A few more cyclic Steiner 2-designs *

Kejun Chen† and Ruizhong Wei

Department of Computer Science, Lakehead University

Thunder Bay, ON, P7B 5E1 Canada

Email: kchen3@lakeheadu.ca, wei@ccc.cs.lakeheadu.ca

Submitted: Mar 31, 2005; Accepted: Jan 23, 2006; Published: Feb 1, 2006
Mathematics Subject Classifications: 05B05

Abstract

In this paper, we prove the existence of a cyclic $(v, 4, 1)$-BIBD for $v = 12t + 4$, $3 \leq t \leq 50$ using computer programs, which are useful in recursive constructions for cyclic designs. Applications of these designs to optical orthogonal codes are also mentioned.

Keywords: cyclic BIBD; difference matrix; optimal optical orthogonal code

1 Introduction

A *group divisible design* of block-size k, index λ and group type g^v ((k, λ))-GDD of type g^v in short) is a triple $(X, \mathcal{G}, \mathcal{B})$, where X is a set of vg points, $\mathcal{G}$ is a partition of X into groups of size g, and $\mathcal{B}$ is a collection of k-subsets of X (*blocks*) with the property that each block meets each group in at most one point and any two points from two distinct groups are contained in exactly λ blocks. A (k, λ)-GDD with group type 1^v is called a *balanced incomplete block design*, denoted by (v, k, λ)-BIBD. A BIBD with $\lambda = 1$ is called a *Steiner 2-design*.

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

*Research supported by NSERC grant 239135-01

†Present address: Department of Mathematics, Yancheng Teachers College, Jiangsu, 224002, China. Research is also supported by NSF of Jiangsu Education Department.

For a (k,λ)-CGDD or a (v,k,λ)-CBIBD, 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 Steiner 2-design. 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 orbits is said to be *full*, otherwise *short*. An arbitrary block from a block orbit is called a *base block*. A base block is also referred to as a *starter* block or an *initial* block. The block orbit which contains the following block is called a *regular short orbit*

$$\left\{0, \frac{v}{k}, \frac{2v}{k}, \cdots, \frac{(k-1)v}{k}\right\}.$$

It is readily to show that a block orbit of a $(v,k,1)$-CBIBD must be a full or a regular short orbit. In this case, it can be shown that a necessary condition for the existence of a $(v,k,1)$-CBIBD is that

$$v \equiv 1, k \pmod{k(k-1)}.$$

A $(v,k,1)$-CBIBD with $v \equiv 1 \pmod{k(k-1)}$ has no short orbit, while a $(v,k,1)$-CBIBD with $v \equiv k \pmod{k(k-1)}$ has a single regular short orbit as well as full orbits. It is easy to see that the existence of a $(v,k,1)$-CBIBD with $v \equiv k \pmod{k(k-1)}$ is equivalent to the existence of a $(k,1)$-CGDD of type $k^{v/k}$.

To construct a CGDD or a CBIBD, we just need to find out all the base blocks.

There is a very extensive literature on cyclic BIBDs with particular attention to cyclic Steiner 2-design [18] (see also [3]). In general, given k and λ, to establish the spectrum of value of v for which there exists a (v,k,λ)-CBIBD is a very difficult problem. It has been solved for $k=3$ and $\lambda=1$ by Peltesohn [24] and for $k=3$ and $\lambda>1$ by Colbourn and Colbourn [19]. The case $(k,\lambda)=(4,1)$ has been treated in many papers. Constructions for $(v,4,1)$-CBIBDs can be found, for instance, in [1, 2, 4, 6, 9, 10, 11, 13, 14, 21, 25]. It is reasonable to believe that a $(v,4,1)$-CBIBD exists for any admissible $v \geq 37$, but the problem is far from settled. We summarized the known results on $(v,4,1)$-CBIBD as follows.

Theorem 1.1 (1) ([6, 14]) *There exists a* $(v,4,1)$*-CBIBD for any prime* $p \equiv 1 \pmod{12}$*;*

(2) ([19, 6, 7, 14]) *There exist a* $(v,4,1)$*-CBIBD and a* $(4v,4,1)$*-CBIBD, where* v *is a product of primes congruent to 1 modulo 12;*

(3) ([10]) *There exists a* $(4u,4,1)$*-CBIBD for any positive integer* u *such that any prime factor* p *of* u *satisfies the conditions* $p \equiv 1 \pmod 6$ *and* $\gcd((p-1)/6, 20!) \neq 1$*;*

(4) ([11]) *There exists a* $(4^n u,4,1)$*-CBIBD, where* $n \geq 3$ *is a positive integer and* u *is a product of primes congruent to 1 modulo 6, or* $n=2$ *and* u *is a product of primes congruent to 1 modulo 6 such that* $\gcd(u, 7\times 13\times 19) \neq 1$*;*

(5) ([1, 2]) *There exists a* $(12t+1,4,1)$*-CBIBD for* $t \leq 50$ *with one exception of* $t=2$*; There exists a* $(12t+4,4,1)$*-CBIBD for* $t \in T_2 = \{3,4,5,6\}$ *and there is no* $(12t+4,4,1)$*-CBIBD for* $t = 1, 2$.

Constructions of designs fall into two categories, direct and recursive. The existence of a $(v,k,1)$-CBIBD for small value v plays an important role in the recursive constructions for new cyclic BIBDs. However, many $(v,k,1)$-CBIBDs for small values v can not be obtained from known recursive constructions. It is desired to get them by direct constructions. In this paper, we continue to investigate the existence of $(v,4,1)$-CBIBDs. For some small values v, we mainly use direct constructions to give the base blocks of $(v,4,1)$-BIBDs, which are believed to be useful in the recursive constructions for larger cyclic BIBDs.

Specifically, we shall prove the following theorem.

Theorem 1.2 *There exists a $(12t+4,4,1)$-CBIBD for $3 \le t \le 50$. There is no $(12t+4,4,4)$-CBIBD for $t = 1,2$.*

In section 2, some known recursive constructions for cyclic BIBDs will be described. The proofs of Theorem 1.2 will be given in Section 3. Some infinite classes of cyclic BIBDs are provided in Section 4, and are translated into optimal optical orthogonal codes in Section 5.

2 Recursive Constructions

In this section, we display some known recursive constructions for CBIBD which will be used in Sections 4.

Colbourn and Colbourn [19] showed the following constructions for cyclic BIBDs.

Lemma 2.1 (Productive Construction, [19]) *Assume that u is an integer which is relative prime to $(k-1)!$.*

(i) *If there exists a $(v,k,1)$-CBIBD with no short orbit (i.e., $v \equiv 1 \pmod{k(k-1)}$) and a $(u,k,1)$-CBIBD, then there exists a $(uv,k,1)$-CBIBD.*

(ii) *If there exists a $(kv,k,1)$-CBIBD and a $(ku,k,1)$-CBIBD, then there exists a $(kuv,k,1)$-CBIBD.*

This construction was generalized by Jimbo and Kuriki [22] and Jimbo [23] utilizing the notation of difference matrix. A similar construction was also given by Yin [26].

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 multiset

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

contains every element of G exactly λ times. When G is abelian, 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, [17] and the references therein. Here is one example.

Lemma 2.2 ([17]) *Let v and k be positive integers such that* $\gcd(v,(k-1)!) = 1$. *Let* $d_{ij} \equiv ij \pmod v$ *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, $2 \le k \le v$.

The following construction for cyclic designs can be found in Yin [26].

Lemma 2.3 (i) *If there exists a* $(k, 1)$*-CGDD of group type* g^v *with no short orbit and a* $(u, k, 1)$*-DM over* Z_u, *then there exists a* $(k, 1)$*-CGDD of group type* $(ug)^v$.

(ii) *If there exist a* $(k, 1)$*-CGDD of group type* g^v *and* $(g, k, 1)$*-CBIBD, then there exists a* $(gv, k, 1)$*-CBIBD.*

Buratti [7] showed the following construction.

Lemma 2.4 *Let v and k be integers such that* $p \equiv 1 \pmod k$ *holds for each prime p in v. If there exists a* $(v, k, 1)$*-CBIBD, then there exists a* $(kv, k, 1)$*-CBIBD.*

3 Proof of Theorem 1.2

In this section, we deal with the existence of $(12t + 4, 4, 1)$-CBIBDs for $t \in [7, 50]$. Some of them are obtained by recursive constructions stated in Section 2. Others are obtained using computer algorithms which will be stated below.

First we use recursive constructions.

Lemma 3.1 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for* $t = 28, 48$.

Proof. For $t = 28, 48$, we have $12t + 4 = 4p_1p_2$, where $p_1 = 5$, $p_2 = 17$ or 29. Clearly, primes p_1 and p_2 are both congruent to 1 modulo 4. From Theorem 1.1 (5) a $(4p_1p_2, 4, 1)$-CBIBD is obtained by Lemma 2.4. ∎

Lemma 3.2 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in T = \{10, 12, 14, 20, 22, 24, 26, 32, 34, 36, 42, 50\}$.

Proof. For each $t \in T$, we have $12t + 4 = 4u$, where $u = 3t + 1$ is a prime $\equiv 1 \pmod 6$ or a product of two primes $\equiv 1 \pmod 6$. The parameters are listed below.

$t = 10, u = 31$; $t = 12, u = 37$; $t = 14, u = 43$; $t = 20, u = 61$;
$t = 22, u = 67$; $t = 24, u = 73$; $t = 26, u = 79$; $t = 32, u = 97$;
$t = 34, u = 103$; $t = 36, u = 109$; $t = 42, u = 127$; $t = 50, u = 151$.

By Theorem 1.1 (3) we obtain the desired $(4u, 4, 1)$-CBIBDs. ∎

Lemma 3.3 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in \{9, 17, 25, 37, 43\}$.

Proof. For $t = 9, 17, 25$, we have $12t + 4 = 4^2u$, where $u = 7, 13, 19$. The corresponding CBIBDs are provided in Theorem 1.1 (4).

For $t = 37$, we have $12t + 4 = 4^3 \cdot 7$. By Theorem 1.1 (4) there exists a $(4^3 \cdot 7, 4, 1)$-CBIBD.

For $t = 43$, we have $12t + 4 = 4 \cdot 10 \cdot 13$. There exist a $(4 \cdot 10, 4, 1)$-CBIBD and a $(4 \cdot 13, 4, 1)$-CBIBD from Theorem 1.1 (5). By Lemma 2.1 (ii) we obtain a $(4 \cdot 10 \cdot 13, 4, 1)$-CBIBD since $\gcd(13, 6) = 1$. ∎

Next we consider direct constructions. The results of the following lemmas are obtained by a computer. In computer searching, a method we used in computer program is applying multipliers of blocks. Since our constructions are over Z_v, we can use both the addition and the multiplication of Z_v. We say that $w \in Z_v^*$ is a *multiplier* of the design, if for each base block $B = \{x_1, x_2, x_3, x_4\}$, there exists some $g \in Z_v$ such that $C = w \cdot B + g = \{w \cdot x_1 + g, w \cdot x_2 + g, w \cdot x_3 + g, w \cdot x_4 + g\}$ is also a base block. We say that $w \in Z_v^*$ is a *partial multiplier* of the design, if for each base block $B \in \mathcal{M}$, where $\mathcal{M}$ is a subset of all the base blocks, there exists some $g \in Z_v$ such that $C = w \cdot B + g$ is also a base block.

In the computer program, we first choose a (partial) multiplier w. Our experiences tell us that choosing a w which has long orbits in the multiplication group of Z_v usually gives better results. Then we start to find base blocks in the following way. When a base block B is found, the algorithm requires that $wB, w^2B, \cdots, w^sB$ can also be different base blocks, where s is a positive number. If we can find all the base blocks in this way, then $w^i, 1 \leq i \leq s$ are multipliers of the design. Otherwise, these are partial multipliers, and the algorithm tries to find the remaining base blocks. To decide the value of s is also important for the success of the algorithm. In practice, we usually let s be as large as possible at the beginning. Then the value of s is reduced if the search time is too long.

In most case, a "shuffling and backtracking" algorithm is also used. This program consists of two parts. One part is a standard backtracking algorithm used to find base blocks. The other part is a shuffling algorithm which shuffles the blocks already found. So this is not an exhaustive search. A start point is set for the shuffling algorithm. For example, if there are 15 base blocks need to be found, then we may set the start point at 5. That means the shuffling algorithm will be called after 5 base blocks have been found. A simple shuffling algorithm just exchanges two blocks. However, we will set the frequency of the calling shuffling algorithm. In our experience, to choose the start point and the appropriate frequency is important for the success of the search.

Lemma 3.4 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in \{8,\ 40\}$.

Proof Apart from the base block $\{0, 3t + 1, 6t + 2, 9t + 3\}$ with the regular short orbit, we list the multipliers for these designs and part of the base blocks so that other base blocks can be obtained by these blocks and the multipliers, in the follows.

For $t = 8$, the multipliers are $7^i, i = 0, 1$ and base blocks are:
$\{0, 1, 3, 9\}$, $\{0, 4, 20, 59\}$, $\{0, 5, 31, 53\}$, $\{0, 11, 30, 62\}$.

For $t = 40$, the multipliers are 9^i, $0 \le i \le 4$ and base blocks are:
$\{0, 1, 3, 8\}$, $\{0, 4, 14, 25\}$, $\{0, 13, 28, 44\}$, $\{0, 17, 37, 66\}$, $\{0, 19, 58, 92\}$,
$\{0, 26, 59, 129\}$, $\{0, 32, 118, 254\}$, $\{0, 35, 183, 283\}$. □

In what follows, we list the partial multipliers and their related base blocks, denoted as D blocks (blocks to be developed), which are multiplied by each of the partial multipliers. The remaining base blocks are listed as R blocks. Here, the base block with the regular short orbit is written in Italic.

Lemma 3.5 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in \{7,\ 11,\ 13,\ 15,\ 16\}$.

Proof. For $t = 7$, the partial multipliers are: 3^i, $0 \le i \le 2$.
D block is: $\{0, 1, 5, 18\}$.
R blocks are:
$\{0, 2, 21, 32\}$, $\{0, 6, 31, 41\}$, $\{0, 7, 27, 55\}$, $\{0, 8, 24, 50\}$, $\{\mathit{0,\ 22,\ 44,\ 66}\}$.

For $t = 11$, the partial multipliers are: 3^i, $0 \le i \le 4$.
D block is: $\{0, 1, 7, 29\}$.
R blocks are:
$\{0, 5, 41, 24\}$, $\{0, 2, 12, 71\}$, $\{0, 8, 56, 98\}$, $\{0, 4, 105, 89\}$, $\{0, 15, 40, 79\}$,
$\{0, 13, 43, 104\}$, $\{\mathit{0,\ 34,\ 68,\ 102}\}$.

For $t = 13$, the partial multipliers are: 3^i, $0 \le i \le 2$.
D blocks are: $\{0, 1, 5, 11\}$, $\{0, 7, 29, 56\}$
R blocks are:
$\{0, 19, 67, 110\}$, $\{0, 14, 46, 71\}$, $\{0, 16, 78, 125\}$, $\{0, 17, 37, 105\}$, $\{0, 23, 108, 64\}$,
$\{0, 2, 60, 134\}$, $\{0, 31, 65, 107\}$, $\{\mathit{0,\ 40,\ 80,\ 120}\}$.

For $t = 15$, the partial multipliers are: 3^i, $0 \le i \le 3$.
D blocks are: $\{0, 1, 5, 11\}$, $\{0, 8, 25, 81\}$.
R blocks are:
$\{0, 13, 100, 114\}$, $\{0, 23, 150, 62\}$, $\{0, 26, 106, 68\}$, $\{0, 2, 69, 134\}$, $\{0, 29, 89, 147\}$,
$\{0, 19, 47, 129\}$, $\{0, 20, 63, 140\}$, $\{\mathit{0,\ 46,\ 92,\ 138}\}$.

For $t = 16$, the partial multipliers are: 3^i, $0 \le i \le 7$.
D blocks are: $\{0, 1, 5, 38\}$.
R blocks are:
$\{0, 16, 116, 136\}$, $\{0, 10, 144, 21\}$, $\{0, 18, 53, 122\}$, $\{0, 14, 166, 48\}$, $\{0, 7, 91, 63\}$,
$\{0, 23, 65, 129\}$, $\{0, 6, 83, 109\}$, $\{0, 32, 86, 126\}$, $\{\mathit{0,\ 49,\ 98,\ 147}\}$. □

Lemma 3.6 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in \{18,\ 19,\ 21,\ 23\}$.

Proof. For $t = 18$, the partial multipliers are: 3^i, $0 \le i \le 4$.
D blocks are: $\{0, 1, 5, 18\}$, $\{0, 7, 50, 114\}$.
R blocks are:

$\{0, 14, 102, 79\}$, $\{0, 20, 80, 148\}$, $\{0, 8, 52, 123\}$, $\{0, 22, 48, 143\}$, $\{0, 16, 94, 180\}$,
$\{0, 25, 186, 66\}$, $\{0, 33, 75, 144\}$, $\{0, 11, 49, 73\}$, $\{$*0, 55, 110, 165*$\}$.

For $t = 19$, the partial multipliers are: 3^i, $0 \leq i \leq 11$.
D block is: $\{0, 1, 5, 54\}$.
R blocks are:
$\{0, 2, 184, 78\}$, $\{0, 18, 208, 64\}$, $\{0, 8, 79, 95\}$, $\{0, 14, 206, 96\}$, $\{0, 19, 51, 171\}$,
$\{0, 6, 176, 104\}$, $\{0, 29, 86, 138\}$, $\{$*0, 58, 116, 174*$\}$.

For $t = 21$, the partial multipliers are: 3^i, $0 \leq i \leq 12$.
D block is: $\{0, 1, 7, 43\}$.
R blocks are:
$\{0, 12, 96, 121\}$, $\{0, 8, 80, 32\}$, $\{0, 19, 56, 168\}$, $\{0, 16, 65, 179\}$, $\{0, 2, 113, 199\}$,
$\{0, 4, 73, 177\}$, $\{0, 14, 185, 225\}$, $\{0, 23, 61, 181\}$, $\{$*0, 64, 128, 192*$\}$.

For $t = 23$, the partial multipliers are: 3^i, $0 \leq i \leq 3$.
D blocks are: $\{0, 1, 5, 18\}$, $\{0, 7, 23, 49\}$, $\{0, 8, 37, 75\}$.
R blocks are:
$\{0, 40, 120, 170\}$, $\{0, 20, 76, 168\}$, $\{0, 2, 97, 180\}$, $\{0, 6, 131, 47\}$, $\{0, 22, 107, 82\}$,
$\{0, 32, 246, 137\}$, $\{0, 10, 103, 184\}$, $\{0, 31, 221, 99\}$, $\{0, 11, 157, 44\}$, $\{0, 35, 124, 176\}$,
$\{0, 28, 86, 116\}$, $\{$*0, 70, 140, 210*$\}$. □

Lemma 3.7 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in \{27, 29, 30, 31, 33\}$.

Proof. For $t = 27$, the partial multipliers are: 5^i, $0 \leq i \leq 7$.
D blocks are: $\{0, 1, 3, 7\}$, $\{0, 8, 17, 166\}$.
R blocks are:
$\{0, 48, 108, 255\}$, $\{0, 12, 139, 208\}$, $\{0, 33, 302, 112\}$, $\{0, 21, 165, 67\}$, $\{0, 34, 195, 77\}$,
$\{0, 13, 52, 143\}$, $\{0, 41, 277, 64\}$, $\{0, 28, 116, 252\}$, $\{0, 56, 152, 215\}$, $\{0, 57, 123, 188\}$,
$\{0, 24, 68, 105\}$, $\{$*0, 82, 164, 246*$\}$.

For $t = 29$, the partial multipliers are: 3^i, $0 \leq i \leq 7$.
D blocks are: $\{0, 1, 5, 11\}$, $\{0, 7, 24, 67\}$.
R blocks are:
$\{0, 22, 291, 66\}$, $\{0, 13, 170, 128\}$, $\{0, 39, 194, 235\}$, $\{0, 20, 181, 58\}$, $\{0, 2, 112, 238\}$,
$\{0, 62, 131, 222\}$, $\{0, 14, 220, 79\}$, $\{0, 32, 145, 265\}$, $\{0, 26, 144, 96\}$, $\{0, 64, 142, 213\}$,
$\{0, 16, 138, 185\}$, $\{0, 8, 266, 186\}$, $\{0, 29, 103, 257\}$, $\{$*0, 88, 176, 264*$\}$.

For $t = 30$, the partial multipliers are: 11^i, $0 \leq i \leq 8$.
D blocks are: $\{0, 1, 5, 22\}$, $\{0, 8, 58, 263\}$.
R blocks are:
$\{0, 13, 126, 340\}$, $\{0, 32, 265, 89\}$, $\{0, 3, 42, 301\}$, $\{0, 51, 195, 299\}$, $\{0, 2, 296, 196\}$,
$\{0, 26, 82, 143\}$, $\{0, 14, 98, 227\}$, $\{0, 12, 60, 312\}$, $\{0, 16, 234, 94\}$, $\{0, 15, 43, 171\}$,
$\{0, 6, 180, 160\}$, $\{0, 33, 165, 200\}$, $\{$*0, 91, 182, 273*$\}$.

For $t = 31$, the partial multipliers are: 3^i, $0 \leq i \leq 9$.

D blocks are: $\{0, 1, 5, 11\}$, $\{0, 8, 75, 193\}$.
R blocks are:
$\{0, 28, 116, 84\}$, $\{0, 20, 60, 264\}$, $\{0, 48, 274, 134\}$, $\{0, 25, 147, 121\}$, $\{0, 35, 74, 326\}$, $\{0, 47, 189, 259\}$, $\{0, 2, 251, 168\}$, $\{0, 17, 256, 240\}$, $\{0, 44, 105, 170\}$, $\{0, 13, 248, 180\}$, $\{0, 51, 154, 232\}$, $\{$*0, 94, 188, 282*$\}$.

For $t = 33$, the partial multipliers are: 3^i, $0 \leq i \leq 9$.
D blocks are: $\{0, 1, 7, 23\}$, $\{0, 13, 37, 164\}$.
R blocks are:
$\{0, 36, 118, 360\}$, $\{0, 5, 139, 354\}$, $\{0, 35, 85, 245\}$, $\{0, 14, 154, 340\}$, $\{0, 34, 172, 278\}$, $\{0, 25, 80, 305\}$, $\{0, 30, 385, 250\}$, $\{0, 59, 247, 17\}$, $\{0, 20, 130, 295\}$, $\{0, 29, 94, 298\}$, $\{0, 10, 284, 62\}$, $\{0, 2, 70, 145\}$, $\{0, 87, 177, 292\}$, $\{$*0, 100, 200, 300*$\}$. □

Lemma 3.8 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in \{35,\ 38,\ 39,\ 41\}$.

Proof. For $t = 35$, the partial multipliers are: 3^i, $0 \leq i \leq 23$.
D block is: $\{0, 1, 11, 351\}$.
R blocks are:
$\{0, 21, 159, 96\}$, $\{0, 15, 367, 319\}$, $\{0, 16, 272, 312\}$, $\{0, 5, 109, 285\}$, $\{0, 8, 192, 289\}$, $\{0, 7, 336, 53\}$, $\{0, 13, 145, 271\}$, $\{0, 19, 47, 136\}$, $\{0, 35, 251, 80\}$, $\{0, 39, 264, 64\}$, $\{0, 24, 56, 291\}$, $\{$*0, 106, 212, 318*$\}$.

For $t = 38$, the partial multipliers are: 3^i, $0 \leq i \leq 20$.
D block is: $\{0, 1, 5, 94\}$.
R blocks are:
$\{0, 6, 210, 159\}$, $\{0, 11, 372, 303\}$, $\{0, 2, 299, 322\}$, $\{0, 17, 407, 224\}$, $\{0, 60, 368, 192\}$, $\{0, 38, 384, 264\}$, $\{0, 20, 290, 130\}$, $\{0, 26, 344, 266\}$, $\{0, 44, 403, 342\}$, $\{0, 10, 50, 106\}$, $\{0, 19, 147, 49\}$, $\{0, 34, 310, 124\}$, $\{0, 32, 112, 212\}$, $\{0, 18, 260, 306\}$, $\{0, 33, 87, 155\}$, $\{0, 29, 261, 398\}$, $\{0, 64, 166, 337\}$, $\{$*0, 115, 230, 345*$\}$.

For $t = 39$, the partial multipliers are: 3^i, $0 \leq i \leq 24$.
D block is: $\{0, 1, 5, 114\}$.
R blocks are:
$\{0, 14, 416, 65\}$, $\{0, 39, 195, 105\}$, $\{0, 2, 154, 202\}$, $\{0, 38, 286, 366\}$, $\{0, 16, 136, 313\}$, $\{0, 22, 442, 280\}$, $\{0, 13, 268, 170\}$, $\{0, 32, 104, 190\}$, $\{0, 6, 184, 344\}$, $\{0, 10, 332, 122\}$, $\{0, 18, 448, 216\}$, $\{0, 8, 96, 304\}$, $\{0, 40, 413, 94\}$, $\{0, 53, 117, 179\}$, $\{$*0, 118, 236, 354*$\}$.

For $t = 41$, the partial multipliers are: 3^i, $0 \leq i \leq 26$.
D block is: $\{0, 1, 18, 211\}$.
R blocks are:
$\{0, 24, 328, 142\}$, $\{0, 2, 267, 403\}$, $\{0, 16, 165, 88\}$, $\{0, 12, 80, 324\}$, $\{0, 6, 336, 305\}$, $\{0, 4, 200, 284\}$, $\{0, 20, 48, 368\}$, $\{0, 49, 444, 104\}$, $\{0, 60, 152, 376\}$, $\{0, 36, 388, 256\}$, $\{0, 40, 116, 228\}$, $\{0, 32, 96, 236\}$, $\{0, 8, 155, 434\}$, $\{0, 44, 100, 332\}$, $\{$*0, 124, 248, 372*$\}$. □

Lemma 3.9 *There exists a* $(12t + 4, 4, 1)$*-CBIBD for each* $t \in \{44,\ 45,\ 46,\ 47,\ 49\}$.

Proof. For $t = 44$, the partial multipliers are: 3^i, $0 \le i \le 8$.

D blocks are: $\{0, 1, 5, 11\}$, $\{0, 7, 23, 49\}$, $\{0, 8, 25, 96\}$.

R blocks are:

$\{0, 57, 285, 202\}$, $\{0, 37, 134, 417\}$, $\{0, 19, 364, 114\}$, $\{0, 31, 160, 421\}$, $\{0, 34, 199, 420\}$, $\{0, 56, 422, 251\}$, $\{0, 53, 140, 393\}$, $\{0, 43, 136, 342\}$, $\{0, 50, 391, 327\}$, $\{0, 29, 222, 448\}$, $\{0, 28, 430, 308\}$, $\{0, 41, 85, 467\}$, $\{0, 52, 246, 369\}$, $\{0, 47, 305, 196\}$, $\{0, 38, 446, 132\}$, $\{0, 55, 456, 214\}$, $\{0, 74, 156, 365\}$, $\{$*0, 133, 266, 399*$\}$.

For $t = 45$, the partial multipliers are: 3^i, $0 \le i \le 15$.

D blocks are: $\{0, 1, 5, 19\}$, $\{0, 7, 35, 125\}$.

R blocks are:

$\{0, 51, 224, 464\}$, $\{0, 17, 102, 255\}$, $\{0, 24, 377, 473\}$, $\{0, 43, 331, 259\}$, $\{0, 16, 456, 296\}$, $\{0, 25, 176, 457\}$, $\{0, 8, 504, 283\}$, $\{0, 56, 208, 129\}$, $\{0, 75, 219, 374\}$, $\{0, 32, 339, 305\}$, $\{0, 68, 425, 225\}$, $\{0, 29, 453, 340\}$, $\{0, 64, 192, 376\}$, $\{$*0, 136, 272, 408*$\}$.

For $t = 46$, the partial multipliers are: 3^i, $0 \le i \le 28$.

D blocks are: $\{0, 1, 7, 24\}$.

R blocks are:

$\{0, 50, 436, 494\}$, $\{0, 34, 234, 138\}$, $\{0, 32, 197, 512\}$, $\{0, 12, 314, 374\}$, $\{0, 55, 380, 508\}$, $\{0, 2, 250, 416\}$, $\{0, 35, 228, 424\}$, $\{0, 16, 137, 384\}$, $\{0, 28, 373, 479\}$, $\{0, 10, 408, 382\}$, $\{0, 4, 150, 286\}$, $\{0, 46, 472, 206\}$, $\{0, 61, 312, 466\}$, $\{0, 36, 118, 304\}$, $\{0, 30, 478, 354\}$, $\{0, 8, 246, 102\}$, $\{0, 40, 185, 376\}$, $\{$*0, 139, 278, 417*$\}$.

For $t = 47$, the partial multipliers are: 7^i, $0 \le i \le 32$.

D block is: $\{0, 1, 3, 29\}$.

R blocks are:

$\{0, 58, 244, 355\}$, $\{0, 15, 368, 216\}$, $\{0, 65, 177, 449\}$, $\{0, 16, 360, 48\}$, $\{0, 24, 327, 432\}$, $\{0, 33, 120, 497\}$, $\{0, 40, 455, 168\}$, $\{0, 4, 375, 166\}$, $\{0, 17, 280, 81\}$, $\{0, 11, 491, 243\}$, $\{0, 41, 137, 465\}$, $\{0, 8, 151, 231\}$, $\{0, 56, 313, 489\}$, $\{0, 72, 167, 264\}$, $\{$*0, 142, 284, 426*$\}$.

For $t = 49$, the partial multipliers are: 5^i, $0 \le i \le 30$.

D block is: $\{0, 1, 3, 12\}$.

R blocks are:

$\{0, 30, 352, 424\}$, $\{0, 34, 96, 450\}$, $\{0, 61, 407, 215\}$, $\{0, 22, 112, 456\}$, $\{0, 6, 366, 470\}$, $\{0, 18, 312, 224\}$, $\{0, 32, 80, 408\}$, $\{0, 52, 287, 431\}$, $\{0, 16, 56, 474\}$, $\{0, 43, 237, 353\}$, $\{0, 71, 260, 150\}$, $\{0, 8, 341, 481\}$, $\{0, 46, 120, 334\}$, $\{0, 47, 409, 199\}$, $\{0, 37, 306, 197\}$, $\{0, 24, 78, 414\}$, $\{0, 42, 426, 106\}$, $\{0, 108, 222, 422\}$, $\{$*0, 148, 296, 444*$\}$. $\square$

Combining the above lemmas with Theorem 1.1, we complete the proof of Theorem 1.2.

4 Some classes of CBIBD

Using the results of small CBIBDs and recursive constructions, we can obtain classes of CBIBD. It is readily seen that there exists a $(u, 4, 1)$-DM whenever $u \equiv 1 \pmod 6$ from

Lemma 2.2. Applying the recursive constructions in Section 2 and the results obtained above, we have the following.

Lemma 4.1 *There exists a* $(4uv, 4, 1)$*-CBIBD, where* u *is a product of primes* $p \equiv 1 \pmod 6$ *such that* $\gcd((p-1)/6, 20!) \neq 1$ *and* $v = 3t+1$ *(not necessarily prime),* $3 \leq t \leq 50$.

Proof. By Theorem 1.2, there exists a $(4v, 4, 1)$-CBIBD. Since $\gcd(u, 6) = 1$ and there exists a $(4u, 4, 1)$-CBIBD by Theorem 1.1(3), a $(4uv, 4, 1)$-CBIBD exists from Lemma 2.1 (ii). □

Lemma 4.2 *There exists a* $(4uv, 4, 1)$*-CBIBD, where* u *is a product of primes* p *such that* $\gcd((p-1)/6, 20!) \neq 1$ *and* $v = v_1 \cdots v_m$*,* $v_i = 6t_i+1$ *(not necessarily prime),* $2 \leq t_i \leq 25$.

Proof. By Theorem 1.2, there exists a $(4v_i, 4, 1)$-CBIBD. Clearly, $\gcd(v_j, 6) = 1$, by Lemma 2.1 (ii), there exists a $(4v, 4, 1)$-CBIBD. Since $\gcd(v, 6) = 1$ and there exists a $(4u, 4, 1)$-CBIBD by Theorem 1.1(3), the conclusion comes from Lemma 2.1 (ii). □

Lemma 4.3 *There exists a* $(4^n uv, 4, 1)$*-CBIBD, where* $n \geq 3$*,* u *is a product of primes* $p \equiv 1 \pmod 6$ *and* $v = v_1 \cdots v_m$*,* $v_i = 6t_i + 1$ *(not necessarily prime),* $2 \leq t_i \leq 25$.

Proof. By Theorem 1.2, there exists a $(4v_i, 4, 1)$-CBIBD. Clearly, $\gcd(v_j, 6) = 1$, by Lemma 2.1 (ii), there exists a $(4v, 4, 1)$-CBIBD. Since $\gcd(v, 6) = 1$ and there exists a $(4^n u, 4, 1)$-CBIBD by Theorem 1.1(4), the conclusion comes from Lemma 2.1 (ii). □

Chang [11] showed the following.

Lemma 4.4 *Let* $t > 0$ *be odd. If there exists* $(16t, 4, 1)$*-CBIBD, then so does a* $(16tu, 4, 1)$*-CBIBD for any* u *which is a product of primes congruent to 1 modulo 6.*

Combing with Theorem 1.2, we have the following.

Lemma 4.5 *There exists a* $(16tu, 4, 1)$*-CBIBD, where* u *is a product of primes congruent to 1 modulo 6 and* $t = 7, 13, 19, 25, 31, 37$.

5 Applications in OOCs

$(v, k, 1)$-CBIBDs are closely related to *optical orthogonal codes* which were introduced in [15] and have many important applications (e.g., see [16]). 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.

Let v, k be positive integers. A $(0, 1)$ sequence of *length* v and *weight* k is a sequence with exactly k 1's and $v-k$ 0's. A $(v, k, 1)$-OOC, $\mathcal{C}$, is a family of $(0, 1)$ sequences (called *codewords*) of length v and weight k satisfying two properties (all subscripts are reduced modulo v).

1) (The Autocorrelation Property)

$$\sum_{0 \le t \le v-1} x_t x_{t+i} \le 1$$

for any $\mathbf{x} = (x_0, x_1, \cdots, x_{v-1}) \in \mathcal{C}$ and any integer $i \not\equiv 0 \pmod v$;

2) (The Cross-Correlation Property)

$$\sum_{0 \le t \le v-1} x_t y_{t+i} \le 1$$

for any

$$\mathbf{x} = (x_0, x_1, \cdots, x_{v-1}) \in \mathcal{C}$$
$$\mathbf{y} = (y_0, y_1, \cdots, y_{v-1}) \in \mathcal{C}$$

with $\mathbf{x} \ne \mathbf{y}$, and any integer i.

Identify any codewords $\mathbf{x} \in \mathcal{C}$ with the subset of Z_v whose characteristic function is $\mathbf{x}$. A $(v, k, 1)$-OOC may be more conveniently viewed as a set $\mathcal{F}$ of k-subsets of Z_v with the property that $\Delta\mathcal{F}$ has no repeated elements. A trivial counting argument shows that the size of a $(v, k, 1)$-OOC can not exceed $\lfloor \frac{v-1}{k(k-1)} \rfloor$. The OOC is said to be *optimal* when its size reaches this bound.

It is clear that a $(12t + 4, 4, 1)$-CBIBD leads to an optimal $(12t + 4, 4, 1)$-OOC. From the results of previous section, we have the following results of OOCs.

Theorem 5.1 *There exist an optimal* $(4u, 4, 1)$*-OOC, where* u *is a product of primes* p *congruent to 1 modulo 12 and an optimal* $(16tu, 4, 1)$*-OOC, where* u *is a product of primes congruent to 1 modulo 6 and* $t = 7, 13, 19, 25, 31, 37$.

Theorem 5.2 *There exist optimal OOCs as follows:*

- *An optimal* $(4uv, 4, 1)$*-OOC, where* u *is a product of primes* p *congruent to 1 modulo 12;*
- *An optimal* $(4uv, 4, 1)$*-OOC, where* u *is a product of primes* p *such that* $\gcd((p-1)/6, 20!) \ne 1$*;*
- *An optimal* $(4^n uv, 4, 1)$*-OOC, where* $n \ge 3$*,* u *is a product of primes* $p \equiv 1 \pmod 6$.

Where $v = v_1 \cdots v_m$ *with* $v_i = 6t_i + 1$ *(not necessarily prime),* $2 \le t_i \le 25$*,* $1 \le i \le m$.

Acknowledgement

The authors thank the anonymous referee who indicated some errors in a previous version of this paper.

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] R. J. R. Abel and M. Buratti, Some progress on $(v, 4, 1)$ difference families and optimal orthogonal codes, J. Combin. Theory (A) 106 (2004), 59-75.

[3] 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.

[4] R. C. Bose, On the construction of balanced incomplete block designs, Ann Eugenics 9 (1939), 353-399.

[5] M. Buratti, Improving two theorems of Bose on difference famiies with q a prime power and $k = 4, 5$, Discrete Math. 138 (1995), 169-175.

[6] M. Buratti, Constructions of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, Discrete Math. 138 (1998), 165-182.

[7] M. Buratti, From a $(G, k, 1)$ to a $(C_k \oplus G, k, 1)$ difference family, Designs, Codes and Cryptography 11 (1997), 5-9.

[8] M. Buratti, Recursive constructions for difference matrices and relative difference families, J. Combin. Designs 6 (1998), 165-182.

[9] M. Buratti, Some regular Steiner 2-designs with block-size 4, Ars. Combin. 55 (2000), 133-137.

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

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

[12] Y. Chang anf Y. Miao, Construction for optimal optical orthogonal codes, Discrete Math. 261 (2003), 127-139

[13] P. L. Check and C. J. Colbourn, Concerning difference families with block size four, Discrete Math. 133 (1994), 285-289.

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

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

[16] C. J. Colbourn, J. H. Dinitz and D. R. Stinson, Applications of combinatorial designs to communitions, cryptography and networking, London Math. Soc. Lecture Note Ser 267 (1999), 37-100.

[17] 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.

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

[19] M. J. Colbourn and C. J. Colbourn, On cyclic block designs, Math. Report and Canadian Academy of Scinence 12 (1980), 95-98.

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

[21] R. Mathon, Constructions for cyclic Steiner 2-designs, Ann Discrete Math. 34 (1987), 353-363.

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

[23] M. Jimbo, Recursive constructions for cyclic BIB designs and their generalizations, Discrete Math. 116 (1993), 79-95.

[24] R. Peltesohn, Eine Losung der beiden Hefferschen Differenzenproblem, Compos. Math. 6 (1938), 251-257.

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

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