On Super-simple Cyclic 2-designs

Kejun Chen*

Department of Mathematics, Yancheng Teachers University
Jiangsu 224002, China

Ruizhong Wei†

Department of Computer Science, Lakehead University
Thunder Bay, ON, P7B 5E1 Canada

Email: kejunchen1@yahoo.com.cn, rwei@lakeheadu.ca

Abstract

In this paper, we investigate super-simple cyclic (v, k, λ)-BIBDs (SCBIBs). Some general constructions for SCBIBs are given. The spectrum of super-simple cyclic $(v, 3, \lambda)$ is completely determined for $\lambda = 2, 3$ and $v - 2$. From that some new optical orthogonal codes are obtained.

Keywords: super-simple cyclic designs, optical orthogonal codes, cyclic t-designs

1 Introduction

A (partial) t-(v, k, λ) design is a pair $(X, \mathcal{B})$ where X is a v-set (the *point* set), and C is a family of k-subsets of X (the family of *blocks*), such that any t-subset of X occurs in (at most) precisely λ blocks.

A *balanced incomplete block design* of block-size k, index λ ((v, k, λ)-BIBD in short) is a 2-(v, k, λ) design. A BIBD with $\lambda = 1$ is called a *Steiner 2-design.*

For a (v, k, λ)-BIBD, $(X, \mathcal{B})$, let σ be a permutation on X. For a block $B \in \mathcal{B}$, let $B^\sigma = \{y^\sigma : y \in B\}$. If $\mathcal{B}^\sigma = \{B^\sigma | B \in \mathcal{B}\} = \mathcal{B}$, then σ is called an *automorphism* of $(X, \mathcal{B})$. If there is an automorphism σ of order $v = |X|$, then the BIBD is said to be *cyclic*, denoted by (v, k, λ)-CBIB.

[*] Research supported by NSFC (NO. 11071207), Jiangsu Provincal NSF (No. BK2008198)

[†] Research supported by NSERC grant 239135-2011

For a (v, k, λ)-CBIB, the set of points X can be identified with Z_v, the residue group of integers modulo v. In this case, the design has an automorphism $\sigma : i \mapsto i+1 \pmod{v}$.

Let $B = \{b_1, \cdots, b_k\}$ be a block of a cyclic BIBD. The block orbit containing B is defined by the set of distinct blocks

$$B + i = \{b_1 + i, \cdots, b_k + i\} \pmod{v}$$

for $i \in Z_v$. If a block orbit has v blocks, then the block orbit is said to be *full*, otherwise *short*. We choose an arbitrary block from a block orbit and call it a *base block*. A base block is also referred to as a *starter* block or an *initial* block.

There is a very extensive literature on cyclic BIBDs with particular attention to cyclic Steiner 2-design [20] (see also [2, 4, 5, 10], etc).

A design is said to be *simple* if it contains no repeated blocks. A design is said to be *super-simple* if the intersection of any two blocks has at most two elements. The existence of super-simple designs have been investigated by many people (refer to [6, 7, 8, 24, 26, 27], etc). When $\lambda = 1$, any BIBD is necessarily super-simple. In this paper, when we talk about super-simple designs, we usually mean the case $\lambda > 1$.

Now we define super-simple cyclic designs. A design is called *super-simple cyclic* if it is both cyclic and super-simple. In the sequel, we will use the shorthand notation (v, k, λ)-SCBIB to denote a super-simple cyclic (v, k, λ)-BIBD with full orbits (without short ones).

It is easy to see the followings are the necessary conditions for the existence of a (v, k, λ)-SCBIB:

1. $v \geq (k-2)\lambda + 2$;
2. $\lambda(v-1) \equiv 0 \pmod{k(k-1)}$.

We now review the concept of an optical orthogonal code. An (v, k, ρ) optical orthogonal code (OOC) C is a family of $(0, 1)$ sequences of length v and weight k which satisfy the following two property (all subscripts are reduced modulo v):

1. The Autocorrelation Property:

$$\sum_{t=0}^{v-1} x_t x_{t+r} \leq \rho$$

for any $X = \{x_t\}_{t=0}^{v-1} \in C$ and every integer r, with $0 < r < v$.

2. The Cross-Correlation Property:

$$\sum_{t=0}^{v-1} x_t y_{t+r} \leq \rho$$

for any $X = \{x_t\}_{t=0}^{v-1} \in \mathcal{C}$, $Y = \{y_t\}_{t=0}^{v-1} \in \mathcal{C}$ with $X \neq Y$ and every integer r.

For a given set of values of v, k and ρ, the largest possible size of an (v, k, ρ)-OOC is denoted by $\Phi(v, k, \rho)$. An (v, k, ρ)-OOC $\mathcal{C}$ is called *optimal* if the number of codewords $|\mathcal{C}| = \Phi(v, k, \rho)$. The most general upper bound for $\Phi(v, k, \rho)$ in [16] is derived from the Johnson bound for constant-weight codes, which is as follows.

Theorem 1.1 *([28]) (Johnson bound)*

$$\Phi(v, k, \rho) \leq J(v, k, \rho),$$

where

$$J(v,k,\rho) = \left\lfloor \frac{1}{k} \left\lfloor \frac{v-1}{k-1} \left\lfloor \frac{v-2}{k-2} \left\lfloor \cdots \left\lfloor \frac{v-\rho}{k-\rho} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor \right\rfloor .$$

Since [16] was published, optical orthogonal codes have attracted a lot of attention in both the information theory area and the combinatorial design field. There are many infinite families of OOCs which have been constructed.

The close relationships between OOCs and cyclic t-designs have been investigated in [21]. The so-called cyclic difference packing or difference families is the main method used in the construction of $(v, k, 1)$ OOCs and fruitful results have been obtained from it.

Recently, some direct and recursive constructions for $(v, k, 2)$ OOCs were given by Chu et al in [13] and [14].

The following result can be found in [14].

Lemma 1.2 *Any t-$(v, k, 1)$ strictly cyclic partial design is equivalent to an $(v, k, t-1)$-OOC, where $t \geq 2$. On the other hand, any (v, k, ρ)-OOC is equivalent to a $(\rho + 1)$-$(v, k, 1)$ strictly cyclic partial design.*

It is well known that a $(v, k, 1)$-CBIB gives an optimal $(v, k, 1)$ optical orthogonal code. We shall show that a (v, k, λ)-SCBIB can be used to construct an $(v, k, 2)$-OOC. In particular, a (v, k, λ)-SCBIB with $\lambda = \left\lfloor \frac{v-2}{k-2} \right\rfloor$ gives an optimal $(v, k, 2)$-OOC.

In fact, a (v, k, λ)-SCBIB is a 3-$(v, k, 1)$ strictly cyclic partial design. So we have the following.

Theorem 1.3 *If there exists a (v, k, λ)-SCBIB, then there exists an $(v, k, 2)$-OOC with $\lambda(v-1)/(k(k-1))$ codewords. Furthermore, the resulted OOC is optimal when $\lambda = \left\lfloor \frac{v-2}{k-2} \right\rfloor$.*

Proof A (v, k, λ)-SCBIB may be viewed as a 3-$(v, k, 1)$ strictly cyclic partial design. By Lemma 1.2, an $(v, k, 2)$-OOC exists.

When $\lambda = \left\lfloor \frac{v-2}{k-2} \right\rfloor$, the number of base blocks is $\left\lfloor \frac{v-2}{k-2} \right\rfloor \frac{v-1}{k(k-1)}$, which approaches the Johnson bound of an $(v, k, 2)$-OOC. So the resulted $(v, k, 2)$-OOC is optimal. □

OOCs were first motivated by an application in a fiber optic code-division multiple access channel ([16]). Suppose there are b codewords in an OOC. Then a communication system using this OOC can handle up to b simultaneous transmitters with v optical chips. This is our main motivation of researching on super-simple cyclic designs. On the other hand, super-simple cyclic designs are also interesting objects in combinatorics. So we will investigated super-simple cyclic designs in general even for those not closely related to OOCs.

The main contributions of this paper are as follows. We investigate super-simple cyclic BIBDs and first consider constructing OOCs from them (cyclic designs have been used of OOCs previously). We give constructions of super-simple cyclic BIBDs for both recursive and direct methods. We have tried to use a uniformed method to summarize known recursive constructions. We give complete solutions for $(v, 3, \lambda)$-SCBIBs, where $\lambda = 2, 3$ and $v - 2$. Some infinite classes of $(v, 3, 4)$-SCBIBs and (v, k, λ)-SCBIBs for $4 \leq k \leq 6$ are also given. From the construction of SCBIBs we obtain some new classes of OOCs.

The rest of this paper is arranged as follows. Direct and recursive constructions for (v, k, λ)-SCBIBs will be described in Section 2.The existence of $(v, 3, \lambda)$-SCBIBs will be discussed in Section 3. For $k = 4, 5$ and $2 \leq \lambda \leq 4$ or $k = 6$ and $\lambda = 2$, the existence of a (v, k, λ)-SCBIBs with v a product of primes congruent to 1 modulo $k(k-1)$ will be shown in Section 4. Finally, new $(v, k, 2)$-OOCs obtained from SCBIBs will be summarized in Section 5.

2 Constructions for (v, k, λ)-SCBIBs

We first consider several constructions for general super-simple cyclic designs.

Let $k \geq 3$, for some small values v, the corresponding super-simple cyclic designs with admissible index $\lambda > 1$ can be found by a computer program. It is easy to see that a family $\mathcal{F}$ of k-subsets of Z_v forms the base blocks of a (v, k, λ)-CBIB with full orbits if and only if the list of differences $\Delta\mathcal{F} = \bigcup_{B \in \mathcal{F}} \Delta B$ is λ times $Z_v \setminus \{0\}$, where $B = \{b_1, b_2, \cdots, b_k\} \in \mathcal{F}$ and $\Delta B = \{b_j - b_i | \ 1 \leq i, j \leq k, i \neq j\}$ is the list of differences from B.

Let $\mathcal{F}$ be a family of k-subsets of Z_v forms the base blocks of a (v, k, λ)-CBIB with full orbits. Clearly $|\mathcal{F}| = \lambda(v-1)/(k(k-1))$. In order to check whether the cyclic design is super-simple, by definition, we form $k(k-1)(k-2)/6$ 3-subsets of each base block and develop them modulo v. Thus we get a list of $\lambda v(v-1)(k-2)/6$ triples. If these $\lambda v(v-1)(k-2)/6$ triples are pairwise distinct, then the design is super-simple. This criteria can be further reduced by the following.

Let $B \in \mathcal{F}$. For any 3-subset $S = \{s_1, s_2, s_3\} \subset B$, let ∇S be a list of the following three pairs

$$\{s_2 - s_1, s_3 - s_1\},\ \{s_1 - s_2, s_3 - s_2\},\ \{s_1 - s_3, s_2 - s_3\}.$$

Denote by

$$\nabla B = \{\nabla S | S = \{s_1, s_2, s_3\} \subset B\}$$

and

$$\nabla \mathcal{F} = \{\nabla B | B \in \mathcal{F}\}.$$

Chen and Wei have proved the following in [9].

Theorem 2.1 *Suppose that $\mathcal{F}$ is a family of k-subsets of Z_v which forms the base blocks of a (v, k, λ)-CBIB with full orbits. Then the cyclic design is super-simple if and only if all pairs listed in $\nabla\mathcal{F}$ are distinct, which is equivalent to the following conditions:*

(i) *for any $B \in \mathcal{F}$, any 3-subset $S \subset B$, the three pairs in ∇S are distinct;*

(ii) *for any $B \in \mathcal{F}$, any two 3-subsets S, S' of B, $S \neq S'$, ∇S and $\nabla S'$ have no common pairs, i.e., $\nabla S \cap \nabla S' = \emptyset$;*

(iii) *for any two base blocks $B, B' \in \mathcal{F}$, $B \neq B'$, ∇B and $\nabla B'$ have no common pairs, i.e., $\nabla B \cap \nabla B' = \emptyset$.*

By Theorem 2.1, to check whether a cyclic design obtained by developing a family $\mathcal{F}$ of $\lambda(v-1)/(k(k-1))$ base blocks over Z_v is super-simple, we need only to check $\lambda(v-1)(k-2)/2$ pairs in $\nabla\mathcal{F}$ to see whether they are pairwise distinct. It should be mentioned that the naive approach of generating a design and then checking for super-simplicity is hopeless with large values of v and λ.

It is readily found that many super-simple $(v, 4, \lambda)$-BIBDs with $\lambda = 2, 3, 4, 6$ and super-simple $(v, 5, \lambda)$-BIBDs with $\lambda = 2, 4, 5$, constructed in Z_v in [6, 7, 8, 26, 27], are cyclic. Bluskov and Heinrich [3] considered the existence of $(v, 4, \lambda)$-BIBDs for $v \leq 32$ with all admissible λ, most of which are also cyclic. [9] also showed the following.

Lemma 2.2 *([9]) There exists a $(v, 4, \lambda)$-SCBIB for all $7 \leq v \leq 41$ and all admissible λ with two exceptions $(v, \lambda) = (9, 3), (13, 5)$.*

Now we consider the recursive constructions for (v,k,λ)-SCBIBs. There are various recursive constructions for cyclic BIBDs. We will modify these methods to construct super-simple cyclic BIBDs. In this subsection, we use a uniformed method to describe these constructions. In our construction, we need the concept of difference matrix, which is defined as follows.

Let $(G,\cdot)$ be a finite group of order v. A (v,k,λ)-*difference matrix* over G is a $k \times v\lambda$ matrix $D = (d_{ij})$ with entries from G, such that for each $1 \le i < j \le k$, the multi-set

$$\{d_{il} \cdot d_{jl}^{-1} : 1 \le l \le v\lambda\}$$

contains every element of G exactly λ times. When G is an Abelian group, typically an additive notation is used, so that the differences $d_{il} - d_{jl}$ are employed. In what follows, we assume that $G = Z_v$. We usually denote a (v,k,λ)-difference matrix over Z_v by (v,k,λ)-DM. Difference matrices have been investigated extensively, see, for example, [18] and the references therein. Here is one example.

Lemma 2.3 ([18]) *Let v and k be positive integers such that* $\gcd(v,(k-1)!) = 1$. *Let* $d_{ij} = ij \pmod{v}$ *for* $i = 0,1,\cdots,k-1$ *and* $j = 0,1,\cdots,v-1$. *Then $D = (d_{ij})$ is a $(v,k,1)$-DM over Z_v. In particular, if v is an odd prime number, then there exists a $(v,k,1)$-DM over Z_v for any integer k, $2 \le k \le v$.*

We give our construction for super-simple cyclic BIBDs in the following.

Theorem 2.4 *(Product Construction) Suppose u, v, k and λ are positive integers. If the following conditions hold:*

(1) there exists (v,k,λ)-SCBIB,

(2) there exists a $(u,k,1)$-DM over Z_u,

(3) there exists a (u,k,λ)-SCBIB,

then there exists a (uv,k,λ)-SCBIB.

Proof Suppose that M_1 and M_2 are the set of all base blocks of a (v,k,λ)-SCBIB and a (u,k,λ)-SCBIB, respectively. Let $D = (d_{ij})$ be a $(u,k,1)$-DM over Z_u. For each $B = \{b_1, b_2, \cdots, b_k\} \in M_1$, define

$$B_j = \{b_i + d_{ij}v |\ i = 1,2,\cdots,k\}, j = 1,2,\cdots,u.$$

For each $B = \{b_1, b_2, \cdots, b_k\} \in M_2$, define

$$vB = \{vb_i |\ i = 1,2,\cdots,k\}.$$

Denote

$$\mathcal{F}_1 = \bigcup_{B \in M_1} \{B_j | j = 1,2,\cdots,u\}$$

and

$$\mathcal{F}_2 = \{vB | B \in M_2\}.$$

Then, it is easy to check that $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$ is a set of all base blocks of a (uv, k, λ)-CBIB.

Next, we shall show that the resulted (uv, k, λ)-CBIB is super-simple. By Theorem 2.1, we need only to prove that the conditions (i)-(iii) mentioned in Theorem 2.1 are satisfied.

Suppose that $C \in \mathcal{F}$, T is a 3-subset of C. If $C \in \mathcal{F}_1$, then there exists a block $B = \{b_1, b_2, \cdots, b_k\} \in M_1$ and an integer j such that $C = B_j$. In this case we can write $T = \{b_{i_1} + d_{i_1 j}v, b_{i_2} + d_{i_2 j}v, b_{i_3} + d_{i_3 j}v\}$. It is easy to see that ∇T is the same as ∇S modulo v, where $S = \{b_{i_1}, b_{i_2}, b_{i_3}\}$ is a 3-subset of B. By Theorem 2.1, the three pairs in ∇S are distinct modulo v, so the three pairs in ∇T are also distinct modulo uv.

If $C \in \mathcal{F}_2$, then there exists a block $B = \{b_1, b_2, \cdots, b_k\} \in M_2$ such that $C = vB$. In this case we can write $T = \{vb_{i_1}, vb_{i_2}, vb_{i_3}\}$. It is easy to see that $\nabla T = v\nabla S$, where $S = \{b_{i_1}, b_{i_2}, b_{i_3}\}$ is a 3-subset of B. By Theorem 2.1, the three pairs in ∇S are distinct under modulo u, so the three pairs in ∇T are also distinct under modulo uv. Thus, condition (i) holds.

In a similar way, one can prove that condition (ii) holds.

Now we check condition (iii). Suppose that $C, C' \in \mathcal{F}$ with $C \neq C'$. If $C \in \mathcal{F}_1$, $C' \in \mathcal{F}_2$, then it is easy to see that $\nabla C \cap \nabla C' = \emptyset$ since any pair listed in $\nabla C'$ is $(0,0)$ under modulo v and no pair in ∇C has this property.

If $C, C' \in \mathcal{F}_1$, then there exist B and B' in M_1 and there exist integers j, j' such that $C = B_j, C' = B'_{j'}$. Let T be a 3-subset of C and T' be 3-subset of C'. If $B \neq B'$, then $\nabla B \cap \nabla B' = \emptyset$ by Theorem 2.1. Note that ∇C and $\nabla C'$ are the same as ∇B and $\nabla B'$ modulo v, respectively. So we have $\nabla C \cap \nabla C' = \emptyset$. If $B = B'$ then we must have $j \neq j'$. Suppose that $T = \{b_{i_1} + d_{i_1 j}v, b_{i_2} + d_{i_2 j}v, b_{i_3} + d_{i_3 j}v\}$, $T' = \{b'_{l_1} + d_{l_1 j'}v, b'_{l_2} + d_{l_2 j'}v, b'_{l_3} + d_{l_3 j'}v\}$. Denote by $S = \{b_{i_1}, b_{i_2}, b_{i_3}\}$, $S' = \{b'_{l_1}, b'_{l_2}, b'_{l_3}\}$. If $S \neq S'$ then $\nabla S \cap \nabla S' = \emptyset$ from Theorem 2.1. Noting that ∇T and $\nabla T'$ are the same as ∇S and $\nabla S'$ under modulo v, respectively. So we have $\nabla T \cap \nabla T' = \emptyset$. If $S = S'$ then we also have $\nabla T \cap \nabla T' = \emptyset$ noting that $d_{ij} - d_{sj} \neq d_{ij'} - d_{sj'}$ when $i \neq s$, $j \neq j'$. Consequently, $\nabla C \cap \nabla C' = \emptyset$.

If $C, C' \in \mathcal{F}_2$, then there exist $B, B' \in M_2$ such that $C = vB, C' = vB'$, where $B \neq B'$. Clearly, $\nabla C = v\nabla B$, $\nabla C' = v\nabla B'$. Since $\nabla B \cap \nabla B' = \emptyset$, we have $\nabla C \cap \nabla C' = \emptyset$. □

It is clear to see that Theorem 2.4 can be used iteratively to construct new SCBIBs if the conditions (1)-(3) hold in each step. We give an example to illustrate this in the following.

Example 2.5 *There exists a* $(17^m \cdot 19^n, 4, 6)$*-SCBIB for all positive integers* m *and* n*.*

Proof Let $\mathcal{F}_1 = \{\{0, 2^i, 2^i \cdot 3, 2^i \cdot 11\} \pmod{17} |\ i = 0, 1, \cdots, 7\}$ and $\mathcal{F}_2 = \{\{0, 2^i, 2^i \cdot 3, 2^i \cdot 4\} \pmod{19} |\ i = 0, 1, \cdots, 8\}$. It is readily checked by Theorem 2.1 that $\mathcal{F}_1$ and $\mathcal{F}_2$ are the set of base blocks of a $(17, 4, 6)$-SCBIB and a $(19, 4, 6)$-SCBIB respectively. Since there exist a $(17, 4, 1)$-DM over Z_{17} and a $(19, 4, 1)$-DM over Z_{19} by Lemma 2.3, a $(17 \cdot 19, 4, 6)$-SCBIB follows from Theorem 2.4. By induction on integers m and n, a $(17^m \cdot 19^n, 4, 6)$-SCBIB is obtained. □

We will generalize the above construction for super-simple cyclic BIBDs. Before proceeding, we define the notion of a group divisible design (GDD).

A GDD with index λ is a triple $(X, \mathcal{G}, \mathcal{B})$ which satisfies the following properties:

(1) $\mathcal{G}$ is a partition of a set X (of points) into subsets called groups,

(2) $\mathcal{B}$ is a set of subsets of X (called blocks), each of cardinality at least two, such that a group and a block contain at most one common point, and

(3) every pair of points from distinct groups occurs in exactly λ blocks.

We denote $(X, \mathcal{G}, \mathcal{B})$ as (v, K, g, λ)-GD if $|X| = v$, $|G| = g$ for every $G \in \mathcal{G}$ and $|B| \in K$ for every $B \in \mathcal{B}$, where K is a set of positive integers. If $K = \{k\}$ we simply write k for K. It is easy to see that a (v, k, λ)-BIBD is just a $(v, k, 1, \lambda)$-GD.

Group divisible designs have been instrumental in the construction of various combinatorial configurations. A GDD $(X, \mathcal{G}, \mathcal{B})$ is said to be *cyclic* if there exists an automorphism σ of X such that $G^\sigma = \{\sigma(a) |\ a \in G\} \in \mathcal{G}$ for any $G \in \mathcal{G}$ and $B^\sigma = \{\sigma(b) |\ b \in B\} \in \mathcal{B}$ for any $B \in \mathcal{B}$. Full and short orbits can be defined as previous. We use the notation (v, K, g, λ)-CGD to denote a cyclic GDD without short orbits. In this case, we can identify X with Z_v and G with the set of cosets of subgroup $H = \{0, w, 2w, \cdots, (g-1)w\}$, where $w = v/g$.

A GDD is called *super-simple* if any two blocks have at most two common elements. If a (v, K, g, λ)-CGD is also super-simple, we call it *super-simple cyclic* and denote it by (v, K, g, λ)-SCGD.

Suppose that $\mathcal{F}$ is the set of base blocks of a cyclic GDD. It is easy to see that this cyclic GDD is super-simple if and only if the conditions (i)-(iii) mentioned in Theorem 2.1 are satisfied. We have the following.

Lemma 2.6 *If there exist a (v, k, g, λ)-SCGD and a (g, k, λ)-SCBIB, then there exists a (v, k, λ)-SCBIB.*

Proof By hypothesis, let $\mathcal{F}_1$ and $\mathcal{F}_2$ be the sets of all base blocks of a (v, k, g, λ)-SCGD and a (g, k, λ)-SCBIB, respectively. Denote $w = v/g$. For any $B \in \mathcal{F}_2$, we construct a new base block wB as follows:

$$wB = \{wb \pmod{v} |\ b \in B\}.$$

Let $w\mathcal{F}_2 = \{wB |\ B \in \mathcal{F}_2\}$. By using Theorem 2.1, one can easily check that $\mathcal{E} = \mathcal{F}_1 \cup (w\mathcal{F}_2)$ is the required family of base blocks. □

Theorem 2.7 *If the following conditions hold:*
(1) *there exists a* (v,k,g,λ)*-SCGD,*
(2) *there exists a* $(u,k,1)$*-DM over* Z_u*,*
then there exists a (uv,k,ug,λ)*-SCGD. Furthermore, if*
(3) *there exists a* (ug,k,λ)*-SCBIB,*
then there exists a (uv,k,λ)*-SCBIB.*

Proof By Lemma 2.6 we need only to construct a (uv,k,ug,λ)-SCGD. By the assumptions (1) and (2), let $\mathcal{F}$ be the family of starter blocks of a (v,k,g,λ)-SCGD and $D=(d_{ij})$ be a $(u,k,1)$-DM over Z_u. For any base block $B=\{b_1,b_2,\cdots,b_k\}$ of $\mathcal{F}$, we construct a family $\mathcal{D}(B)=\{B_j|\ j=1,2,\cdots,u\}$, where

$$B_j=\{b_i+d_{ij}v \pmod{uv}|\ i=1,2,\cdots,k\},\ j=1,2,\cdots,u.$$

Let $\mathcal{E}=\bigcup_{B\in\mathcal{F}}\mathcal{D}(B)$. Then $\mathcal{E}$ is the desired family of base blocks of a (uv,k,ug,λ)-SCGD. The detailed verification is similar to that in the proof of Theorem 2.4, we omit it here. □

We give an example to illustrate the above constructions in the following.

Example 2.8 *There exist a* $(5^n\cdot 17,4,5^{n-1}\cdot 17,6)$*-SCGD and a* $(5^n\cdot 17,4,6)$*-SCBIB for all integer* $n\geq 1$*.*

Proof We first construct a $(5\cdot 17,4,17,6)$-SCGD, whose base blocks are listed bellow:

$3^i\{0,1,27,54\}$, $3^i\{0,7,9,63\}$, $3^i\{0,7,39,71\}$, $0\leq i\leq 7$,
$\{0,23,29,36\}$, $\{0,4,21,47\}$, $\{0,17,61,78\}$, $\{0,51,59,77\}$,
$\{0,22,34,73\}$, $\{0,51,72,79\}$, $\{0,51,67,69\}$, $\{0,49,66,83\}$,
$\{0,23,69,71\}$, $\{0,6,37,54\}$.

A $(17,4,6)$-SCBIB was shown in the proof of Example 2.5. By Lemma 2.6, a $(5\cdot 17,4,6)$-SCBIB is obtained.

On the other hand, there exists a $(5,4,1)$-DM over Z_5 from Lemma 2.3. Start from a $(5\cdot 17,4,17,6)$-SCGD and apply Theorem 2.7, a $(5^2\cdot 17,4,5\cdot 17,6)$-SCGD is obtained. Consequently, there exists a $(5^2\cdot 17,4,6)$-SCBIB. By induction on n, we obtain a $(5^n\cdot 17,4,5^{n-1}\cdot 17,6)$-SCGD and a $(5^n\cdot 17,4,6)$-SCBIB. □

As mentioned above, when $g=1$, a (v,k,g,λ)-SCGD is just a (v,k,λ)-SCBIB. So Theorem 2.7 can be consider as a generalization of Theorem 2.4.

We shall give a more generalized construction for super-simple cyclic BIBDs. To do this, we introduce the notion of a generalized difference matrix, which will be used in our generalized construction, just as a DM used in previous construction.

Let u, k, λ and h be positive integers such that $k \le h$ and $\lambda uh(h-1) \equiv 0 \pmod{k(k-1)}$. Let $n = \frac{\lambda uh(h-1)}{k(k-1)}$. A (h, u, k, λ)- *generalized difference matrix* D over $Z_u \cup \{x\}$ ((h, u, k, λ)-GDM in short) is a $h \times n$ matrix $D = (d_{ij})$ with entries from $Z_u \cup \{x\}$ satisfying the following two conditions:

(1) each column of D contains exactly k elements of Z_u. In other words, x appears exactly $h - k$ times in each column,

(2) for any $1 \le i < j \le h$, the multiset $\Delta_{ij} = \{d_{is} - d_{js} |\ d_{is}, d_{js} \in Z_u, 1 \le s \le n\}$ contains every element of Z_u exactly λ times.

From the above definition one can see that when $k = h$, a (h, u, k, λ)-GDM is just a (u, k, λ)-DM. To illustrate the above definition, we give the following two examples.

Example 2.9 *A* $(5, 3, 4, 1)$*-GDM over* $Z_3 \cup \{x\}$ *is shown as follows*

$$\begin{array}{ccccc}
x & 1 & 0 & 0 & 1 \\
1 & x & 1 & 0 & 0 \\
0 & 1 & x & 1 & 0 \\
0 & 0 & 1 & x & 1 \\
1 & 0 & 0 & 1 & x
\end{array}$$

Example 2.10 *A* $(6, 6, 4, 1)$*-GDM over* $Z_6 \cup \{x\}$ *is listed below.*

$$\begin{array}{ccccccccccccccc}
x & x & x & x & x & 0 & 2 & 3 & 0 & 0 & 0 & 0 & 5 & 0 & 1 \\
x & 2 & 0 & 0 & 1 & x & x & x & x & 0 & 2 & 1 & 4 & 3 & 5 \\
1 & x & 3 & 0 & 5 & x & 0 & 0 & 0 & x & x & x & 0 & 2 & 0 \\
5 & 0 & x & 2 & 4 & 1 & x & 1 & 3 & x & 2 & 0 & x & x & 0 \\
0 & 0 & 0 & x & 0 & 5 & 0 & x & 2 & 1 & x & 3 & x & 0 & x \\
0 & 2 & 1 & 2 & x & 4 & 3 & 0 & x & 5 & 0 & x & 1 & x & x
\end{array}$$

It is easy to show that a generalized difference matrix can be used to form a group divisible design. Specifically, we have the following.

Lemma 2.11 *If there exists a* (h, u, k, λ)*-GDM, then there exists a* (hu, k, u, λ)*-GD.*

Proof Let $D = (d_{ij})$ be a given (h, u, k, λ)-GDM over $Z_u \cup \{x\}$ and let $n = \frac{\lambda uh(h-1)}{k(k-1)}$. Denote $I_h = \{1, 2, \cdots, h\}$. Let $X = I_h \times Z_u$ and $\mathcal{G} = \{G_i | G_i = \{i\} \times Z_u, i \in I_h\}$. Take $\mathcal{F} = \{B_j | j = 1, 2, \cdots, n\}$, where B_js are defined as follows:

$$B_j = \{(i, d_{ij}) | d_{ij} \in Z_v, i \in I_h\},\ j = 1, 2, \cdots, n,$$

Denote

$$B_j + s = \{(i, d_{ij} + s) | d_{ij} \in Z_v, i \in I_h\}, s \in Z_u,$$

where the addition is taken under modulo u.

Let

$$\mathcal{B} = \{B_j + s | B_j \in \mathcal{F}, s \in Z_u\}.$$

It is readily checked that $(X, \mathcal{G}, \mathcal{B}\}$ is a (hu, k, u, λ)-GD. □

Examples 2.9 and 2.10 are modified from [30].

Now we describe our generalized construction for super-simple cyclic BIBDs.

Theorem 2.12 *If the following conditions hold:*

(1) *there exists a* (v, K, g, λ)-*SCGD,*

(2) *there exists a* $(h, u, k, 1)$-*GDM over* $Z_u \cup \{x\}$ *for each* $h \in K$,

then there exists a (uv, k, ug, λ)-*SCGD. Furthermore, if*

(3) *there exists a* (ug, k, λ)-*SCBIB,*

then there exists a (uv, k, λ)-*SCBIB.*

Proof By Lemma 2.6 we need only to construct a (uv, k, ug, λ)-SCGD. According to the assumption (1), let $\mathcal{F}_1$ be the family of starter blocks of a (v, K, g, λ)-SCGD. Let $B = \{b_1, b_2, \cdots, b_h\}$ be a starter block of $\mathcal{F}_1$. By hypothesis, we have a $(n, h, k, 1)$-GDM, $D = (d_{ij})$, over $Z_u \cup \{x\}$. Let $n = \frac{\lambda uh(h-1)}{k(k-1)}$. Denote $\mathcal{D}(B) = \{B_1, B_2, \cdots, B_n\}$, where

$$B_j = \{b_i + d_{ij}v \pmod{uv} | \ b_i \in B, d_{ij} \in Z_u, i \in I_n\}, \ 1 \le j \le n.$$

As B ranges over $\mathcal{F}_1$, we obtain a family $\mathcal{E}_1 = \bigcup_{B \in \mathcal{F}} \mathcal{D}(B)$ of starter blocks.

We claim that $\mathcal{E}_1$ is the set of base blocks of a (uv, k, ug, λ)-SCGD. Let $H = \{0, w, 2w, \cdots, (ug-1)w\}$, where $w = v/g$. It is readily checked that every integer of $Z_{uv} \backslash H$ appears exactly λ times as a difference in $\Delta\mathcal{E}_1$. This is straightforward since every nonzero integer b of $Z_{uv} \setminus H$ can be written as $b = sv + r$ with $0 \le s \le u-1$ and $1 \le r \le v-1$ (i.e., $b \equiv r \pmod{v}$). As for super-simplicity, using a similar way shown in the proof of Theorem 2.4, one can prove that the conditions (i)-(iii) mentioned in Theorem 2.1 are satisfied. □

We give an example to illustrate the above construction.

Example 2.13 *There exists a* $(195, 4, 6)$-*SCBIB.*

Proof We can write $195 = 3 \cdot 5 \cdot 13$. Let $K = \{5\}$, $v = 65$, $g = 5$ and $\lambda = 6$. We first construct a $(5 \cdot 13, 5, 5, 6)$-SCGD. Take $\mathcal{F} = \{2^i\{0, 1, 2, 5, 7\}, 2^i\{0, 1, 10, 15, 22\}, 2^i\{0, 5, 22, 34, 43\} | \ 0 \le i \le 5\}$. It is readily checked that $\mathcal{F}$ is a set of base blocks of a $(65, 5, 5, 6)$-SCGD.

Let $h = 5$, $u = 3$ and $k = 4$. A $(5,3,4,1)$-GDM over $Z_3 \cup \{x\}$ was shown in Example 2.9. By Theorem 2.12, we obtain a $(195,4,15,6)$-SCGD.

To construct a $(195,4,6)$-SCBIB, by Lemma 2.6 or Theorem 2.12, we need only to construct a $(15,4,6)$-SCBIB over Z_{15}. The desired base blocks are listed bellow.

$2^i\{0,1,2,6\}$, $0 \le i \le 3$, $\{0,1,4,10\}$, $\{0,1,9,13\}$, $\{0,2,5,8\}$. □

3 $(v,3,\lambda)$-SCBIBs

Clearly, a $(v,3,\lambda)$-SCBIB is just a simple $(v,3,\lambda)$-CBIB. It is easy to see that the following is the necessary condition of a $(v,3,\lambda)$-SCBIB:

$$\lambda(v-1) \equiv 0 \pmod 6,\ v \ge \lambda + 2.$$

The existence of $(v,3,\lambda)$-CBIBs has been determined by Colbourn and Colbourn in [17]. It should be mentioned that the cyclic designs constructed in [17] may contain repeated blocks. However, some of them can be modified to be a simple cyclic design. In this section, we concentrate our attention to the existence of $(v,3,\lambda)$-SCBIBs. By modifying the construction for Mendelsohn triple system given by Hoffman and Linder in [25] and the constructions for cyclic triple systems given by Colbourn and Colbourn in [17], we determine the spectrum of $(v,3,\lambda)$-SCBIBs with $\lambda = 2,3$ and $v-2$. For $\lambda = 4$, some partial results are also provided.

3.1 The case: $\lambda = 2$

When $\lambda = 2$, the necessary condition of a $(v,3,\lambda)$-SCBIB becomes $v \equiv 1 \pmod 3$ and $v \ge 4$.

It was shown in [17] that there does not exist any $(v,3,2)$-CBIB for $v \equiv 10 \pmod{12}$. Thus we have the following.

Lemma 3.1 *There is no $(v,3,2)$-SCBIB for any $v \equiv 10 \pmod{12}$.*

So we need only to consider the case $v \equiv 1,4,7 \pmod{12}$. When $v \equiv 1,7 \pmod{12}$ (i.e., $v \equiv 1 \pmod 6$), we have the following result.

Lemma 3.2 *There exists a $(v,3,2)$-SCBIB for any $v \equiv 1,7 \pmod{12}$ (i.e., $\equiv 1 \pmod 6$)) and $v \ge 7$.*

Proof Suppose $v = 6t+1$ and $t \ge 1$. Let

$$B_i = \{0, i, t+2i\},\ 1 \le i \le t,$$

$$B_{t+i} = \{0, t+2i-1, 2t+i\}\ 1 \le i \le t.$$

It is readily checked that $B_1, B_2, \cdots, B_{2t}$ are the desired base blocks. □

When $v \equiv 4 \pmod{12}$, we have the following result.

Lemma 3.3 *There exists a $(v,3,2)$-SCBIB for any $v \equiv 4 \pmod{12}$ and $v \geq 4$.*

Proof Suppose $v = 12t+4$ and $t \geq 0$. Let

$B_i = \{0, 2i, 3t+i+1\}$, $B_{t+i} = \{0, 3t-i+1, 3t+i+1\}$, $1 \leq i \leq t$,

$B_{2t+i} = \{0, 2t-2i+1, 6t-i+2\}$, $B_{3t+i} = \{0, 4t+i+1, 6t-i+2\}$, $1 \leq i \leq t$,

$B_{4t+1} = \{0, 3t+1, 6t+2\}$.

It is readily checked that $B_1, B_2, \cdots, B_{4t+1}$ are the required base blocks.

□

3.2 The case: $\lambda = 3$

When $\lambda = 3$, the necessary condition of a $(v,3,\lambda)$-SCBIB becomes $v \equiv 1 \pmod{2}$ and $v \geq 5$. We can show that this condition is also sufficient. The proof is obtained by modifying the construction for cyclic triple systems given by Colbourn and Colbourn in [17].

Theorem 3.4 *There exists a $(v,3,3)$-SCBIB if and only if $v \equiv 1 \pmod{2}$ and $v \geq 5$.*

Proof Let $v = 2t+1$, $t \geq 2$. When $v \not\equiv 0 \pmod{3}$, let

$$B_i = \{0, i, 2i\},\ 1 \leq i \leq t.$$

For $v \equiv 0 \pmod{3}$, let

$$B_i = \{0, i, 2i\},\ 1 \leq i \leq t,\ i \neq \frac{t-1}{3}, \frac{2t+1}{3}, t,$$

$$B_{\frac{t-1}{3}} = \{0, \frac{t-1}{3}, t\},$$

$$B_{\frac{2t+1}{3}} = \{0, \frac{2t+1}{3}, t\},$$

$$B_t = \{0, 1, \frac{2t+1}{3}\}.$$

It is readily checked that $B_1, B_2, \cdots, B_t$ are the required base blocks.

□

3.3 The case: $\lambda = 4$

When $\lambda = 4$, the necessary condition of a $(v, 3, \lambda)$-SCBIB becomes $v \equiv 1 \pmod 3$ and $v \geq 7$. For $v \equiv 1 \pmod 6$ or $v \equiv 10 \pmod{12}$, we shall give the construction of $(v, 3, 4)$-SCBIBs in the following.

Lemma 3.5 *There exists a $(v, 3, 4)$-SCBIB for any $v \equiv 1 \pmod 6$.*

Proof There is a $(v, 3, 1)$-CBIB from [18]. Let $\mathcal{B}$ be the base blocks of such a design. Let $\mathcal{A} = \{\{0, i, 2i\} | i = 1, \ldots, v-1\}$. Then $\mathcal{A} \cup \mathcal{B}$ forms a $(v, 3, 4)$-SCBIB. □

Lemma 3.6 *There exists a $(v, 3, 4)$-SCBIB for any $v \equiv 10 \pmod{12}$.*

Proof Let $v = 12t + 10$, $t \geq 0$. The required base blocks are listed below (which are modified from a construction of [19] .

$B_i = \{0, 2i-1, 3t+i+3\}$, $\quad B_{t+i} = \{0, 2i, 5t+i+5\}, 1 \leq i \leq t$,
$B_{2t+i} = \{0, 2i-1, 3t+i+2\}$, $\quad B_{3t+i} = \{0, 2i, 5t+i+4\}, 1 \leq i \leq t$,
$B_{4t+i} = \{0, 2i, 3t+i+1\}$, $\quad B_{5t+i} = \{0, 2i-1, 5t+i+5\}$,
$1 \leq i \leq t$,
$B_{6t+i} = \{0, 2i, 3t+i+2\}$, $\quad B_{7t+i} = \{0, 2i-1, 5t+i+3\}$,
$1 \leq i \leq t$,
$B_{8t+1} = \{0, 2t+1, 4t+3\}$, $\quad B_{8t+2} = \{0, 2t+1, 4t+4\}$,
$B_{8t+3} = \{0, 2t+1, 6t+4\}$, $\quad B_{8t+4} = \{0, 2t+2, 5t+4\}$,
$B_{8t+5} = \{0, 3t+1, 7t+5\}$, $\quad B_{8t+6} = \{0, 4t+2, 8t+5\}$. □

3.4 The case: $\lambda = v - 2$

When $\lambda = v-2$, the necessary condition of a $(v, 3, \lambda)$-SCBIB becomes $v \not\equiv 0 \pmod 3$, and $v \geq 5$. We shall show that this condition is also sufficient. Specifically, we have the following.

Theorem 3.7 *There exists a $(v, 3, v-2)$-SCBIB if and only if $v \not\equiv 0 \pmod 3$ and $v \geq 4$.*

Proof We need only to prove the sufficiency. Let $\mathcal{B}$ be the set of all 3-subsets of Z_v. Clearly, $|\mathcal{B}| = v(v-1)(v-2)/6$. We shall show that $(Z_v, \mathcal{B})$ is the required $(v, 3, v-2)$-SCBIB. For any $B \in \mathcal{B}$, let *dev* $B = \{B_i | 0 \leq i \leq v-1\}$, where $B_i = \{b + i \pmod v | \, b \in B\}$, $0 \leq i \leq v-1$. Note that $v \not\equiv 0 \pmod 3$, it is not difficult to check that for any $i \neq j$, we have $B_i \neq B_j$, and for any $B' \in \mathcal{B} \setminus$ *dev* B, we have *dev* $B \cap$ *dev* $B' = \emptyset$. From this, $\mathcal{B}$ can be divided into $(v-1)(v-2)/6$ parallel classes. Choose one block from each parallel class, we get $(v-1)(v-2)/6$ blocks, which are the desired base blocks. □

4 (v, k, λ)-SCBIBs with $4 \leq k \leq 6$

In this section, we consider the existence of (v, k, λ)-SCBIBs, mostly for integers v such that any of its prime factor is congruent to 1 modulo $k(k-1)$, where $k = 4, 5$ and $2 \leq \lambda \leq 4$ or $k = 6$ and $\lambda = 2$. Some of them are constructed from known $(v, k, 1)$-CBIBs.

The following result was proved by Gronau et al in [27].

Lemma 4.1 *Suppose that $\mathcal{B} = \{B_1, \cdots, B_s\}$ is the set of base blocks of a $(v, k, 1)$-CBIB design. Then $\mathcal{B} \cup (-\mathcal{B})$ is the set of base blocks of a $(v, k, 2)$-SCBIB.*

It has been known that there exists a $(q, k, 1)$-CBIB with $q \equiv 1 \pmod{k (k-1)}$ a prime number and $k = 4, 5, 6$ except when $q = 61$ and $k = 6$ (see [11] and [12]).

Let $\mathcal{F} = \{11^i\{0, 1, 2, 4, 7, 25\}, 11^i\{0, 4, 14, 27, 34, 46\} | i = 0, 1\}$. It is easy to check that $\mathcal{F}$ is a set of base blocks of a $(61, 6, 2)$-SCBIB.

So we have the following theorem.

Theorem 4.2 *Let $p \equiv 1 \pmod{k(k-1)}$ be a prime number. Then there exists a $(p, k, 2)$-SCBIB for $k = 4, 5$ and 6.*

The following is obvious.

Lemma 4.3 *Suppose that $\mathcal{B} = \{B_1, \cdots, B_s\}$ is the set of base blocks of a $(v, k, 1)$-CBIB. If there exists a subset M of Z_v such that for any $a, b \in M$, $a \neq b$, $a\mathcal{B} \cup b\mathcal{B}$ generates a $(v, k, 2)$-SCBIB. Then there is a (v, k, λ)-SCBIB with $2 \leq \lambda \leq |M|$.*

Proof For each λ, $2 \leq \lambda \leq |M|$, let M_1 be a subset of size λ of M. Denote by

$$\mathcal{T} = \bigcup_{a \in M_1} a\mathcal{B}.$$

Clearly, $\mathcal{T}$ is the set of base blocks of a (v, k, λ)-CBIB. We shall show that the cyclic design is also super-simple. In fact, for any two elements $a, b \in M_1$, by hypothesis, $a\mathcal{B} \cup b\mathcal{B}$ generates a $(v, k, 2)$-SCBIB. By Theorem 2.1 all pairs listed in $\nabla a\mathcal{B} \cup \nabla b\mathcal{B}$ are distinct. Consequently, all pairs listed in $\nabla \mathcal{T} = \bigcup_{a \in M_1} \nabla a\mathcal{B}$ are also distinct. By Theorem 2.1 we get our conclusion.

□

Now, we focus our attention to the existence of (q, k, λ)-SCBIB with q a prime number and $k = 4, 5$, where $2 \leq \lambda \leq 4$. We shall show that such a SCBIB always exists.

Let $q = ef + 1$ be a prime power and ω be a primitive element of $GF(q)$. Denote by H^e the unique subgroup of order f of the cyclic multiplicative group $GF(q) \setminus \{0\}$, i.e., $H^e = \{\omega^{ei} : i = 0, 1, \cdots, f-1\}$. The cosets H_0^e, H_1^e, $\cdots$, H_{e-1}^e are defined by

$$H_i^e = \omega^i H^e, \ i = 0, 1, \cdots, e-1.$$

For $k = 4, 5$, let $q \equiv 1 \pmod{k(k-1)}$ be a prime number. For a k-subset $B = \{b_1, b_2, \cdots, b_k\}$ of Z_q, we set $\Delta^+ B = \{b^j - b^i : 1 \le i < j \le k\}$. Chen and Zhu [11] showed that for any prime number $q \equiv 1 \pmod{k(k-1)}$, there exists an element $x \in Z_q$ such that $B = \{0, 1, x, \cdots, x^{k-2}\}$ and $\Delta^+ B$ is a system of representatives for the cosets of H^e with $e = \frac{k(k-1)}{2}$. Consequently, $\mathcal{B} = \{sB : s \in S\}$ is the set of base blocks of a $(q, k, 1)$-CBIB, where S is a system of the representatives for the cosets of the factor group $H^e/\{1, -1\}$ so that $H^e = S \circ \{1, -1\}$ (see the proof of Theorem 2 in [29]).

Clearly, for any $c \in Z_q \setminus \{0\}$, $c\mathcal{B}$ is also the set base blocks of a $(q, k, 1)$-CBIB. By Lemma 4.1 $c\mathcal{B} \cup (-c\mathcal{B}) = \{csB : s \in H_0^e\}$ is the set of base blocks of a $(q, k, 2)$-SCBIB. We wish to find an element $c \in Z_q$ so that $\mathcal{B} \cup (c\mathcal{B})$ and $-\mathcal{B} \cup (c\mathcal{B})$ can both generate a $(q, k, 2)$-SCBIB. Consequently, $\mathcal{B} \cup (-\mathcal{B}) \cup (c\mathcal{B})$ generates a $(q, k, 3)$-SCBIB and $\mathcal{B} \cup (-\mathcal{B}) \cup (c\mathcal{B}) \cup (-c\mathcal{B})$ generates a $(q, k, 4)$-SCBIB. These hold if and only if c satisfies the following condition:

(i) $\nabla(\mathcal{B} \cup (-\mathcal{B})) \cap \nabla(c\mathcal{B} \cup (-c\mathcal{B})) = \emptyset$.

Note that $\nabla\mathcal{B} \cup \nabla(-\mathcal{B}) = \{s\nabla B : s \in H_0^e\}$, $\nabla c\mathcal{B} \cup \nabla(-c\mathcal{B}) = c\{s\nabla B : s \in H_0^e\}$. Condition (i) is equivalent to the condition $(cs\nabla B) \cap (s'\nabla B) = \emptyset$ for any $s, s' \in H_0^e$, i.e.,

(ii) $(cs\nabla B) \cap \nabla B = \emptyset$ for any $s \in H_0^e$.

We shall show that such an element c always exists in Z_q.

When $k = 4$, we have $B = \{0, 1, x, x^2\}$ and $\nabla B = \{\{1, x\}, \{-1, x-1\}, \{-x, 1-x\}, \{1, x^2\}, \{-1, x^2-1\}, \{-x^2, 1-x^2\}, \{x, x^2\}, \{-x, x^2-x\}, \{-x^2, x-x^2\}, \{x-1, x^2-1\}, \{1-x, x^2-x\}, \{1-x^2, x-x^2\}\}$.

Note that $e = 6$ and $\Delta^+ B = \{1, x, x^2, x-1, x(x-1), (x+1)(x-1)\}$ is a system of representatives for the cosets of H^6. Since $1 \in H_0^6$, we may assume that $x \in H_i^6$, $x-1 \in H_j^6$, $x+1 \in H_m^6$, where $i, j, m \ne 0$ are distinct. Without loss of generality, we may further assume that $\{i, 2i, j, i+j, m+j\} = \{1, 2, 3, 4, 5\} \pmod 6$. So we have $i \ne 0, 3$, $j \ne 0, \pm i, 2i \pmod 6$ and $m \ne 0, i, i-j, 2i-j \pmod 6$.

Let $c \in H_3^6$. Suppose $x \in H_i^6$, $i \ne 0, 3$, then $cs \in H_3^6$ and $csx \in H_{3+i}^6$ for any $s \in H_0^6$. Note that $-1 \in H_0^6$, it is easy to see that $cs \ne \pm 1, \pm x, \pm x^2$ and $csx \ne \pm 1, \pm x, \pm x^2$, which implies that for $c \in H_3^6$, $cs\{1, x\} \not\in \{\{1, x\}, \{-1, x-1\}, \{-x, 1-x\}, \{1, x^2\}, \{-1, x^2-1\}, \{-x^2, 1-x^2\}, \{x, x^2\}, \{-x, x^2-x\}, \{-x^2, x-x^2\}\}$.

If $cs = x-1$, then $csx = x(x-1) \neq x^2-1$; if $cs = x^2-1$ and $csx = x-1$, then we have $x(x+1) = 1$, thus $cs = -x \in H^6_{6-i}$, which implies $i = 3$, a contradiction. So we have $cs\{1, x\} \neq \{x-1, x^2-1\}$.

If $cs = 1-x$, then $csx = -x(x-1) \neq x^2 - x$; if $cs = x^2 - x$, then $csx = x(x^2-x) = x^2(x-1) \neq 1-x$ since $x^2 \neq -1$. So we have $cs\{1, x\} \neq \{1-x, x^2-x\}$.

If $cs = 1-x^2$, then $csx = x(1-x^2) \neq x - x^2$ since $x \neq \pm 1$; if $cs = x - x^2$ and $csx = 1 - x^2$, then we have $x^2 = x+1$, which implies $cs = -1$, a contradiction. So we have $cs\{1, x\} \neq \{1-x^2, x-x^2\}$.

From above, we have shown that $cs\{1, x\} \notin \nabla B$. In a similar way, one can check that any other element in $cs\nabla B$ does not belong to ∇B. Thus condition (ii) holds.

When $k = 5$, we have $e = 10$, $B = \{0, 1, x, x^2, x^3\}$ and $\nabla B = \bigcup_{\{a,b,c\} \subset B} \{\{b - a, c - a\}, \{a - b, c - b\}, \{a - c, b - c\}\}$.

Since $\Delta^+ B = \{1, x, x^2, x^3, x-1, x(x-1), x^2(x-1), x^2-1, x(x^2-1), x^3-1\}$ is a system of the representatives for the cosets of H^{10}, without loss of generality, we may assume that $x \in H_i^{10}$, $x-1 \in H_j^{10}$, $x+1 \in H_m^{10}$ and $x^2+x+1 \in H_l^{10}$ such that $\{i, 2i, 3i, j, i+j, 2i+j, j+m, i+j+m, j+l\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \pmod{10}$. So we have $i \neq 0, 5$, $j \neq 0, \pm i, \pm 2i, 3i \pmod{10}$, $m \neq 0, \pm i, \pm j, 2i, i-j, 2i-j, 3i-j \pmod{10}$ and $l \neq 0, i, j, 2i, m, i+m, i-j, 2i-j, 3i-j \pmod{10}$.

Let $c \in H_5^{10}$. With a similar way as above one can check that condition (ii) holds. So we have the following.

Theorem 4.4 *Suppose $k = 4, 5$. Then for any prime number $q \equiv 1 \pmod{k(k-1)}$, there exists a (q, k, λ)-SCBIB with $\lambda = 2, 3, 4$.*

For $k = 4, 5, 6$, by Lemma 2.3 there exists a $(q, k, 1)$-DM over Z_q with any prime number $q \equiv 1 \pmod{k(k-1)}$. Combining Theorem 4.2 and Theorem 4.4 with Theorem 2.4, we have the following.

Corollary 4.5 *Suppose $k = 4, 5$ and $\lambda = 2, 3, 4$. There exists a (v, k, λ)-SCBIB for each integer v of which all prime factors congruent to 1 modulo $k(k-1)$.*

Corollary 4.6 *There exists a $(v, 6, 2)$-SCBIB for each integer v of which all prime factors are congruent to 1 modulo* 30.

5 Applications to OOCs

We summarize the new resulting OOCs obtained from SCBIBs constructed in the previous sections as follows.

Theorem 5.1 *There exists an optimal* $(v, 3, 2)$*-OOC for each* $v \not\equiv 0 \pmod 3$ *and* $v \geq 4$.

Proof Combining Theorem 3.7 with Theorem 1.3. □

Remark: For a given value of v, the above construction gives an OOC with $\frac{(v-1)(v-2)}{6}$ codewords which is the largest number of codewords for all known OOCs. To obtain more codewords, we need either to choose a larger ρ or to choose a smaller k. To improve above result, one need to consider $(v, 4, 3)$-OOC because we always have $\rho \leq k - 1$.

Theorem 5.2 *For* $k = 4, 5$*, there exists an* $(v, k, 2)$*-OOC with* $\frac{4(v-1)}{k(k-1)}$ *codewords, where* v *is a product of primes congruent to 1 modulo* $k(k-1)$.

Proof Combining Corollary 4.5 with Theorem 1.3. □

Remark: The OOCs in the above theorem has more codewords than those OOCs constructed in [21, 22, 23, 30]. Although a $(v, 3, 2)$-OOC has more codewords than a $(v, 4, 2)$-OOC in general, a $(v, 4, 2)$-OOC has the advantage that the difference between k and ρ is larger. This property will benefit to applications by reducing possible errors.

Theorem 5.3 *There exists an* $(v, 6, 2)$*-OOC with* $\frac{v-1}{15}$ *codewords, where* v *is a product of primes congruent to 1 modulo* 30.

Proof Combining Corollary 4.6 with Theorem 1.3. □

In [14], by using so-called r-simple matrices, several recursive constructions were given.

Let G be an Abelian group of size v. Let r be a positive integer. An $s \times t$ matrix $A = (a_{ij})$ over G is called *r-simple*, if the difference of any two column vectors of A contains any element in G at most $r - 1$ times. Modifying some constructions for OOCs in [14], we have the following.

Theorem 5.4 *Suppose there exists a* (v, k, λ)*-SCBIB. If there exists an* $k \times N$ r*-simple matrix over* Z_g*, then there exists an* $(ng, k, 2)$*-OOC with* NT *codewords, where* $T = \frac{\lambda(v-1)}{k(k-1)}$.

Proof By Theorem 1.3 there exists a $(v, k, 2)$-OOC with T codewords. The conclusion followed from Theorem 4 in [14]. □

In particular, we have the following.

Theorem 5.5 *Suppose there exists a* (v, k, λ)*-SCBIB. Let* $u = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ *be a positive integer, where* p_i*,* $1 \leq i \leq t$*, are primes not less than* k*. Then there exists an* $(uv, k, 2)$*-OOC with* Tu^2 *codewords, where* $T = \frac{\lambda(v-1)}{k(k-1)}$.

Proof The conclusion followed from Theorem 1.3 and Corollary 3 in [14]. □

Combining Theorem 5.5 with Corollary 4.5 and Corollary 4.6 respectively, we have the following.

Corollary 5.6 *Suppose $k = 4, 5$. Let v be a product of primes all congruent to 1 modulo $k(k-1)$. Then for any odd integer u of which all prime factors are not less then k, there exists an $(uq, k, 2)$-OOC with $\frac{4(v-1)u^2}{k(k-1)}$ codewords.*

Corollary 5.7 *Let v be a product of primes congruent to 1 modulo 30. Then for any odd integer u of which all prime factors are not less then 6, there exists an $(uq, 6, 2)$-OOC with $\frac{(v-1)u^2}{15}$ codewords.*

It is easy to see that a 3-$(v, k, 1)$ strictly cyclic design is just a $(v, k, \frac{v-2}{k-2})$-SCBIB. On the other hand, when $\lambda = \frac{v-2}{k-2}$, a (v, k, λ)-SCBIB is also a 3-$(v, k, 1)$ strictly cyclic design. So we have the following.

Theorem 5.8 *There exists a 3-$(v, k, 1)$ strictly cyclic design if and only if there exists a super-simple $(v, k, \frac{v-2}{k-2})$ cyclic design.*

Acknowledgment

The authors thank a referee who gives very detailed comments on a previous version of this paper, which helped us to correct many typos and errors.

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, FL., 1996, pp. 270-287.

[2] I. Anderson, Some cyclic and 1-rotational designs, In J. W. P. Hirschfeld (Ed.) Surveys in Combinatorics 2001, Cambridge University Press, 2001, pp. 47-73.

[3] I. Bluskov and K. Heinrich, Super-simple designs with $v \leq 32$, J. Statist. Plann. Inference 95 (2001), 121-131.

[4] M. Buratti, Cyclic designs with block size 4 and related optimal optical orthogonal codes, Des. Codes Cryptogr. 26 (2002), 111-125.

[5] Y. Chang, Some cyclic BIBDs with block size four, J. Combin. Designs 12 (2004), 177-183.

[6] K. Chen, On the existence of super-simple $(v, 4, 3)$-BIBDs, J. Combin. Math. Combin. Comput. 17 (1995), 149-159.

[7] K. Chen, On the existence of super-simple $(v, 4, 4)$-BIBDs, J. Statist. Plann. Inference 51 (1996), 339-350.

[8] K. Chen, Z. Cao and R. Wei, Super-simple balanced incomplete block designs with block size 4 and index 6, J. Statist. Plann. Inference, 133 (2005), 537-554.

[9] K. Chen and R. Wei, Super-simple cyclic designs with small values, J. Statist. Plann. Inference, 137(2007), 2034-2044.

[10] K. Chen and R. Wei, A few more cyclic Steiner 2-designs, Electron. J. Combin. 13(2006),♯R10

[11] 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.

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

[13] W. Chu and C. J. Colbourn, Optimal $(v, 4, 2)$-OOC of small orders, Discrete Math. 279 (2004), 163-172.

[14] W. Chu and C. J. Colbourn, Recusive constructions for optimal $(v, 4, 2)$-OOCs, J. Combin. Des. 12 (2004), 333-345.

[15] W. Chu and S. W. Colomb, A new recursive constructions for optical orthogonal codes, IEEE Trans. Inform. Theory 49 (2003), 3072-3076.

[16] F. R. K. Chung, J. A. Salehi and V. K. Wei, Optical orthogonal codes: Design, analysis and applications, IEEE Trans. Inform. Theory 35 (1989), 595-604.

[17] M. J. Colbourn and C. J. Colbourn, Cyclic block designs with block size 3, European J. Combin. 2 (1981), 21-26.

[18] 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, FL., 1996, pp. 287-297.

[19] C.J. Colbourn and A. Rosa, Triple Systems, Oxford-Clarendon Press, 1999.

[20] M. J. Colbourn and R. A. Mathon, On cyclic 2-designs, Ann Discrete Math. 7 (1980), 215-253.

[21] R. Fuji-Hara and Y. Miao, Optimal orthogonal codes: Their bounds and new optimal constructions, IEEE Trans. Inform. Theory 46 (2000), 2396-2406.

[22] R. Fuji-Hara, Y. Miao and J. Yin, Optimal $(9v, 4, 1)$ optical orthogonal codes, SIAM J. Discrete Math. 14 (2001), 256-266.

[23] G. Ge and J. Yin, Constructions for optimal $(v, 4, 1)$ optical orthogonal codes, IEEE Tran. Inform. Theory, 47(2001), 2998-3004.

[24] S. Hartmann, Superpure digraph designs, J. Combin. Des. 10 (2000), 239-255.

[25] D. G. Hoffman and C. C. Linder, Embeddings of Mendelsohn triple systems, Ars Combin. 11 (1981), 265-269.

[26] H.-D. O. F. Gronau and R. C. Mullin, On super-simple $2-(v, 4, \lambda)$ designs, J. Combin. Math. Combin. Comput. 11 (1992), 113-121.

[27] H.-D. O. F. Gronau, D. L. Kreher and A. C. H. Ling, Super-simple $(v, 5, 2)$-designs, Discrete Appl. Math. 138 (2004), 65-77.

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

[29] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory 4 (1972), 17-47.

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