Cyclic resolutions of the BIB design in $PG(5,2)$

Takaaki Hishida

Department of Information Science,
Gifu University, Gifu, 501-1193, JAPAN
hishida@info.gifu-u.ac.jp

Masakazu Jimbo

Department of Mathematics,
Keio University, Yokohama, 223-8522, JAPAN
jimbo@math.keio.ac.jp

Abstract

The BIB design in $PG(n,2)$, which is the n-dimensional projective geometry over $GF(2)$, has the following automorphisms:

(i) an automorphism of order $v = 2^{n+1} - 1$;

(ii) an automorphism of order $w = 2^n - 1$.

A BIB design with the first automorphism is called *a cyclic BIB design*, and one with the second is called *a 2-rotational BIB design*. In $PG(n,2)$, a BIB design generated by the points and planes has parameters $v = 2^{n+1} - 1$, $k = 7$, $\lambda = 2^{n-1} - 1$. As far as we know, it is not known whether a BIB design consisting of points and planes in $PG(5,2)$ is resolvable, or not.

In this paper, we shall show that the BIB design generated by the planes in $PG(5,2)$ has the above 2 automorphisms. Furthermore, these designs are cyclically resolvable. Similarly, it is well known that the BIB design generated by points and lines in $PG(2m+1,2)$ for positive integer m is resolvable, but it is not known whether the design is cyclically resolvable, or not.

1 Introduction

A pair $(\mathcal{V}, \mathcal{B})$ is called a *BIB design* if $\mathcal{V}$ is a set of v *points* and $\mathcal{B}$ is a collection of b k-subsets of $\mathcal{V}$ (called *blocks*) such that every pair of points is contained in exactly λ blocks.

For a BIB design $(\mathcal{V}, \mathcal{B})$, let σ be a permutation on $\mathcal{V}$. If $\mathcal{B}^\sigma = \{B^\sigma \mid B \in \mathcal{B}\} = \mathcal{B}$ then σ is called an *automorphism* of $(\mathcal{V}, \mathcal{B})$, where $B^\sigma = \{b_1^\sigma, b_2^\sigma, \ldots, b_k^\sigma\}$ for any

$B = \{b_1, b_2, \ldots, b_k\} \in \mathcal{B}$. If an automorphism σ of $(\mathcal{V}, \mathcal{B})$ has a cycle of length v, the design is called *cyclic.*

Let τ be an automorphism of a BIB design $(\mathcal{V}, \mathcal{B})$. If a design $(\mathcal{V}, \mathcal{B})$ has an automorphism τ of order $\frac{v-1}{l}$ which admits a single fixed point ∞, and if each of its orbit lengths is $\frac{v-1}{l}$ then $(\mathcal{V}, \mathcal{B})$ is called *l-rotational.* It is well known that the BIB design generated by the planes in $PG(n, 2)$ has the following automorphisms:

(i) σ : a cyclic automorphism of order $v = 2^{n+1} - 1$;

(ii) τ : a 2-rotational automorphism of order $w = 2^n - 1$.

For a cyclic BIB design, we can identify $\mathcal{V}$ with $\boldsymbol{Z}_v = \{0, 1, \ldots, v-1\} \pmod v$. In this case $\sigma : x \mapsto x+1 \pmod v$ and $B^\sigma = B+1 = \{b_1+1, b_2+1, \ldots, b_k+1\} \pmod v$. The *block orbit* containing $B = \{b_1, b_2, \ldots, b_k\}$ is defined by the set of distinct blocks

$$B^{\sigma^i} = B + i = \{b_1 + i, b_2 + i, \ldots, b_k + i\} \pmod v$$

for $i \in \boldsymbol{Z}_v$. If a block orbit has v blocks, then the block orbit is called *full*, otherwise *short*. We fix one block from each block orbit and call it a *base block.*

For a 2-rotational BIB design, we can identify

$$\begin{aligned} \mathcal{V} &= \boldsymbol{Z}_w \times \{0, 1\} \cup \{\infty\} \\ &= \{0_0, 1_0, \cdots, (w-1)_0\} \cup \{0_1, 1_1, \cdots, (w-1)_1\} \cup \{\infty\} \pmod w. \end{aligned}$$

In this case $\tau : x \mapsto x + 1 \pmod w$ and $B^\tau = B + 1 \pmod w$. The block orbit containing $B = \{b_1, b_2, \ldots, b_k\}$ is defined by the set of distinct blocks $B^{\tau^i} = B + i \pmod w$ for $i \in \boldsymbol{Z}_w$.

If R is a set of blocks such that every point of $\mathcal{V}$ is contained in exactly one block in R, then R is called a *resolution class (spread).* If the set of blocks in a BIB design $(\mathcal{V}, \mathcal{B})$ is partitioned into resolution classes $R_1, R_2, \ldots, R_d$ then the design is called *resolvable.* And $\mathcal{R} = \{R_1, R_2, \ldots, R_d\}$ is called a *resolution.*

Assume that a cyclic BIB design $(\mathcal{V}, \mathcal{B})$ is resolvable and let $\mathcal{R} = \{R_1, R_2, \ldots, R_d\}$ be a set of resolution classes of $(\mathcal{V}, \mathcal{B})$. For a resolution class R_i, let $R_i + 1 = \{B + 1 \pmod v \mid B \in R_i\}$, and $\mathcal{R} + 1 = \{R_1 + 1, R_2 + 1, \ldots, R_d + 1\}$. If $\mathcal{R} + 1 = \{R_1 + 1, R_2 + 1, \ldots, R_d + 1\} = \mathcal{R}$ then the design is called *cyclically resolvable.* Similarly, let a design $(\mathcal{V}, \mathcal{B})$ be a 2-rotational and a resolvable design. For a resolution class R_i of $(\mathcal{V}, \mathcal{B})$, let $R_i + 1 = \{B + 1 \pmod w \mid B \in R_i\}$. If $\mathcal{R} + 1 = \mathcal{R}$ then the design is also called cyclically resolvable.

In this paper, a cyclic BIB design which is cyclically resolvable is merely called *a cyclically resolvable BIB design* and denoted by CRB(v,k,λ), although several authors named it as "cyclically resolvable cyclic BIB (CRCB) design". A 2-rotational BIB design which is cyclically resolvable is called *a 2-rotationally resolvable BIB design* denoted by 2-RRB(v,k,λ).

The notion of a CRB was first introduced by Genma, Mishima and Jimbo [4], and they showed a direct construction in the case when the block size is odd. Mishima and Jimbo [7] classified cyclically resolvable cyclic Steiner 2-designs into three types according to their relation with cyclic quasiframes, cyclic semiframes, or cyclically resolvable cyclic GDDs (group divisible design). Furthermore, Lam and Miao [5] presented a direct construction of cyclically resolvable cyclic Steiner 2-designs for one of the three types above, no matter whether the block size is odd or even. And Lam, Miao and Mishima [6] enumerated all of the non-isomorphic CRB(52, 4, 1) by using a tactical decomposition. On the other hand, it is well known that the incidence relation of points and lines in $PG(n, q)$ is a BIB design with parameters $v = q^{n+1} - 1, k = 3, \lambda = 1$. Beutelspacher [3] showed the existence of a resolution in $PG(2^i - 1, q)$ for $i \geq 2$. Baker [1] and Wettl [10] gave constructions of resolutions in $PG(2m + 1, 2)$, for any positive integer m. The resolution given by Baker [1] has a 2-rotational automorphism on the point set. Recently, Sarmiento [8] showed that the BIB design consisting of points and lines in $PG(5, 2)$ was cyclically resolvable by using a computer, and enumerated all inequivalent resolutions. In $PG(n, 2)$, a BIB design consisting of points and planes has parameters

$$v = 2^{n+1} - 1, \quad k = 7, \quad \lambda = 2^{n-1} - 1.$$

As far as we know, there is no known result on whether the BIB design generated by the planes in a projective geometry is resolvable, or not. So our aim is to find a cyclic resolution of the BIB design generated by the planes in $PG(5, 2)$. In section 2, we shall show that a cyclic BIB design consisting of points and planes in $PG(5, 2)$ is cyclically resolvable. In section 3, we consider 2-rotational automorphism and we will show that a 2-rotational BIB design is cyclically resolvable.

2 Cyclically resolvable BIB design of planes in $PG(5, 2)$

In this section, we will show a cyclic resolution of the BIB design generated by planes in $PG(5, 2)$. In $PG(5, 2)$, there are 63 points and in a plane there are 7 points, furthermore every 2 points in $PG(5, 2)$ are contained in 15 planes. Thus, let $(\mathcal{V}, \mathcal{B})$ be the BIB design consisting of points and planes in $PG(5, 2)$, the design $(\mathcal{V}, \mathcal{B})$ has $v = 63, k = 7, \lambda = 15$. Let α be a primitive element of $GF(2^6)$, then the points of $PG(5, 2)$ are represented by $\alpha^0, \alpha^1, \ldots, \alpha^{v-1}$. In this paper, α is fixed to be a root of the primitive irreducible polynomial $f(x) = x^6 + x^4 + x^3 + x + 1$ and we denote a point α^i by i to simplify the notation. The design $(\mathcal{V}, \mathcal{B})$ has 1395 blocks, and the blocks in $(\mathcal{V}, \mathcal{B})$ can be partitioned into 22 full orbits and a single short orbit. A full block orbit has length 63 and a short block orbit has length 9. We denote the full orbits by $\mathcal{O}_0, \mathcal{O}_1, \ldots, \mathcal{O}_{21}$ and the short orbit by $\mathcal{O}_s$. Let $B_0, B_1, \ldots, B_{21}, B_s$ be base blocks of $\mathcal{O}_0, \mathcal{O}_1, \ldots, \mathcal{O}_{21}, \mathcal{O}_s$, respectively. These base blocks are listed in Table 1.

Let R be a resolution class of a CRB. Then $R + i \pmod{v}$ are also resolution classes for any i. Let d be the smallest positive integer such that $R + d = R$. Then d is called the *orbit length* of R. And $\{R, R+1, \ldots, R+d-1\}$ is called the *cyclic orbit of resolution classes* including R, denoted by CR_d. It is obvious that $d|v$ and if $B \in R$ then $B + d \in R$. Thus if R does not contain any block of the short orbit, then it is

Table 1: Base blocks of block orbits generated by planes in $PG(5,2)$

full orbits

orbit	base block	orbit	base block
$\mathcal{O}_0$	{0, 1, 2, 20, 49, 56, 57}	$\mathcal{O}_{11}$	{0, 1, 22, 37, 43, 46, 56}
$\mathcal{O}_1$	{0, 1, 3, 13, 50, 53, 56}	$\mathcal{O}_{12}$	{0, 1, 29, 33, 38, 44, 56}
$\mathcal{O}_2$	{0, 1, 4, 14, 16, 35, 56}	$\mathcal{O}_{13}$	{0, 2, 4, 35, 40, 49, 51}
$\mathcal{O}_3$	{0, 1, 5, 30, 36, 45, 56}	$\mathcal{O}_{14}$	{0, 2, 5, 15, 30, 34, 49}
$\mathcal{O}_4$	{0, 1, 6, 26, 31, 56, 59}	$\mathcal{O}_{15}$	{0, 2, 6, 26, 37, 43, 49}
$\mathcal{O}_5$	{0, 1, 10, 28, 32, 56, 60}	$\mathcal{O}_{16}$	{0, 2, 11, 23, 29, 44, 49}
$\mathcal{O}_6$	{0, 1, 11, 23, 47, 56, 61}	$\mathcal{O}_{17}$	{0, 2, 17, 36, 39, 45, 49}
$\mathcal{O}_7$	{0, 1, 12, 24, 41, 52, 56}	$\mathcal{O}_{18}$	{0, 2, 22, 31, 46, 49, 59}
$\mathcal{O}_8$	{0, 1, 15, 17, 34, 39, 56}	$\mathcal{O}_{19}$	{0, 3, 13, 18, 37, 43, 54}
$\mathcal{O}_9$	{0, 1, 18, 40, 51, 54, 56}	$\mathcal{O}_{20}$	{0, 3, 13, 22, 40, 46, 51}
$\mathcal{O}_{10}$	{0, 1, 21, 25, 42, 56, 58}	$\mathcal{O}_{21}$	{0, 3, 13, 24, 36, 41, 45}

the regular short orbit

orbit	B_s
$\mathcal{O}_s$	{0, 9, 18, 27, 36, 45, 54}

easy to see that $k|d$ and

$$R = \{B_{i_t} + j_t + ud \mid t = 1, \ldots, \frac{d}{k}; u = 0, \ldots, \frac{v}{d} - 1\}$$

holds for suitable base blocks B_{i_t} and for suitable integers j_t. By relations between the length of resolution and the differences of base blocks, we can get the following facts:

(i) Possible d is 7,21 or 63 if R does not contain any block of the short orbit;

(ii) $R = \{B_s, B_s + 1, \ldots, B_s + \frac{v}{k} - 1\}$, that is, R consists of all blocks in the short orbit and $d = 1$.

Thus, there are CR_1, CR_7, CR_{21} or CR_{63} in $(\mathcal{V}, \mathcal{B})$. And by using a computer we can easily get the following Lemmas:

Lemma 1. There exists at least one CR_{63}.

Lemma 2. CR_7 can be generated by $\mathcal{O}_{19}$ and $\mathcal{O}_{20}$

Table 2: An example of CRCB generated by planes in $PG(5,2)$

$$\begin{array}{rl}
1: & [\{0,9,18,27,54,36,45\}^*] \\
63: & [\{0,1,2,56,49,57,20\},\{16,17,19,9,29,3,6\},\{11,12,15,4,46,25,27\}, \\
 & \{37,38,48,30,60,35,21\},\{52,53,10,45,31,47,14\},\{58,59,24,51,39,28,33\}, \\
 & \{32,34,43,18,55,61,13\},\{5,7,22,54,44,41,50\},\{40,42,62,36,23,26,8\}] \\
63: & [\{0,1,5,56,30,36,45\},\{15,16,25,8,12,43,47\},\{20,21,32,13,9,44,61\}, \\
 & \{18,19,33,11,52,35,57\},\{48,49,7,41,31,28,22\},\{2,4,6,51,37,53,42\}, \\
 & \{24,26,29,10,54,39,58\},\{60,62,3,46,23,34,40\},\{14,17,38,27,55,59,50\}] \\
21: & [\{0,1,6,56,26,31,59\},\{11,12,29,4,2,51,62\},\{15,18,37,28,61,3,55\}] \\
7: & [\{0,3,18,13,54,37,43\}]
\end{array}$$

$*$ the regular short orbit.

Lemma 3. For $d = 21$, an R containing a block in $\mathcal{O}_2$, $\mathcal{O}_{10}$,$\mathcal{O}_{11}$,$\mathcal{O}_{16}$ or $\mathcal{O}_{21}$ does not exist.

Lemma 4. For $d = 63$, an R containing a block in all orbits of $\mathcal{O}_2$, $\mathcal{O}_{10}$,$\mathcal{O}_{11}$,$\mathcal{O}_{16}$ and $\mathcal{O}_{21}$ does not exist.

From the above facts, we can easy see that the CRB generated by the planes in PG(5,2) can be partitioned into CR_d's of the following pattern:

$$\{CR_1, CR_7, CR_{21}, CR_{64}, CR_{64}\}$$

and in Table 2 we present an example of the above pattern. In the notation

$$d : [\{b_1, b_2, b_3\}, \{b_4, b_5, b_6\}, \ldots],$$

d gives the length of the cyclic orbit of the resolution class, and base blocks are listed in the bracket. A base block with $*$ implies a regular short orbit. For example, 21:[{0, 1, 6, 56, 26, 31, 59},{11, 12, 29, 4, 2, 51, 62}, {15, 18, 37, 28, 61, 3, 55}] is the cyclic orbit of resolution classes with length 21 and a representative class has the following blocks

$$\begin{array}{l}
\{\{0,1,6,56,26,31,59\},\{21,22,27,14,47,52,17\},\ldots, \\
\quad \{11,12,29,4,2,51,62\},\{32,33,50,25,23,9,20\},\ldots, \\
\quad\quad \{15,18,37,28,61,3,55\},\{36,39,58,49,19,24,13\},\ldots\}.
\end{array}$$

Recently, Sarmiento [9] enumerated all inequivalent cyclic resolutions of planes in $PG(5,2)$. There exist exactly 82 cyclic resolutions.

3 2-rotationally resolvable BIB design of planes in $PG(5,2)$

In this section, we consider a 2-rotational automorphism in $PG(5,2)$. In $PG(5,2)$, we can identify $\mathcal{V}$ with the vector $\boldsymbol{y} = (y_i)$, for $y_i \in \boldsymbol{Z}_2$ and $i = 0, \cdots, 5$, except for the all zero vector. Note the vector (000001); we denote (000001) by the fixed point ∞. For this automorphism, the points of $PG(5,2)$ are represented by

$$\begin{aligned} \mathcal{V} &= GF(2^5) \times \{0,1\} \cup \{(000001)\} \\ &= \{0_0, 1_0, \cdots, 30_0\} \cup \{0_1, 1_1, \cdots, 30_1\} \cup \{\infty\}, \end{aligned}$$

a 2-orbit of orbit length 31 and by a fixed point. As it is easy to treat, we consider a BIB design with a Frobenius cycle. A BIB design of planes in $PG(5,2)$ has 63 points and the block size is 7, thus we need 9 blocks to make a resolution. Let $\mathcal{R}$ be a 9-subset of blocks of a BIB design $(\mathcal{V}, \mathcal{B})$. To generate the planes of $PG(5,2)$, we multiply each block of $\mathcal{R}$ by 2, and so obtain another 9 blocks. By continuing this process we obtain 45 blocks. Next, by adding one to each of these 45 blocks, we obtain 31 Singer cycles. By this process, we can obtain $9 \times 5 \times 31 (= 1395)$ blocks; these 1395 block generate all planes of $PG(5,2)$. Thus, if $\mathcal{R}$ is a resolution class, then it is easy to generate cyclic resolution. So, in this section, our aim is to find a resolution by translating each of the base blocks by a Frobenius cycle and a Singer cycle. For example, the following 9 blocks are a resolution class.

$$\begin{aligned} &\{4_0, \infty_1, 21_1, 8_1, 8_0, 21_0, 4_1\}, \\ &\{5_0, 6_0, 2_0, 23_0, 10_0, 17_0, 19_0\}, \\ &\{29_0, 26_1, 19_1, 9_0, 13_1, 28_0, 3_1\}, \\ &\{14_0, 25_0, 30_1, 17_1, 22_1, 13_0, 20_1\}, \\ &\{24_1, 30_0, 2_1, 7_1, 9_1, 11_0, 0_0\}, \\ &\{16_0, 29_1, 6_1, 22_0, 12_1, 1_0, 0_1\}, \\ &\{12_0, 23_1, 28_1, 18_1, 11_1, 20_0, 15_0\}, \\ &\{27_0, 7_0, 10_1, 16_1, 26_0, 15_1, 14_1\}, \\ &\{1_1, 5_1, 27_1, 24_0, 18_0, 3_0, 25_1\}. \end{aligned}$$

From these blocks we can generate all planes of $PG(5,2)$ by Frobenius cycles and Singer cycles. Furthermore, we find that there exist at most 92 inequivalent cyclic resolutions which admit Frobenius cycles and Singer cycles, by examining the multiplier automorphisms.

Finally, all the results of this paper are mainly obtained by using a computer, thus our further project is to find a theoretical proof of these results.

Acknowledgement

We would like to thank Professor Malcolm Greig for reading the manuscript and for giving us many valuable comments.

References

[1] R. D. Baker (1976). Partitioning the planes of $AG_{2m}(2)$ into 2-designs, *Discrete Math*, **15**, 205-211.

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory,* Cambridge University Press, Cambridge, England (1986).

[3] A. Beutelspacher (1974). On parallelism of finite projective spaces, *Geom. Dedicata*, **3**, 35-40.

[4] M. Genma, M. Mishima and M. Jimbo (1997). Cyclic resolvability of cyclic Steiner 2-designs, *J. Combinatorial Designs*, **3**, 177-187.

[5] C. Lam and Y. Miao (1998). On cyclically resolvable cyclic Steiner 2-designs, *preprint.*

[6] C. Lam , Y. Miao and M. Mishima (1998). Cyclically resolvable cyclic Steiner 2-systems S(2,4,52), *preprint.*

[7] M. Mishima and M. Jimbo (1997). Some types of cyclically resolvable cyclic Steiner 2-designs, *Congressus Numerantium*, **123**, 193-203.

[8] J. Sarmiento (1997). On cyclic resolvability of $PG(5,2)$, *preprint.*

[9] J. Sarmiento (1998). *private communication.*

[10] F. Wettl (1991). On parallelism of odd-dimensional finite projective spaces, *Proceedings of the Second International Mathematical Miniconference*, **16**, 27-34.

(Received 5/7/99)