we construct an optimal CP\((k, 1; g)\) over \(H\), by hypothesis. For a \((g_1, g_2, \ldots, g_r; u)\)-regular CP\((k, 1; v)\), we replace \(H\) by a \((g_1, g_2, \ldots, g_r; u)\)-regular CP\((k, 1; g)\). \(\square\)

As an immediate consequence of Lemma 2.4 and Lemma 2.5, we obtain the following general construction concerning cyclic packings with block size \(k\).

**Theorem 2.6.** Suppose that the following exist:

1. a \((g_1, g_2, \ldots, g_r; u)\)-regular CP\((K, 1; v)\):
2. a \(k\)-SCGDD of type \(m^h\) for every \(h \in K\):
3. an \(mu\)-regular CP\((k, 1; mg_j)\) for \(1 \leq j \leq r - 1\).

Then there exists an \(mg_r\)-regular CP\((k, 1; mv)\). Moreover, an optimal CP\((k, 1; mv)\) exists provided an optimal CP\((k, 1; mg_r)\) exists.

We should add at this stage that the requirement (2) of Theorem 2.6 is satisfied trivially when \(m = 1\), and so is the requirement (3) when \(r = 1\).
To illustrate the construction we give an example.

Example 2.7. Suppose that we wish to construct an optimal CP(3, 1; 72). We may let $K = \{3\}, k = m = 3$ in Theorem 2.6 and proceed in the following steps.

1. Take a (8, 6; 2)-regular CP(3, 1; 24) over $\mathbb{Z}_{24}$, say

$$\mathcal{A} = \{\{0, 1, 11\}, \{0, 2, 7\}\}.$$ 

Then we have $H_1 = \{0, 3, \ldots, 21\}, H_2 = \{0, 4, \ldots, 20\}, H = \{0, 12\}$.

2. Take a 3-SCGDD of type $3^3$, say its base blocks are

$$\{(1, 0), (2, 0), (3, 0)\}, \{(1, 1), (2, 1), (3, 2)\}, \{(1, 2), (2, 2), (3, 1)\}.$$ 

Then use this 3-SCGDD to produce the following 3-subsets of $\mathbb{Z}_{72}$ from $\mathcal{A}$ (as indicated in the proof of Lemma 2.3):

$$\{0, 1, 11\} \quad \{0, 25, 59\} \quad \{0, 49, 35\}$$

$$\{0, 2, 7\} \quad \{0, 26, 55\} \quad \{0, 50, 31\}.$$ 

This creates a (24, 18; 6)-CP(3, 1; 72) over $\mathbb{Z}_{72}$. Its difference leave along with zero is the union of the following two additive subgroups of $\mathbb{Z}_{72}$,

$$\bar{H}_1 = \{d + 24 \cdot \mathbb{Z}_3 : d \in H_1\} = 3 \cdot \mathbb{Z}_{24},$$

$$\bar{H}_2 = \{d + 24 \cdot \mathbb{Z}_3 : d \in H_2\} = 4 \cdot \mathbb{Z}_{18},$$

where $\bar{H}_1 \cap \bar{H}_2 = \{d + 24 \cdot \mathbb{Z}_3 : d \in H\} = 12 \cdot \mathbb{Z}_6$.

3. To complete an optimal CP(3, 1; 72), put a 6-regular CP(3, 1; 24) over $\bar{H}_1$:

$$3 \cdot \{0, 1, 10\}, 3 \cdot \{0, 2, 5\}, 3 \cdot \{0, 6, 13\}.$$ 

Its difference leave along with zero is just $\bar{H}_1 \cap \bar{H}_2$. Finally, put an optimal CP(3, 1; 18) over $\bar{H}_2$:

$$4 \cdot \{0, 1, 3\}, 4 \cdot \{0, 4, 10\}.$$ 

3. COROLLARIES AND APPLICATIONS

It should be emphasized that the notion of a $(g_1, g_2, \ldots, g_r; u)$-regular CP($K$, 1; $v$) defined in Section 1 is quite general. Some of its special cases have been given other names in design theory. For example, using our notation a cyclic double group divisible design [19] without short block
orbits is essentially a \((g_1, g_2; u)\)-regular \(CP(K, 1; v)\). A cyclic group divisible design [6] without short block orbits is essentially a \(u\)-regular \(CP(K, 1; v)\). A cyclic PBD \(B(K, 1; v)\) without short block orbits can be viewed as a \(1\)-regular \(CP(K, 1; v)\). Especially, a cyclic \((v, k, 1)\) difference family [6] is just a \(1\)-regular \(CP(k, 1; v)\), which can be developed over \(Z_v\) to obtain a cyclic BIBD \(B(k, 1; v)\) with \(v \equiv 1 \pmod{k(k-1)}\) and vice versa. And a cyclic \((v, k, 1)\) partial difference family [6] is a \(k\)-regular \(CP(k, 1; v)\), which gives a cyclic \(B(k, 1; v)\) with \(v \equiv k \pmod{k(k-1)}\) and vice versa.

As corollaries of the construction shown in Theorem 2.6, we are able to derive many known constructions regarding cyclic designs which we develop below.

**Theorem 3.1** [18]. Suppose that there exist:

1. a \(g\)-regular \(CP(K, 1; v)\);
2. a \(k\)-SCGDD of type \(m^h\) for every \(h \in K\);
3. an optimal \(CP(k, 1; mg)\).

Then there exists an optimal \(CP(k, 1; mv)\).

**Proof.** Apply Theorem 2.6 with \(r = 1\).

**Theorem 3.2** [18]. Suppose that there exist:

1. a cyclic PBD \(B(K, 1; v)\) without short block orbits;
2. a \(k\)-SCGDD of type \(m^h\) for every \(h \in K\);
3. an optimal \(CP(k, 1; m)\).

Then there exists an optimal \(CP(k, 1; mv)\).

**Proof.** Regard the given cyclic PBD as a \(1\)-regular \(CP(K, 1; v)\) and apply Theorem 2.6 with \(r = u = 1\).

**Theorem 3.3** [18]. Suppose that there exist:

1. a cyclic BIBD \(B(h, 1; v)\) with \(v \equiv 1 \pmod{h(h-1)}\);
2. a \(k\)-SCGDD of type \(m^h\);
3. an optimal \(CP(k, 1; m)\).

Then there exists an optimal \(CP(k, 1; mv)\).

**Proof.** Regard the given cyclic BIBD as a \(1\)-regular \(CP(h, 1; v)\) and apply Theorem 2.6 with \(r = u = 1\) and \(K = \{h\}\).
Theorem 3.4 [11]. Let \( e = 1 \) or \( k \). Suppose that there exist:

1. a cyclic BIBD \( B(k, 1; v) \) with \( v \equiv e \mod k(k-1) \);
2. an \( (k, m) \)-CDM;
3. a cyclic BIBD \( B(k, 1; me) \).

Then there exists a cyclic BIBD \( B(k, 1; mv) \).

Proof. Apply Theorem 2.6 with \( r = 1, u = e \), and \( K = \{k\} \).

Theorem 3.5 [11]. Let \( k \) be a prime power. Suppose that both a cyclic BIBD \( B(k, 1; v) \) and a cyclic BIBD \( B(k, 1; m) \) with \( m \equiv 1 \mod k(k-1) \) exist. Then a cyclic BIBD \( B(k, 1; mv) \) exists provided one of the following is satisfied:

1. \( v \equiv 1 \mod k(k-1) \);
2. \( v \equiv k \mod k(k-1) \) and a cyclic \( B(k, 1; mk) \) exists.

Proof. This is an immediate consequence of Theorem 3.4 and Lemma 2.2.

Theorem 3.6 [5]. Let \( m \) be a positive integer which is relatively prime to \( (k-1)! \). Suppose that a cyclic BIBD \( B(k, 1; v) \) exists. Then a cyclic BIBD \( B(k, 1; mv) \) exists provided one of the following is satisfied:

1. \( v \equiv 1 \mod k(k-1) \) and a cyclic \( B(k, 1; m) \) exists;
2. \( v \equiv k \mod k(k-1) \) and a cyclic \( B(k, 1; mk) \) exists.

Proof. This follows directly from Theorem 3.4 and Lemma 2.1.

So far we have touched upon some corollaries of Theorem 2.6. However, this is by no means an exhaustive coverage. In addition, the technique used in Theorem 2.6 can undoubtedly be carried over to construction of cyclic designs with index greater than one, as well as to cyclic tournament designs, mutatis mutandis.

As applications of Theorem 2.6, we now give infinite series of new CP\((k, 1; v)\)s in the remainder of this section. To do this we require a few preliminary results as ingredients.

Lemma 3.7 [3]. Let \( w \) be a positive integer whose prime factors are all greater than 5. Then there exists a 6-regular CP\((4, 1; 6w)\).

Lemma 3.8 [10]. Let \( p \) be a prime congruent to 1 modulo 4 and greater than 5. Then there exists a 5-regular CP\((5, 1; 5p)\).

Lemma 3.9 [18]. There exists a 4-SCGDD of type \( 6^4 \).
Lemma 3.10 [8]. Let \( w \) be a positive integer whose prime factors are all congruent to 1 modulo \( k \). Then there exists a \((w, k)\)-regular \( CP(k, 1; kw) \).

Lemma 3.11 [8]. Let \( p = nt + 1 \) be a prime where \( 2 \leq n \leq 7 \), \( t \geq n-1 \), and \( n \) and \( t \) are not both even. Then there exists a \((nt+1, n+2)\)-regular \( CP(n+1, 1; (nt+1)(n+2)) \).

Now we are in a position to establish the following two existence results by means of Theorem 2.6.

Theorem 3.12. Let \( w \) be a positive integer whose prime factors are all congruent to 1 modulo 6. Then there exists an optimal \( CP(4, 1; 36w) \), or equivalently an optimal \( (36w, 4, 1)\)-OOC.

Proof. Apply Theorem 2.6 to a \((w, 6)\)-regular \( CP(6, 1; 6w) \), in which \( m = 6, u = 1, k = 4 \) and \( K = \{6\} \). The ingredients required are all satisfied by Lemmas 3.7, 3.9 and 3.10, except for an optimal \( CP(4, 1; 36) \) which is obtained by taking following two base blocks:

\[
\{0, 1, 5, 8\}, \{0, 2, 11, 17\}. \]

Theorem 3.13. Let \( w \) be a positive integer whose prime factors are all congruent to 5 modulo 8 and greater than 5. Then there exists an optimal \( CP(5, 1; 30w) \), or equivalently an optimal \( (30w, 5, 1)\)-OOC.

Proof. Let \( p > 5 \) be an arbitrary prime congruent to 5 modulo 8. Start with a \((p, 6)\)-regular \( CP(5, 1; 6p) \) which exists by Lemma 3.11. Apply Theorem 2.6 with \( m = k = 5, u = 1 \) and \( K = \{5\} \) to obtain a 30-regular \( CP(5, 1; 30p) \). The ingredients required are all satisfied by Lemmas 2.1 and 3.8. We can then apply Theorem 2.6 inductively by taking \( m \) to be prime factors of \( w \) to obtain a 30-regular \( CP(5, 1; 30w) \), since a \((5, p)\)-CDM exists for any prime \( p \) by Lemma 2.1. The conclusion then follows from the existence of an optimal \( CP(5, 1; 30) \), which is obtained by simply taking base block \( \{0, 1, 4, 9, 11\} \).

4. CONCLUDING REMARKS

The determination of those parameters \( v \) and \( k \) for which an optimal \( CP(k, 1; v) \) exists is apparently a difficult combinatorial problem. It has been proved in [2, 4] that an optimal \( CP(3, 1; v) \) exists for all integers \( v \geq 3 \) except for \( v = 6t+2 \) with \( t \equiv 2 \) or \( 3 \mod 4 \). However, knowledge on
the case $k \geq 4$ is very limited so far. For a brief survey of known results, the reader is referred to [7, 18]. Theorems 3.12 and 3.13 provide two infinite series of new optimal cyclic packing designs. It is hoped that Theorem 2.6 in conjunction with Lemma 2.3 may be applied to produce more new optimal cyclic packings, which is currently under investigation. Further results concerning optimal CP($4, 1; v$)'s will be reported in subsequent papers.

ACKNOWLEDGMENT

The author thanks the referees for their helpful comments.

REFERENCES

1. I. C. M. Bird and A. D. Keedwell, Design and applications of optical orthogonal codes—
2. E. F. Brickell and V. K. Wei, Optical orthogonal codes and cyclic block designs, 
4. F. P. K. Chung, J. A. Salehi, and V. K. Wei, Optical orthogonal codes: Design, analysis, 
Sci. 2 (1980), 95–98.
6. C. J. Colbourn and J. H. Dinitz (Eds.), The CRC Handbook of Combinatorial 
7. C. J. Colbourn, J. H. Dinitz, and D. R. Stinson, Applications of combinatorial designs to 
communications, cryptography and networking, in “London Math. Soc. Lecture Note Ser.,” 
8. R. Fuji-Hara and Y. Miao, Optimal orthogonal codes: Their bounds and new optimal 
249–255.
12. S. V. Maric and V. K. N. Lau, Multirate fiber-optic CDMA: System design and performance 
13. S. V. Maric, O. Moreno, and C. Corrada, Multimedia transmission in fiber-optic LANs 
14. W. H. Mills and R. C. Mullin, Coverings and packings, in “Contemporary Design 
Theory: A Collection of Surveys” (J. H. Dinitz and D. R. Stinson, Eds.), pp. 371–399, 

