Cyclically Resolvable Cyclic Steiner 2-Systems $\mathrm{S}(2,4,52)$

Clement Lam and Ying Miao [1]
Centre Interuniversitaire en Calcul Mathématique Algébrique
Department of Computer Science
Concordia University
Montreal, Quebec H3G 1M8, Canada
lam@cs.concordia.ca and ymiao@cs.concordia.ca

Miwako Mishima
Department of Information Science
Gifu University
Gifu, 501-1193, Japan
miwako@info.gifu-u.ac.jp

Dedicated to S.S. Shrikhande

Abstract: All cyclically resolvable cyclic Steiner 2-systems $\mathrm{S}(2,4,52)$ are enumerated. Up to isomorphism, there are exactly six such 2-systems. Together with the well-known cyclically resolvable 1-rotational Steiner 2-system $\mathrm{S}(2,4,52)$, there exist at least seven non-isomorphic resolvable Steiner 2-systems $\mathrm{S}(2,4,52)$.

Key words and phrases: BIBD, Steiner systems, Cyclically resolvable, cyclic designs
AMS 1991 *subject classification*: 05B05, Secondary 05B20

1. Introduction

Let $\mathcal{V}$ be a set of $v = mn$ elements (*points*), $\mathcal{G}$ be a partition of $\mathcal{V}$ into n subsets of size m called *groups*, and $\mathcal{B}$ be a collection of k-subsets of $\mathcal{V}$ called *blocks*. A triple $(\mathcal{V}, \mathcal{G}, \mathcal{B})$ is called a *group divisible design* (*GDD*), if it satisfies the following properties:

(1) for each group $G \in \mathcal{G}$ and for each block $B \in \mathcal{B}$, $|G \cap B| \leq 1$, and

(2) every pair of points from distinct groups occurs together in exactly λ blocks of $\mathcal{B}$.

Note that when $m = 1$, the design is a *balanced incomplete block design* (*BIBD*). Especially a BIBD with $\lambda = 1$ is called a *Steiner* 2-*system*, denoted by $\mathrm{S}(2,k,v)$.

[1] The current address of the second author is Institute of Policy and Planning Sciences, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan. miao@sk.tsukuba.ac.jp

Given a GDD $(\mathcal{V},\mathcal{G},\mathcal{B})$, let σ be a permutation on $\mathcal{V}$. For any block $B=\{b_1,\cdots,b_k\}\in\mathcal{B}$ and any group $G=\{g_1,\cdots,g_m\}\in\mathcal{G}$, define $B^\sigma=\{b_1^\sigma,\cdots,b_k^\sigma\}$ and $G^\sigma=\{g_1^\sigma,\cdots,g_m^\sigma\}$. If $\mathcal{B}^\sigma=\{B^\sigma : B\in\mathcal{B}\}=\mathcal{B}$ and $\mathcal{G}^\sigma=\{G^\sigma : G\in\mathcal{G}\}=\mathcal{G}$, then σ is called an *automorphism* of the GDD $(\mathcal{V},\mathcal{G},\mathcal{B})$. If there is an automorphism of order $|\mathcal{V}|$, then the GDD is said to be *cyclic*. For a cyclic GDD $(\mathcal{V},\mathcal{G},\mathcal{B})$, the point set $\mathcal{V}$ can be identified with Z_v, the residue ring of integers modulo v. In this case, the GDD has an automorphism $\sigma : i\longmapsto i+1 \pmod v$, and each group of $\mathcal{G}$ must be the subgroup

$$nZ_m=\{0,n,2n,\cdots.(m-1)n\}$$

of $Z_{mn}=Z_v$ or its cosets (see [9]).

Let $B=\{b_1,\cdots,b_k\}$ be a block of a cyclic GDD $(\mathcal{V},\mathcal{G},\mathcal{B})$. The *block orbit* containing B is defined to be the set of the following distinct blocks

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

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

Let $(\mathcal{V},\mathcal{G},\mathcal{B})$ be a GDD. For a subcollection $\mathcal{B}'\subseteq\mathcal{B}$ and for a subset $H\subseteq\mathcal{V}$, if the union $\mathcal{B}'\cup\{H\}$ is a partition of the point set $\mathcal{V}$, then $\mathcal{B}'$ is called a *holey resolution class* (or a *partial parallel class*) *with respect to* H and H is called a *hole*. Especially when $H=\emptyset$, $\mathcal{B}'$ is simply called a *resolution class* (or *parallel class*). Let $\mathcal{H}$ be a collection of subsets of $\mathcal{V}$. If $\mathcal{B}$ can be written as a disjoint union $\mathcal{B}=\mathcal{P}\cup\mathcal{Q}$, where $\mathcal{P}$ is a family of holey resolution classes with respect to holes $H\in\mathcal{H}$, and $\mathcal{Q}$ is a family of resolution classes, then we call such a GDD a *quasiframe*, denoted by a quadruple $(\mathcal{V},\mathcal{G},\mathcal{H},\mathcal{B})$.

In a quasiframe, if $\mathcal{H}=\mathcal{G}$, then it is called a *semiframe*; furthermore, if $\mathcal{Q}=\emptyset$, it is called a *frame*. If $\mathcal{P}=\emptyset$, then it is called a *resolvable GDD*; furthermore, if $m=\lambda=1$, it is called a *resolvable Steiner* 2*-system*. Frames and resolvable designs had been studied extensively in the monograph [2], while semiframes had been studied, for example, in [4].

Given a quasiframe $(\mathcal{V},\ \mathcal{G},\ \mathcal{H},\ \mathcal{B})$ such that $(\mathcal{V},\mathcal{G},\mathcal{B})$ is a cyclic GDD with respect to the automorphism $\sigma : i\longmapsto i+1 \pmod v$, where $\mathcal{V}=Z_v$, then $\mathcal{P}^\sigma=\{P^\sigma : P\in\mathcal{P}\}=\{P+1 \pmod v : P\in\mathcal{P}\}$ and $\mathcal{Q}^\sigma=\{Q^\sigma : Q\in\mathcal{Q}\}=\{Q+1 \pmod v : Q\in\mathcal{Q}\}$. If σ also preserves respectively the families of holey resolution classes $\mathcal{P}$ and resolution classes $\mathcal{Q}$, that is, if $\mathcal{P}^\sigma=\mathcal{P}$ and $\mathcal{Q}^\sigma=\mathcal{Q}$, then we say that this quasiframe is a *cyclic quasiframe with respect to* σ. In this case, an *orbit of holey resolution class* (or *resolution class*) and a *base holey resolution class* (or *base resolution class*) can be defined similar to the cases of block orbit and base block respectively, and we call the minimum positive integer ℓ which satisfies

$P + \ell = P$ (or $Q + \ell = Q$) the *orbit length* of the holey resolution class P (or the resolution class Q). Evidently, ℓ divides $|\mathcal{V}|$.

In a cyclic quasiframe, it is obvious that $\mathcal{H}^\sigma = \{H^\sigma : H \in \mathcal{H}\} = \mathcal{H}$ holds. When $\mathcal{H} = \mathcal{G}$, it becomes a *cyclic semiframe*. If $\mathcal{P} = \emptyset$, it is called a *cyclically resolvable cyclic GDD*. In particular, if $\mathcal{P} = \emptyset$ and $m = 1$, the design is called a *cyclically resolvable cyclic balanced incomplete block design* (*CRCBIBD*). When $\lambda = 1$, a CRCBIBD is called a *cyclically resolvable cyclic Steiner* 2*-system*, denoted by CRCS$(2, k, v)$.

We also need the concept of isomorphic Steiner 2-systems. Two Steiner 2-systems $(\mathcal{V}_1, \mathcal{B}_1)$ and $(\mathcal{V}_2, \mathcal{B}_2)$ are said to be isomorphic if there exists a bijection $\varphi : \mathcal{V}_1 \to \mathcal{V}_2$ such that $\mathcal{B}_1^\varphi = \mathcal{B}_2$. Two resolvable Steiner 2-systems $(\mathcal{V}_1, \mathcal{B}_1)$ and $(\mathcal{V}_2, \mathcal{B}_2)$ with resolutions $\mathcal{R}_1$ and $\mathcal{R}_2$ respectively are isomorphic if there exists such a bijection φ so that $\mathcal{R}_1^\varphi = \mathcal{R}_2$. Note that an automorphism is in fact an isomorphism of a design with itself.

In this paper, we will only deal with the case $\lambda = 1$. Note that a cyclically resolvable cyclic Steiner 2-system CRCS$(2, k, v)$ contains a unique short block orbit called its *regular short block orbit*. The base block of the regular short block orbit can be chosen as

$$(v/k)Z_k = \{0, v/k, \cdots, (k-1)v/k\}.$$

Mishima and Jimbo [8] classified cyclically resolvable cyclic Steiner 2-systems into three types according to their relations with cyclic quasiframes, cyclic semiframes, or cyclically resolvable cyclic GDDs. Formally, a cyclically resolvable cyclic Steiner 2-system is of type (T1), or (T2), or (T3), if, by removing the regular short block orbit from it, it becomes

(T1) a cyclically resolvable GDD, that is, it has no holey resolution class, or

(T2) a cyclic semiframe, that is, $\mathcal{G} = \mathcal{H}$, $\mathcal{H} \neq \emptyset$, and it has both holey resolution classes and resolution classes, or

(T3) a cyclic quasiframe, that is, $\mathcal{G} \neq \mathcal{H}$, $\mathcal{H} \neq \emptyset$, and it has both holey resolution classes and resolution classes.

In (T3), if $\mathcal{G} = \mathcal{H}$ is allowed, then the type (T3) includes (T2) and if $\mathcal{H} = \emptyset$ is allowed, the type (T1) is also included in (T3).

In connection with a cyclic Steiner 2-system S$(2, k, v)$, a Steiner 2-system S$(2, k, v)$ is said to be 1*-rotational* if it has an automorphism of order $|\mathcal{V}|-1$ with one fixed point. In this case, the point set $\mathcal{V}$ can be identified with $Z_{v-1} \cup \{\infty\}$, and it has an automorphism σ: $Z_{v-1} \cup \{\infty\} \to Z_{v-1} \cup \{\infty\}$, $i \mapsto i + 1 \pmod{v-1}$, $\infty \mapsto \infty$. A *cyclically resolvable* 1*-rotational*

Steiner 2-system CRRS$(2,k,v)$ is a resolvable 1-rotational Steiner 2-system S$(2,k,v)$ where its resolution is preserved by the the automorphism σ of order $v-1$ mentioned above.

In this paper, we enumerate all cyclically resolvable cyclic Steiner 2-systems CRCS$(2,4,52)$. Up to isomorphism, there are exactly six non-isomorphic cyclically resolvable cyclic Steiner 2-systems CRCS$(2,4,52)$. Together with the well-known cyclically resolvable 1-rotational Steiner 2-system CRRS$(2,4,52)$ (see, for instance, [5]), we know that there are at least seven non-isomorphic resolvable Steiner 2-systems S$(2,4,52)$. More precisely, the best known lower bound for the number Nr of pairwise non-isomorphic resolutions of the design No. 174 in [7] is now 7, instead of 1.

2. Non-existence of CRCS(2, 4, 52) of type (T1) or (T3)

Given a set of parameters k and v such that $v \equiv k \pmod{k(k-1)}$, which is a necessary condition for the existence of a CRCS$(2,k,v)$ (cf. [3]), usually we do not know the existence of a CRCS$(2,k,v)$; and even if we know it, we do not know its type, unless we have its collection of blocks. In this section we will show that any cyclically resolvable cyclic Steiner 2-system CRCS$(2,4,52)$, if exists, must be of type (T2).

The regular short block orbit of cyclically resolvable cyclic Steiner 2-systems is arranged differently according to their types. If there exists a CRCS$(2,k,kv)$ of type (T3), its regular short orbit must be arranged in some $v_1 \times v_2$ array (see [8]), where v_1 and v_2 are two factors of v such that $v_1 \cdot v_2 = v$. But since 13 is a prime number, any CRCS$(2,4,52)$ of type (T3) must be degenerated into type (T1) or type (T2).

For a CRCS$(2,k,kv)$ of type (T1), Mishima and Jimbo [8] showed the following condition for its non-existence.

Lemma 2.1. *Let $v = p^\alpha$ for a prime number p and assume that p is relatively prime to k. Then there does not exist any CRCS$(2,k,kv)$ of type* (T1)*.*

Corollary 2.2. *There does not exist any CRCS$(2,4,52)$ of type* (T1)*.*

Proof: Apply Lemma 2.1 with the fact that $gcd(4,13) = 1$. □

As an immediate consequence, we have the following result.

Theorem 2.3. *Any cyclically resolvable cyclic Steiner 2-system CRCS$(2,4,52)$, if exists, must be of type* (T2)*.*

3. Possible sets of base blocks for CRCS(2, 4, 52) of type (T2)

Since $gcd(4, 13) = 1$, we have $Z_{52} \cong Z_4 \times Z_{13}$. In this section, instead of using Z_{52} as the point set and $\sigma : i \longmapsto i + 1 \pmod{52}$ as the automorphism, we will use $Z_4 \times Z_{13}$ as the point set and $\sigma : (i, j) \longmapsto (i, j) + (1, 1) \pmod{(4, 13)}$ as the automorphism.

The regular short block orbit of CRCS$(2, 4, 52)$ is then $\{\{(0, 0), (1, 0), (2, 0), (3, 0)\}, \bmod (-, 13)\}$, where $D = \{(0, 0), (1, 0), (2, 0), (3, 0)\}$ is a base block of this block orbit. Since the number b of blocks of CRCS$(2, 4, 52)$ is $13 \cdot 17$, and there is no short block orbit other than D, there are still four base blocks, that is, the possible set of base blocks for CRCS$(2, 4, 52)$ of type (T2) must be of the form

$$\begin{aligned} &\{(0,0),(1,0),(2,0),(3,0)\}, \ \bmod (-,13), \\ &\{(*,*),(*,*),(*,*),(*,*)\}, \ \bmod (4,13), \\ &\{(*,*),(*,*),(*,*),(*,*)\}, \ \bmod (4,13), \\ &\{(*,*),(*,*),(*,*),(*,*)\}, \ \bmod (4,13), \\ &\{(*,*),(*,*),(*,*),(*,*)\}, \ \bmod (4,13). \end{aligned} \tag{3.1}$$

We want to determine the first components of the second, third, fourth and fifth base blocks.

Let A be a real-valued $m \times n$-matrix with $m, n \in \mathcal{N}$. Let $\{R_0, \cdots, R_{s-1}\}$ be a partition of the set $\{1, 2, \cdots, m\}$ of row indices and $\{C_0, \cdots, C_{t-1}\}$ be a partition of the set $\{1, 2, \cdots, n\}$ of column indices. If for each $i \in \{0, \cdots, s-1\}$ and each $j \in \{0, \cdots, t-1\}$, the submatrix $A_{ij} = A|R_i \times C_j$ has constant row sums d_{ij} and constant column sums f_{ij}, then the family (A_{ij}) $(i \in \{0, \cdots, s-1\}, j \in \{0, \cdots, t-1\})$ is said to be a *tactical decomposition* of A.

Let $\mathcal{D}$ be a Steiner 2-system $S(2, k, v)$. Let $x_1, \cdots, x_v$ be a labelling of the points of $\mathcal{D}$ and let $B_1, \cdots, B_b$ be a labelling of the blocks of $\mathcal{D}$, where $b = v(v-1)/(k(k-1))$. We define a matrix $N = (n_{ij})$ by $n_{ij} = 1$ if x_i is on B_j and $n_{ij} = 0$ otherwise. Thus N is a $v \times b$ matrix with each entry either 1 or 0. We call N an *incidence matrix* for $\mathcal{D}$.

Let G be a permutation group acting on $\mathcal{V}$. For $x \in \mathcal{V}$ the set $x^G = \{x^g : g \in G\}$ is called the *orbit of x under G* or the *G-orbit of x*. It is clear that the set of G-orbits is a partition of $\mathcal{V}$.

Lemma 3.1. *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B}, N)$ be an incidence structure with incidence matrix N and G an automorphism group of $\mathcal{D}$. Let $\{\mathcal{V}_0, \cdots, \mathcal{V}_{s-1}\}$ be the set of G-orbits in $\mathcal{V}$, and $\{\mathcal{B}_0, \cdots, \mathcal{B}_{t-1}\}$ be the set of G-orbits in $\mathcal{B}$. For $i \in \{0, \cdots, s-1\}$ and $j \in \{0, \cdots, t-1\}$, let $N_{ij} = N|\mathcal{V}_i \times \mathcal{B}_j$. Then (N_{ij}) is a tactical decomposition of N.*

The *orbit matrices* of $\mathcal{D}$ with respect to G are the matrices $C = (c_{ij})$ and $R = (r_{ij})$ ($i \in \{0, \cdots, s-1\}$, $j \in \{0, \cdots, t-1\}$) such that $c_{ij} = |\mathcal{V}_i \cap B|$ for $B \in \mathcal{B}_j$ and $r_{ij} = |\{B : x \in B, B \in \mathcal{B}_j\}|$ for $x \in \mathcal{V}_i$. Equivalently entry c_{ij} corresponds to the sum of a column in N_{ij}, and entry r_{ij} corresponds to the sum of a row in N_{ij}. There are two relations for the entries of any orbit matrix C.

Lemma 3.2. [6] *Let n be the total number of block orbits, m be the total number of point orbits, σ_i be the size of the i-th point orbit, τ_j be the size of the j-th block orbit, and $r = (v-1)/(k-1)$ be the number of replications. Then in an orbit matrix $C = (c_{ij})$,*

$$\sum_{h=0}^{n-1} c_{ih} c_{jh} \tau_h = \begin{cases} \sigma_i \sigma_j, & \text{if } i \neq j,\ 0 \leq i, j \leq m-1, \\ \sigma_i^2 + (r-1)\sigma_i, & \text{if } i = j = 0, \cdots, m-1, \end{cases}$$

and

$$\sum_{h=0}^{n-1} c_{ih} \tau_h = r\sigma_i, \qquad i = 0, \cdots, m-1.$$

Consider a CRCS$(2, 4, 52)$, $\mathcal{D}$, with the automorphism $\sigma : (i, j) \mapsto (i, j) + (1, 1) \pmod{(4, 13)}$. Then $\sigma^{40} : (i, j) \mapsto (i, j) + (0, 1) \pmod{(4, 13)}$ is an automorphism of order 13 without fixed points or blocks. The action of $\langle \sigma^{40} \rangle$, the cyclic group of order 13 generated by σ^{40}, on the blocks is given by

$$\sigma^{40} = ((0,0), (0,1), \cdots, (0,12))((1,0), (1,1), \cdots, (1,12)) \cdots ((16,0), (16,1), \cdots, (16,12)),$$

and the action of $\langle \sigma^{40} \rangle$ on the points is given by

$$\sigma^{40} = ((0,0), (0,1), \cdots, (0,12))((1,0), (1,1), \cdots, (1,12)) \cdots ((3,0), (3,1), \cdots, (3,12)).$$

This action devides the incidence matrix N of $\mathcal{D}$ into sixty-eight 13×13 circulant submatrices N_{ij}, $0 \leq i \leq 3$, $0 \leq j \leq 16$, as shown by (3.2), where the labelling of the points and the blocks of N_{ij} are $((i,0), (i,1), \cdots, (i,12))$ and $((j,0), (j,1), \cdots, (j,12))$, respectively.

$$\begin{pmatrix} N_{00} & N_{01} & \cdots & N_{04} & N_{05} & \cdots & N_{08} & N_{09} & \cdots & N_{0,12} & N_{0,13} & \cdots & N_{0,16} \\ N_{10} & N_{11} & \cdots & N_{14} & N_{15} & \cdots & N_{18} & N_{19} & \cdots & N_{1,12} & N_{1,13} & \cdots & N_{1,16} \\ N_{20} & N_{21} & \cdots & N_{24} & N_{25} & \cdots & N_{28} & N_{29} & \cdots & N_{2,12} & N_{2,13} & \cdots & N_{2,16} \\ N_{30} & N_{31} & \cdots & N_{34} & N_{35} & \cdots & N_{38} & N_{39} & \cdots & N_{3,12} & N_{3,13} & \cdots & N_{3,16} \end{pmatrix}. \tag{3.2}$$

Here we may suppose, by permuting the submatrices, that

$$D = \begin{pmatrix} N_{00} \\ N_{10} \\ N_{20} \\ N_{30} \end{pmatrix}$$

corresponds to the regular short block orbit,

$$A = \begin{pmatrix} N_{01} & \cdots & N_{04} \\ N_{11} & \cdots & N_{14} \\ N_{21} & \cdots & N_{24} \\ N_{31} & \cdots & N_{34} \end{pmatrix}$$

corresponds to the full block orbit containing the second base block in (3.1) modulo $(4, 13)$,

$$B = \begin{pmatrix} N_{05} & \cdots & N_{08} \\ N_{15} & \cdots & N_{18} \\ N_{25} & \cdots & N_{28} \\ N_{35} & \cdots & N_{38} \end{pmatrix}$$

corresponds to the full block orbit containing the third base block in (3.1) modulo $(4, 13)$,

$$E = \begin{pmatrix} N_{09} & \cdots & N_{0,12} \\ N_{19} & \cdots & N_{1,12} \\ N_{29} & \cdots & N_{2,12} \\ N_{39} & \cdots & N_{3,12} \end{pmatrix}$$

corresponds to the full block orbit containing the fourth base block in (3.1) modulo $(4, 13)$, and

$$F = \begin{pmatrix} N_{0,13} & \cdots & N_{0,16} \\ N_{1,13} & \cdots & N_{1,16} \\ N_{2,13} & \cdots & N_{2,16} \\ N_{3,13} & \cdots & N_{3,16} \end{pmatrix}$$

corresponds to the full block orbit containing the last base block in (3.1) modulo $(4, 13)$. Note that N_{ij}, $0 \le i \le 3$, $0 \le j \le 16$, and A, B, E, F are all circulant matrices. As a consequence, the family (N_{ij}) $(i \in \{0, \cdots, 3\}, j \in \{0, \cdots, 16\})$ is a tactical decomposition of N.

Now we prove that the orbit length ℓ of every resolution class orbit not containing any block from the regular short block orbit is 4.

Assume that the cyclically resolvable cyclic Steiner 2-system CRCS$(2, 4, 52)$ has a resolution class not containing any block from the regular short block orbit with length ℓ. Since the blocks contained in the resolution class orbit are partitioned into full block orbits, $52/\ell$ must devide 13, which means $\ell = 4$ or 52. When $\ell = 52$, we have a contradiction because $r = (v-1)/(k-1) = 17 < 52$. So $\ell = 4$.

We may suppose also, by permuting columns, that the part F corresponds to the resolution class orbit containing no block from the regular short block orbit. Then the orbit matrix of F is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

We also note that then there is a symmetry among A, B and E.

We try continuing to determine the orbit matrix C of $\mathcal{D}$ with respect to $\langle\sigma^{40}\rangle$. By applying Lemma 3.2 to $\mathcal{D}$, we have

$$\sum_{h=0}^{16} c_{ih}c_{jh} = \begin{cases} 13, & \text{if } i \neq j,\ 0 \leq i, j \leq 3, \\ 29, & \text{if } i = j = 0, \cdots, 3, \end{cases} \tag{3.3}$$

and

$$\sum_{h=0}^{16} c_{ih} = 17, \quad i = 0, \cdots, 3. \tag{3.4}$$

So we know that

$$C \cdot C^T = \begin{pmatrix} 29 & 13 & 13 & 13 \\ 13 & 29 & 13 & 13 \\ 13 & 13 & 29 & 13 \\ 13 & 13 & 13 & 29 \end{pmatrix}. \tag{3.5}$$

Let a_i be the number of entries equaling i in a row of the orbit matrix C. Since $k = 4$ in our case, we have $i \leq 4$. Also a_i is a non-negative integer. We have the following system of equations:

$$\begin{cases} 4^2a_4 + 3^2a_3 + 2^2a_2 + 1^2a_1 + 0^2a_0 = 29, \\ 4a_4 + 3a_3 + 2a_2 + 1a_1 + 0a_0 = 17, \\ a_4 + a_3 + a_2 + a_1 + a_0 = 17. \end{cases} \tag{3.6}$$

The first equation comes from (3.3), the second from (3.4), and the third from the definition of the orbit matrix.

We can solve this system of equations (3.6), and obtain exactly the following four solutions:

$$(a_4, a_3, a_2, a_1, a_0) = (1, 0, 0, 13, 3), (0, 2, 0, 11, 4), (0, 1, 3, 8, 5), (0, 0, 6, 5, 6).$$

We can prove that the solution $(a_4, a_3, a_2, a_1, a_0) = (0, 2, 0, 11, 4)$ is not admissible. Since $k = 4$, by permuting rows and/or columns, we may assume that the matrices A and B, are of one of the following three forms:

$$\begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 3 \\ 3 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 3 \\ 3 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 3 \\ 3 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \end{pmatrix},$$

and that E is of the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

The possible values of the dot-product of any two distinct rows of A and B are 0, 3, or 6. The values of the dot-products of any two distinct rows of D, E, F are 1, 4, and 4, respectively. So the dot-product of the two distinct rows of the orbit matrix C has the value $1+4+4+$ a multiple of 3, which cannot equal 13. This is a contradiction to (3.5).

Secondly, we consider the solution $(a_4, a_3, a_2, a_1, a_0) = (1, 0, 0, 13, 3)$. Noting that $k = 4$, the orbit matrix C must be of the following form:

$$\begin{pmatrix} 1 & 4 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 4 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 4 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Thirdly, we consider the solution $(a_4, a_3, a_2, a_1, a_0) = (0, 1, 3, 8, 5)$. There are exactly eighteen possible orbit matrices for C. The only one satisfying equation (3.5) is:

$$\begin{pmatrix} 1 & 3 & 0 & 1 & 0 & 2 & 2 & 0 & 0 & 2 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 3 & 0 & 1 & 0 & 2 & 2 & 0 & 1 & 2 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 3 & 0 & 0 & 0 & 2 & 2 & 0 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 3 & 2 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Finally, we consider the solution $(a_4, a_3, a_2, a_1, a_0) = (0, 0, 6, 5, 6)$. There are exactly four possible orbit matrices for C. The only one satisfying equation (3.5) is:

$$\begin{pmatrix} 1 & 2 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 2 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 1 \\ 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We next restate the three orbit matrices as three set of base blocks. Note that the symmetry of permuting columns and rows in an orbit matrice is reflected as adding an arbitrary element $(i, j) \bmod (4, 13)$ to the elements in all the base blocks. Sets of base blocks which differs only the the addition of $(i, j) \bmod (4, 13)$ are said to be *equivalent*.

Theorem 3.3. *The set of base blocks of any cyclically resolvable cyclic Steiner* 2*-system* $CRCS(2, 4, 52)$ *of type* (T2)*, if exists, must be equivalent to one of the following three forms:*

$$\{(0,0),(1,0),(2,0),(3,0)\}, \ \bmod (-,13),$$
$$\{(0,*),(0,*),(0,*),(0,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(1,*),(2,*),(3,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(1,*),(2,*),(3,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(1,*),(2,*),(3,*)\}, \ \bmod (4,13);$$

$$\{(0,0),(1,0),(2,0),(3,0)\}, \ \bmod (-,13),$$
$$\{(0,*),(0,*),(0,*),(2,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(0,*),(1,*),(1,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(0,*),(1,*),(3,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(1,*),(2,*),(3,*)\}, \ \bmod (4,13);$$

$$\{(0,0),(1,0),(2,0),(3,0)\}, \ \bmod (-,13),$$
$$\{(0,*),(0,*),(2,*),(2,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(0,*),(1,*),(1,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(0,*),(1,*),(1,*)\}, \ \bmod (4,13),$$
$$\{(0,*),(1,*),(2,*),(3,*)\}, \ \bmod (4,13).$$

4. Enumeration

In order to get cyclically resolvable cyclic Steiner 2-systems CRCS$(2, 4, 52)$, each set of base blocks shown in Theorem 3.3 should generate a CRCS$(2, 4, 52)$, and the second components of the second, third and fourth base blocks should form a partition of $Z_{13} - \{0\}$.

Colbourn and Mathon [1] found that there are exactly two hundred and six non-isomorphic cyclic Steiner systems S(2, 4, 52). We can check their solutuions to see whether they satisfy our conditions by transforming the point set Z_{52} into $Z_4 \times Z_{13}$. We first check whether the base blocks are equivalent to one of the forms in Theorem 3.3. We then identify the candidates for base blocks 2 to 4. Next, we check the requirement that the second component of these three base blocks should not overlap. To avoid overlaps, we shift the third and fourth base blocks by adding $(0, j) \bmod (-, 13)$ independently to these two blocks. Finally, we may have to shift the first base block in order that its second component do not overlap those in the second to fourth base blocks. We find, out of these two hundred and six solutions of S(2, 4, 52), exactly six are cyclically resolvable cyclic Steiner 2-systems. They are listed in Appendix A, where the numbers are those in [1]. Their full automorphism group are all of size 52. However, since their underlying cyclic Steiner 2-systems $S(2, 4, 52)$ are non-isomorphic, these six cyclically resolvable cyclic Steiner 2-systems $CRCS(2, 4, 52)$ are of course non-isomorphic.

Theorem 4.1. *There are exactly six non-isomorphic cyclically resolvable cyclic Steiner* 2-*systems CRCS*$(2, 4, 52)$.

On the other hand, there exists (see, for example, [5]) a cyclically resolvable 1-rotational Steiner 2-system $CRRS(2, 4, 52)$ based on the point set $Z_{51} \cup \{\infty\}$ with an automorphism $\sigma : Z_{51} \cup \{\infty\} \to Z_{51} \cup \{\infty\}$, such that $i \mapsto i+1$, and $\infty \mapsto \infty$. It is obvious that this cyclically resolvable 1-rotational Steiner 2-system $S(2, 4, 52)$ is not isomorphic to any of the above six cyclically resolvable cyclic Steiner 2-systems $CRCS(2, 4, 52)$, because their automorphisms of point sets are different.

As a consequence, we have the following assertion.

Theorem 4.2. *There are at least seven non-isomorphic resolvable Steiner* 2-*systems S*$(2, 4, 52)$, *among which six are cyclically resolvable cyclic Steiner* 2-*systems, and one is cyclically resolvable* 1-*rotational Steiner* 2-*system.*

Acknowledgements

The first author is supported in part by the National Science and Research Council of Canada and Funds pour la Formation de Chercheurs et l'Aide à la Recherche. The second author is supported in part by a Post-Doctoral Fellowship from the Centre Interuniversitare en Calcul Mathématique Algébrique.

References

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

[2] S. Furino, Y. Miao and J. Yin, *Frames and Resolvable Designs: Uses, Constructions, and Existence*, CRC Press, Boca Raton, 1996.

[3] M. Genma, M. Mishima and M. Jimbo, *Cyclic resolvability of cyclic Steiner 2-designs*, J. Combin. Designs 5 (1997), 177–187.

[4] S. Kageyama and Y. Miao, *Some constructions of semiframes*, Ars Combinatoria 43 (1996), 17–31.

[5] S. Kageyama and Y. Miao, *Note on a paper "1-Rotational designs with block size 4"*, Bulletin of the ICA 20 (1997), 82–84.

[6] R. Mathon, *Computational methods in design theory*, in: *Surveys in Combinatorial 1991* (ed. A. D. Keedwell), *London Mathematical Society Lecture Note Series* 166, Cambridge University Press, Cambridge (1991), 101–118.

[7] R. Mathon and A. Rosa, 2-(v, k, λ) *designs of small order*, in: *The CRC Handbook of Combinatorial Designs* (eds. C. J. Colbourn and J. H. Dinitz), CRC Press, Boca Raton (1996), 3–41.

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

[9] R. Mukerjee, M. Jimbo and S. Kageyama, *On cyclic semi-regular group divisible designs*, Osaka J. Math. 24 (1987), 395–407.

Appendix A:

No.125

$$\{(0,3),(1,3),(2,3),(3,3)\},\ \bmod (-,13),$$
$$\{(0,0),(0,4),(1,9),(1,6)\},\ \bmod (4,13),$$
$$\{(0,1),(0,8),(2,7),(2,5)\},\ \bmod (4,13),$$
$$\{(0,2),(0,10),(3,12),(3,11)\},\ \bmod (4,13),$$
$$\{(0,0),(1,1),(2,8),(3,3)\},\ \bmod (4,13).$$

No.132

$$\{(0,1),(1,1),(2,1),(3,1)\},\ \bmod (-,13),$$
$$\{(0,0),(0,4),(3,11),(3,8)\},\ \bmod (4,13),$$
$$\{(0,10),(2,3),(0,12),(2,9)\},\ \bmod (4,13),$$
$$\{(0,7),(0,2),(1,5),(1,6)\},\ \bmod (4,13),$$
$$\{(0,0),(1,1),(2,8),(3,3)\},\ \bmod (4,13).$$

No.163

$$\{(0,6),(1,6),(2,6),(3,6)\},\ \bmod (-,13),$$
$$\{(0,0),(0,4),(1,1),(1,8)\},\ \bmod (4,13),$$
$$\{(0,9),(0,12),(0,7),(2,11)\},\ \bmod (4,13),$$
$$\{(3,10),(0,2),(1,5),(0,3)\},\ \bmod (4,13),$$
$$\{(0,0),(2,6),(3,2),(1,12)\},\ \bmod (4,13).$$

No.164

$$\{(0,6),(1,6),(2,6),(3,6)\},\ \bmod (-,13),$$
$$\{(0,0),(1,1),(0,4),(1,8)\},\ \bmod (4,13),$$
$$\{(0,9),(2,11),(0,12),(0,7)\},\ \bmod (4,13),$$
$$\{(3,10),(0,2),(1,5),(0,3)\},\ \bmod (4,13),$$
$$\{(0,0),(2,6),(1,7),(3,4)\},\ \bmod (4,13).$$

No.167

$$\{(0,12),(1,12),(2,12),(3,12)\},\ \bmod (-,13),$$
$$\{(0,0),(1,1),(0,4),(1,8)\},\ \bmod (4,13),$$
$$\{(0,7),(2,9),(2,11),(2,6)\},\ \bmod (4,13),$$
$$\{(0,10),(1,2),(2,5),(1,3)\},\ \bmod (4,13),$$
$$\{(0,0),(2,6),(3,2),(1,12)\},\ \bmod (4,13).$$

No.168

$$\{(0,12),(1,12),(2,12),(3,12)\},\ \bmod\ (-,13),$$
$$\{(0,0),(1,1),(0,4),(1,8)\},\ \bmod\ (4,13),$$
$$\{(0,7),(2,9),(2,11),(2,6)\},\ \bmod\ (4,13),$$
$$\{(0,10),(1,2),(2,5),(1,3)\},\ \bmod\ (4,13),$$
$$\{(0,0),(2,6),(1,7),(3,4)\},\ \bmod\ (4,13).$$