

# Coherent configurations over copies of association schemes of prime order

Reza Sharafdini \*

*Department of Mathematics, Faculty of Science, Persian Gulf University,  
Bushehr 75169–13817, Iran.*

Mitsugu Hirasaka

*Department of Mathematics, College of Natural Sciences, Pusan National University,  
Busan 609–735, South Korea.*

Received 21 November 2014, accepted 17 May 2016, published online 2 November 2016

---

## Abstract

Let  $G$  be a group acting faithfully and transitively on  $\Omega_i$  for  $i = 1, 2$ . A famous theorem by Burnside implies the following fact: If  $|\Omega_1| = |\Omega_2|$  is a prime and the rank of one of the actions is greater than two, then the actions are equivalent, or equivalently  $|(\alpha, \beta)^G| = |\Omega_1| = |\Omega_2|$  for some  $(\alpha, \beta) \in \Omega_1 \times \Omega_2$ .

In this paper we consider a combinatorial analogue to this fact through the theory of coherent configurations, and give some arithmetic sufficient conditions for a coherent configuration with two homogeneous components of prime order to be uniquely determined by one of the homogeneous components.

*Keywords:* Coherent configurations, association schemes, prime order, symmetric designs.

*Math. Subj. Class.:* 05C15, 05C10

---

## 1 Introduction

A famous theorem by Burnside states that each transitive permutation group of prime degree with rank greater than two is Frobenius or regular. Since any Frobenius group of prime degree is a subgroup of one-dimensional affine group, it follows that such a permutation group is uniquely determined by its rank and degree up to equivalence of group actions. Especially, if a group acts faithfully, transitively but not 2-transitively on each of two sets of the same prime size, then the two actions are equivalent. Let us formulate this fact in the following two paragraphs.

---

\*Corresponding author.

*E-mail addresses:* sharafdini@pgu.ac.ir (Reza Sharafdini), hirasaka@pusan.ac.kr (Mitsugu Hirasaka)

Let  $G$  be a group acting transitively on  $\Omega_i$  for  $i = 1, 2$ . Then  $G$  acts on  $\Omega_i \times \Omega_j$  by

$$(\alpha, \beta)^g = (\alpha^g, \beta^g) \quad \text{for } (\alpha, \beta) \in \Omega_i \times \Omega_j \quad \text{and } g \in G,$$

for all  $i, j = 1, 2$ . It is well-known that (e.g., see [6, Lemma 1.6B]) the following are equivalent:

- (a) The action of  $G$  on  $\Omega_1$  is equivalent to that on  $\Omega_2$ ;
- (b) There exists  $(\alpha, \beta) \in \Omega_1 \times \Omega_2$  such that  $G_\alpha = G_\beta$ ;
- (c) There exists  $(\alpha, \beta) \in \Omega_1 \times \Omega_2$  such that  $|(\alpha, \beta)^G| = |\Omega_1| = |\Omega_2|$ .

Note that the rank of the action of  $G$  on  $\Omega_i$  is equal to the number of orbits of  $G$  on  $\Omega_i \times \Omega_i$ , and if  $G$  acts faithfully on  $\Omega_i$ , then  $G$  can be identified with a permutation group of  $\Omega_i$ .

Suppose that  $G$  acts faithfully on  $\Omega_i$  with  $i = 1, 2$  and  $|\Omega_1| = |\Omega_2|$  is a prime. Then, as mentioned in the first paragraph, these actions are equivalent if the rank of one of the actions is greater than two, and so there exists an orbit  $R$  of  $G$  on  $\Omega_1 \times \Omega_2$  such that  $|R| = |\Omega_1| = |\Omega_2|$ .

In this paper we consider a combinatorial analogy to this fact through the theory of coherent configurations. The concept of coherent configurations was first introduced by Higman who published a series of papers (e.g., [11], [12], [13]) to associate a lot of important criterions with group actions.

Here we define a coherent configuration, its intersection numbers and its fibers according to the notations as in [7].

**Definition 1.1.** Let  $V$  be a finite set and  $\mathcal{R}$  a partition of  $V \times V$ . We say that the pair  $\mathcal{C} = (V, \mathcal{R})$  is a *coherent configuration* if it satisfies the following:

1. The diagonal relation  $\Delta_V$  is a union of elements of  $\mathcal{R}$  where we denote  $\{(u, u) \mid u \in U\}$  by  $\Delta_U$  for a set  $U$ .
2. For each  $R \in \mathcal{R}$  its transpose  $R^t = \{(u, v) \mid (v, u) \in R\}$  is an element of  $\mathcal{R}$ .
3. For all  $R, S, T \in \mathcal{R}$  there exists a constant  $c_{RS}^T$  such that

$$c_{RS}^T = |R(u) \cap S^t(v)| \text{ for all } (u, v) \in T,$$

where we denote by  $T(w)$  the set  $\{z \in V \mid (w, z) \in T\}$  for  $w \in V$  and  $T \in \mathcal{R}$ .

The constants  $c_{RS}^T$  are called the *intersection numbers*. A subset  $X$  of  $V$  is called a *fiber* of  $\mathcal{C}$  if  $\Delta_X \in \mathcal{R}$ . We denote the set of all fibers of  $\mathcal{C}$  by  $\text{Fib}(\mathcal{C})$ . By Definition 1.1(i),  $V$  is partitioned into the fibers of  $\mathcal{C}$ , and by Definition 1.1(i),(iii),  $\mathcal{R}$  is partitioned into

$$\left\{ \mathcal{R}_{X,Y} \mid X, Y \in \text{Fib}(\mathcal{C}) \right\} \text{ where } \mathcal{R}_{X,Y} = \left\{ R \in \mathcal{R} \mid R \subseteq X \times Y \right\}.$$

Let  $U$  be a union of fibers of  $\mathcal{C}$ . Then the pair

$$\left( U, \{R \in \mathcal{R} \mid R \subseteq U \times U\} \right),$$

is also a coherent configuration, which is denoted by  $\mathcal{C}_U$ .

For  $R \in \mathcal{R}_{X,Y}$  we denote  $c_{RR^t}^X$  by  $d_R$ . Then, by two-way counting we have

$$|R| = d_R|X| = d_{R^t}|Y|. \tag{1.1}$$

For  $X \in \text{Fib}(\mathcal{C})$ ,  $\mathcal{C}_X$  is nothing but an *association scheme*, i.e., a coherent configuration with only one fiber (see [2] or [20] for its background). For short we shall write  $\mathcal{R}_{X,X}$  as  $\mathcal{R}_X$  and  $\mathcal{C}_X$  is called a *homogeneous component* of  $\mathcal{C}$ .

A general question here is formulated as follows: what can be said about the coherent configuration if its homogeneous components are known. For example, it is a well-known fact that the coherent configuration corresponds to a system of linked block designs if  $|\mathcal{R}_X| = 2$  for all  $X \in \text{Fib}(\mathcal{C})$ . After the seminal Hanaki-Uno theorem on association schemes of prime order (see [10] or Theorem 3.1), it seems quite natural to ask on a possible structure of a coherent configuration each homogeneous component of which is of prime order. The following is our first main result answering to this question:

**Theorem 1.2.** *Let  $X, Y \in \text{Fib}(\mathcal{C})$  such that  $|X| = |Y|$  is a prime. Then  $|\mathcal{R}_{X,Y}| \in \{1, |\mathcal{R}_X|\}$ . In particular, if  $|\mathcal{R}_{X,Y}| > 1$ , then*

$$|\mathcal{R}_{X,Y}| = |\mathcal{R}_X| = |\mathcal{R}_Y|.$$

In order to state our second main theorem we need to recall the following observation. Let  $G$  be a group acting on a finite set  $\Omega$ . Then  $G$  acts on  $\Omega \times \Omega$  componentwise, and an orbit of  $G$  on  $\Omega \times \Omega$  is called an *orbital* (or 2-orbit) of  $G$ . We denote the set of orbitals of  $G$  by  $\mathcal{O}_G$ . Then it is well-known that  $\mathcal{C}_G = (\Omega, \mathcal{O}_G)$  is a coherent configuration, and  $\text{Fib}(\mathcal{C}_G)$  is the set of orbits of  $G$  on  $\Omega$ . In this sense, a coherent configuration is a combinatorial object to generalize the orbitals of a group action.

Now we assume that  $\mathcal{C} = (V, \mathcal{R})$  is a coherent configuration with exactly two fibers  $X, Y$ . Then (1.1) proves the equivalence of the first two statements of the following (see [16] for the remaining):

- (d) There exists  $R \in \mathcal{R}_{X,Y}$  such that  $|R| = |X| = |Y|$ .
- (e)  $1 \in \{d_R \mid R \in \mathcal{R}_{X,Y}\} \cap \{d_R \mid R \in \mathcal{R}_{Y,X}\}$ .
- (f)  $\mathcal{C}$  is isomorphic to  $\mathcal{C}_X \otimes \mathcal{T}_2$  where  $\mathcal{T}_n = \left( \{1, 2, \dots, n\}, \{ \{(i, j)\} \mid 1 \leq i, j \leq n \} \right)$  (see Section 2 for the definition of isomorphism and  $\otimes$ ).

We notice the following:

(d) is a combinatorial analogy to (c), and such  $R$  is a matching between  $X$  and  $Y$ ; (e) is a simple arithmetic condition on intersection numbers; (f) implies that  $\mathcal{C}_X$  and  $\mathcal{C}_Y$  are isomorphic, and  $\mathcal{C}$  is uniquely determined by  $\mathcal{C}_X$ .

In this paper we aim to obtain the analogous conclusion (d)–(f) to (a)–(c). The following is our second main result to generalize the fact as in the first paragraph under certain arithmetic conditions on intersection numbers:

**Theorem 1.3.** *Suppose that  $\mathcal{C} = (V, \mathcal{R})$  is a coherent configuration with exactly two fibers  $X, Y$  satisfying*

$$|X| = |Y| \text{ is a prime, } |\mathcal{R}_{X,X}| > 2 \text{ and } |\mathcal{R}_{X,Y}| > 1. \tag{1.2}$$

*Then there exists  $R \in \mathcal{R}_{X,Y}$  such that  $|R| = |X| = |Y|$  if one of the following conditions holds with  $k = \frac{|X| - 1}{|\mathcal{R}_{X,X}| - 1}$ :*

- (i)  $|\mathcal{R}_{X,X}| > k^2(k + e - 2)$  where  $e$  is the number of prime divisors of  $k$ ;

- (ii)  $k \in \{q, 2q, 3q\}$  for some prime power  $q$ ;
- (iii)  $k = 4q$  for some prime power  $q$  with  $3 \nmid q + 1$ .

Let us show the reason why we exclude the case of  $|\mathcal{R}_{X,X}| = 2$ . Each symmetric design induces the coherent configuration with exactly two fibers and eight relations (see [14] or [16, Example 1.3]), and if the design is a non-trivial one on a prime number of points, like the Fano plane, then the induced coherent configuration does not satisfy (d)–(f).

Of course, if  $|\mathcal{R}_{X,Y}| = 1$ , then none of (d)–(f) hold, while  $\mathcal{C}$  is the direct sum of  $\mathcal{C}_X$  and  $\mathcal{C}_Y$  (see [16] for the definition of direct sum).

**Remark 1.4.** Applying Theorem 1.3 for  $\mathcal{C}_{X \cup Y}$  with  $|X| < 100$  we obtain the same conclusion as Theorem 1.3 except for the case  $(|X|, k) = (71, 35)$  (see Section 5 for the details).

Suppose that

$$(|X|, k) = (71, 35) \text{ and } 1 \notin \{d_R \mid R \in \mathcal{R}_{X,Y}\}. \tag{1.3}$$

Then by Theorem 1.2,  $|\mathcal{R}_{X,Y}| = 3$ . The three elements of  $\mathcal{R}_{X,Y}$  must form three symmetric designs whose parameters  $(v, k, \lambda)$  are  $(71, 35, 17)$ ,  $(71, 21, 6)$  and  $(71, 15, 3)$ , respectively. Though each of such symmetric designs exists (see [1], [3], [5], [9] and [17] or [4, II.6.24, VI.16.30]), it does not guarantee the existence of a coherent configuration satisfying (1.3).

In [14], Higman gave a result to eliminate the case of  $(|X|, k) = (71, 35)$  as in the previous paragraph. But, the proof given in [14, (3.2)] contains a serious gap, so the result may not be recognized to be true, while we have not found any counterexample. We would be able to disprove [14, (3.2)] if there exists a coherent configuration satisfying (1.3).

In Section 2 we prepare several basic results on intersection numbers and introduce the concepts of complex products and equitable partitions. In Section 3 we give a proof of Theorem 1.2. In Section 4 we give a proof of Theorem 1.3. We add Section 5 for the elimination of coherent configurations on at most 200 points satisfying (1.2).

## 2 Preliminaries

Throughout this section we assume that  $\mathcal{C} = (V, \mathcal{R})$  is a coherent configuration.

Let  $\mathcal{C}_i = (V_i, \mathcal{R}_i)$  be a coherent configurations,  $i = 1, 2$ .

An *isomorphism* from  $\mathcal{C}_1$  to  $\mathcal{C}_2$  is defined to be a bijection  $\psi : V_1 \cup \mathcal{R}_1 \rightarrow V_2 \cup \mathcal{R}_2$  such that for all  $u, v \in V_1$  and  $R \in \mathcal{R}_1$ ,

$$(u, v) \in R \iff (\psi(u), \psi(v)) \in \psi(R).$$

We say that  $\mathcal{C}_1$  is *isomorphic* to  $\mathcal{C}_2$  and denote it by  $\mathcal{C}_1 \simeq \mathcal{C}_2$  if there exists an isomorphism from  $\mathcal{C}_1$  to  $\mathcal{C}_2$ .

We set

$$\mathcal{R}_1 \otimes \mathcal{R}_2 = \left\{ R_1 \otimes R_2 \mid R_1 \in \mathcal{R}_1, R_2 \in \mathcal{R}_2 \right\},$$

where

$$R_1 \otimes R_2 = \left\{ ((u_1, u_2), (v_1, v_2)) \mid (u_1, v_1) \in R_1, (u_2, v_2) \in R_2 \right\}.$$

Then  $(V_1 \times V_2, \mathcal{R}_1 \otimes \mathcal{R}_2)$  is a coherent configuration called the *tensor product* of  $\mathcal{C}_1$  and  $\mathcal{C}_2$  and denoted by  $\mathcal{C}_1 \otimes \mathcal{C}_2$ .

Following [20] we define the *complex product* on the power set of  $\mathcal{R}$ . For all subsets  $\mathcal{S}$  and  $\mathcal{T}$  of  $\mathcal{R}$  we define the complex product  $\mathcal{ST}$  of  $\mathcal{S}$  and  $\mathcal{T}$  to be the subset

$$\left\{ R \in \mathcal{R} \mid \exists (S, T) \in \mathcal{S} \times \mathcal{T}; c_{ST}^R > 0 \right\}.$$

The complex product is an associative binary operation on the power set of  $\mathcal{R}$  where the proof is parallel to that for association schemes (see [20]). For convenience we shall write  $\mathcal{S}\{T\}$ ,  $\{S\}\mathcal{T}$  and  $\{S\}\{T\}$  as  $ST$ ,  $ST$  and  $ST$ , respectively.

In this paper we need intersection numbers  $c_{RS}^T$  for  $R \in \mathcal{R}_{X,Y}$ ,  $S \in \mathcal{R}_{Y,Z}$  and  $T \in \mathcal{R}_{X,Z}$  under the assumption  $|X| = |Y| = |Z|$ . The following is a collection of simplified equations on such intersection numbers (see [19] or [16, Lemma 2.2] for general formed equations<sup>1</sup>). For  $\mathcal{U} \subseteq \mathcal{R}$  we shall write  $d_{\mathcal{U}}$  instead of  $\sum_{U \in \mathcal{U}} d_U$ .

**Lemma 2.1.** *For all  $X, Y, Z \in \text{Fib}(\mathcal{C})$  with  $|X| = |Y| = |Z|$  and all  $R \in \mathcal{R}_{X,Y}$ ,  $S \in \mathcal{R}_{Y,Z}$  and  $T \in \mathcal{R}_{X,Z}$  we have the following:*

1.  $d_R d_S = \sum_{T \in \mathcal{R}_{X,Z}} c_{RS}^T d_T$ ;
2.  $c_{RS}^T d_T = c_{TS}^R d_R = c_{R^t T}^S d_S$  and  $\text{lcm}(d_R, d_S) \mid c_{RS}^T d_T$ ;
3.  $|\{U \in \mathcal{R} \mid c_{RS}^U > 0\}| \leq \text{gcd}(d_R, d_S)$ , i.e.,  $|RS| \leq \text{gcd}(d_R, d_S)$ ;
4.  $|X| = d_{\mathcal{R}_{X,X}} = d_{\mathcal{R}_{X,Y}}$ .

The following lemmata were proved in [18, Lemma 2.3, Lemma 2.2]<sup>2</sup>:

**Lemma 2.2.** *For all  $S, T \in \mathcal{R}_{X,Y}$  with  $|X| = |Y|$ , we have*

$$SS^t \cap TT^t \subseteq \{\Delta_X\} \text{ if and only if } c_{S^t T}^R \leq 1 \text{ for each } R \in \mathcal{R}.$$

**Lemma 2.3.** *Let  $Z \in \text{Fib}(\mathcal{C})$  such that  $|Z|$  is a prime. Then for each  $R \in \mathcal{R}_Z \setminus \{\Delta_Z\}$  we have:*

1.  $d_R = k$  where  $k = \frac{|Z| - 1}{|\mathcal{R}_Z| - 1}$ ;
2.  $\sum_{S \in \mathcal{R}_Z} c_{S^t}^R = k - 1$ .

According to [8] or [15] we define an equitable partition of a homogeneous component.

**Definition 2.4.** Let  $X \in \text{Fib}(\mathcal{C})$  and  $\Pi = \{C_1, C_2, \dots, C_m\}$  be a partition of  $X$ , i.e.,

$$X = \bigcup_{i=1}^m C_i, \quad C_i \cap C_j \neq \emptyset \text{ if } i \neq j, \text{ and } C_i \neq \emptyset \text{ for each } i = 1, 2, \dots, m.$$

An element of  $\Pi$  is called a *cell*. We say that  $\Pi$  is an *equitable partition* of  $\mathcal{C}_X$  if, for all  $i, j = 1, 2, \dots, m$  and each  $R \in \mathcal{R}_X$ ,  $|R(x) \cap C_j|$  is constant whenever  $x \in C_i$ .

<sup>1</sup>We missed to assume that all fibers of  $\mathcal{C}$  have the same size at Lemma 2.2 in [16] where the lemma is used only for such coherent configurations in [16].

<sup>2</sup>Though it is a statement for association schemes, a parallel way to the proof can be applied for balanced coherent configurations.

For example,  $\{X\}$  and  $\{\{x\} \mid x \in X\}$  are equitable partitions of  $\mathcal{C}_X$ .  
 For each  $Y \in \text{Fib}(\mathcal{C})$  and each  $y \in Y$  we define

$$\Pi_y := \{T(y) \mid T \in \mathcal{R}_{Y,X}\}. \tag{2.1}$$

Then  $\Pi_y$  is an equitable partition of  $\mathcal{C}_X$ , since

$$|R(x) \cap S(y)| = c_{RS^t}^T \text{ whenever } x \in T(y).$$

### 3 Proof of Theorem 1.2

In [10] Hanaki and Uno proved the following brilliant theorem:

**Theorem 3.1.** *All non-principal irreducible characters of an association scheme of prime order are algebraic conjugate and of degree one.*

The following proposition is obtained as a consequence of the previous theorem:

**Proposition 3.2.** *Let  $\mathcal{C} = (V, \mathcal{R})$  be an association scheme of prime order and  $\Pi$  be an equitable partition of  $\mathcal{C}$ . Then  $|\Pi| \equiv 1 \pmod{|\mathcal{R}| - 1}$ .*

*Proof.* Let  $\mathcal{A}$  denote the adjacency algebra of  $\mathcal{C}$  over  $\mathbb{C}$ . Then the subspace  $W$  spanned by the characteristic vectors of the cells in  $\Pi$  is a left  $\mathcal{A}$ -module with respect to the ordinary matrix product. Since  $\mathcal{A}$  is semi-simple,  $W$  is a direct sum of irreducible submodules.

Note that the subspace spanned by the all-one vector is an  $\mathcal{A}$ -submodule of  $W$  affording the principal character, and its multiplicity is one.

Since the character afforded by  $W$  is integral valued, it is left invariant from any algebraic conjugate action. It follows from Theorem 3.1 that all non-principal irreducible submodules of  $W$  have the same multiplicity, say  $m$ . Since

$$\dim_{\mathbb{C}}(W) = |\Pi| \text{ and } \dim_{\mathbb{C}}(\mathcal{A}) = |\mathcal{R}|,$$

it follows that

$$|\Pi| = 1 + m(|\mathcal{R}| - 1).$$

□

**Proof of Theorem 1.2.** Let  $\mathcal{C} = (V, \mathcal{R})$  be a coherent configuration with  $X, Y \in \text{Fib}(\mathcal{C})$  such that  $|X| = |Y|$  is a prime. Recall that  $\Pi_y$  is an equitable partition of  $\mathcal{C}_X$  where  $y \in Y$ . By (2.1),  $|\Pi_y| = |\mathcal{R}_{X,Y}|$ . Then it follows from Proposition 3.2 that

$$|\mathcal{R}_{X,Y}| \equiv 1 \pmod{|\mathcal{R}_X| - 1}.$$

Since  $|\mathcal{R}_{X,Y}| \leq |\mathcal{R}_X|$  (see [13, p.223] or [16, Proposition 2.7]),  $|\mathcal{R}_{X,Y}| \in \{1, |\mathcal{R}_X|\}$ . Applying the first statement for  $\mathcal{C}_Y$  with  $|\mathcal{R}_{X,Y}| \leq |\mathcal{R}_Y|$ , we obtain the second statement.

□

### 4 Proof of Theorem 1.3

For the remainder of this paper we assume that  $\mathcal{C} = (V, \mathcal{R})$  is a coherent configuration with  $X, Y \in \text{Fib}(\mathcal{C})$  such that

$$m = |X| = |Y| \text{ is a prime, } r = |\mathcal{R}_X| > 2 \text{ and } |\mathcal{R}_{X,Y}| > 1.$$

By Theorem 1.2, we have

$$r = |\mathcal{R}_X| = |\mathcal{R}_{X,Y}| = |\mathcal{R}_Y|.$$

For the remainder of this paper we set

$$k = \frac{m-1}{r-1}.$$

By Lemma 2.3(i) the multi-set  $(d_R \mid R \in \mathcal{R}_Z)$  with  $Z \in \{X, Y\}$  coincides with  $(1, k, \dots, k)$  by a suitable ordering. In this section we aim to show that  $1 \in \{d_R \mid R \in \mathcal{R}_{X,Y}\}$ , which implies that the multi-set  $(d_R \mid R \in \mathcal{R}_{X,Y})$  coincides with  $(1, k, \dots, k)$  by a suitable ordering, since the complex product  $SR$  is a singleton with  $d_{SR} = d_S$  whenever  $S \in \mathcal{R}_X$  and  $d_R = 1$  by Lemma 2.1(iii).

**Lemma 4.1.** *For all  $S, T \in \mathcal{R}_{X,Y}$  with  $S \neq T$  we have the following:*

- (i)  $d_S d_S \equiv d_S \pmod{k}$ ;
- (ii)  $d_S d_T \equiv 0 \pmod{k}$ .

*Proof.* (i) Applying Lemma 2.1(i) for  $S$  and  $S^t$  with  $d_S = d_{S^t}$  and  $c_{SS^t}^{\Delta_X} = d_S$ , we obtain that

$$d_S d_S = d_S + k \sum_{\substack{T \in \mathcal{R}_{X,X} \\ T \neq \Delta_X}} c_{SS^t}^T.$$

(ii) Applying Lemma 2.1(i) for  $S$  and  $T^t$  with  $d_T = d_{T^t}$  and  $\Delta_X \notin ST^t$ , we obtain that

$$d_S d_T = k \sum_{T \in \mathcal{R}_{X,X}} c_{ST^t}^T.$$

□

We set

$$\mathcal{S}_1 := \{T \in \mathcal{R}_{X,Y} \mid k \nmid d_T\}, \quad \mathcal{S}_2 := \{T \in \mathcal{R}_{X,Y} \mid d_T = k\} \text{ and}$$

$$\mathcal{S}_3 := \{T \in \mathcal{R}_{X,Y} \mid k \mid d_T, k < d_T\}.$$

**Lemma 4.2.** *Let  $k = p_1^{\alpha_1} \cdots p_e^{\alpha_e}$  where  $p_i$  are the distinct prime divisors of  $k$  and  $\alpha_i$  are positive integers. Then we have the following:*

1. For each  $i = 1, \dots, e$  there exists a unique  $S \in \mathcal{R}_{X,Y}$  such that  $p_i \nmid d_S$ ;
2.  $|\mathcal{S}_1| \leq e$ ;
3.  $k|\mathcal{S}_3| + d_{\mathcal{S}_1} \leq 1 + k(e-1)$ .

*Proof.* (i) By Lemma 2.1(iv) and Lemma 2.3(i),

$$m = 1 + (r - 1)k \equiv 1 \pmod{p_i}.$$

Since  $m = d_{\mathcal{R}_{X,Y}}$ , there exists an  $S \in \mathcal{R}_{X,Y}$  such that  $p_i \nmid d_S$ . The uniqueness of such  $S$  is a direct consequence of Lemma 4.1(ii).

(ii) The correspondence given in (i) gives a function from  $\{p_1, p_2, \dots, p_e\}$  to  $\mathcal{S}_1$ . It remains to show that this function is onto.

Let  $S \in \mathcal{S}_1$ . By the definition of  $\mathcal{S}_1$ , there exists  $p_i$  such that  $p_i^{\alpha_i}$  does not divide  $d_S$ . By Lemma 4.1(i),

$$d_S d_S \equiv d_S \pmod{k}.$$

Therefore  $d_S(d_S - 1)$  is divided by  $k$ . Since  $d_S$  and  $d_S - 1$  are relatively prime,  $p_i^{\alpha_i} \nmid d_S$  implies that  $p_i \nmid d_S$ . It follows from (i) that  $d_S$  lies in the range of the function.

(iii) Note that  $r = |\mathcal{S}_1| + |\mathcal{S}_2| + |\mathcal{S}_3|$  and

$$m = \sum_{S \in \mathcal{R}_{X,Y}} d_S = \sum_{i=1}^3 d_{\mathcal{S}_i} \geq d_{\mathcal{S}_1} + k|\mathcal{S}_2| + 2k|\mathcal{S}_3|.$$

Since  $k|\mathcal{S}_2| + k|\mathcal{S}_3| = k(r - |\mathcal{S}_1|)$  and  $m = 1 + k(r - 1)$ , it follows that

$$1 + k(|\mathcal{S}_1| - 1) \geq d_{\mathcal{S}_1} + k|\mathcal{S}_3|.$$

By (ii), we have

$$1 + k(e - 1) \geq d_{\mathcal{S}_1} + k|\mathcal{S}_3|.$$

This completes the proof of (iii). □

**Lemma 4.3.** We have  $\max\{d_S \mid S \in \mathcal{R}_{X,Y}\} \leq k \cdot \min\{d_S \mid S \in \mathcal{R}_{X,Y}\}$ .

*Proof.* Let  $S, T \in \mathcal{R}_{X,Y}$  such that

$$d_S = \min\{d_S \mid S \in \mathcal{R}_{X,Y}\} \text{ and } d_T := \max\{d_S \mid S \in \mathcal{R}_{X,Y}\}.$$

Then  $T \in RS$  for some  $R \in \mathcal{R}_X$  since  $T \in \mathcal{R}_X S$ . Applying Lemma 2.1(i) we have  $d_T \leq kd_S$ . □

For  $S \in \mathcal{R}_{X,Y}$  we define

$$\mathcal{U}_S := \{R \in \mathcal{R}_X \mid R^t R \cap S S^t = \{\Delta_X\}\}.$$

**Lemma 4.4.** For each  $S \in \mathcal{R}_{X,Y}$  we have the following:

1.  $r - |\mathcal{U}_S| \leq (d_S - 1)(k - 1)$ .
2. If  $R \in \mathcal{U}_S - \{\Delta_X\}$ , then  $k$  divides  $d_T$  for each  $T \in RS$ .
3. If  $\mathcal{U}_S S \cap \mathcal{S}_2 = \emptyset$ , then  $r < d_S(k + e - 2)$ .



*Proof.* (i) Note that

$$\mathcal{R}_X - \mathcal{U}_S = \bigcup_{R_1 \in SS^t - \{\Delta_X\}} \{R \in \mathcal{R}_X \mid R_1 \in R^t R\}.$$

By Lemma 2.1(iii) with  $c_{SS^t}^{\Delta_X} > 0$ ,

$$|SS^t - \{\Delta_X\}| \leq d_S - 1.$$

It follows from Lemma 2.3(ii) that

$$|\{R \in \mathcal{R}_X \mid R_1 \in R^t R\}| \leq \sum_{R \in \mathcal{R}} c_{R^t R}^{R_1} = k - 1.$$

This implies that

$$r - |\mathcal{U}_S| = |\mathcal{R}_X - \mathcal{U}_S| \leq (d_S - 1)(k - 1).$$

(ii) It is an immediate consequence of Lemma 2.1(ii) and Lemma 2.2.

(iii) Suppose that

$$\mathcal{U}_S S \cap \mathcal{S}_2 = \emptyset.$$

Then we have

$$\mathcal{U}_S S \subseteq \mathcal{R}_{X,Y} - \mathcal{S}_2.$$

It follows from (ii) that

$$(\mathcal{U}_S - \{\Delta_X\})S \subseteq \mathcal{S}_3.$$

By Lemma 4.2(iii) and Lemma 4.3,

$$d_{\mathcal{S}_3} \leq d_S k |\mathcal{S}_3| \leq d_S [1 + k(e - 1) - d_{\mathcal{S}_1}]. \quad (4.1)$$

On the other hand, applying Lemma 2.2 and Lemma 2.1(iv) for the first inequality and (i) for the second one,

$$d_{\mathcal{U}_S S} \geq 1 + (|\mathcal{U}_S| - 1)k - d_S \geq 1 + [r - (d_S - 1)(k - 1) - 1]k. \quad (4.2)$$

Since  $(\mathcal{U}_S - \{\Delta_X\})S \subseteq \mathcal{S}_3$ ,

$$d_{\mathcal{U}_S S} - d_S \leq d_{(\mathcal{U}_S - \{\Delta_X\})S} \leq d_{\mathcal{S}_3}.$$

It follows from (4.1) and (4.2) that

$$1 + [r - (d_S - 1)(k - 1) - 1]k - d_S \leq d_S [1 + k(e - 1) - d_{\mathcal{S}_1}],$$

and hence,

$$r \leq \frac{d_S}{k} [2 + k(e - 1) - d_{\mathcal{S}_1}] - \frac{1}{k} + (d_S - 1)(k - 1) + 1.$$

Thus,

$$r \leq d_S \left[ \frac{2}{k} + e - 1 - \frac{d_{\mathcal{S}_1}}{k} + k - 1 \right] - k + 2 - \frac{1}{k} < d_S (k + e - 2).$$

This completes the proof of (iii). □

**Proposition 4.5.** *If  $r > k^2(k + e - 2)$  where  $e$  is the number of prime divisors of  $k$ , then  $1 \in \{d_S \mid S \in \mathcal{R}_{X,Y}\}$ .*

*Proof.* We claim that

$$\min\{d_S \mid S \in \mathcal{R}_{X,Y}\} \leq k.$$

If not, then

$$1 + k(r - 1) = m = \sum_{S \in \mathcal{R}_{X,Y}} d_S > kr,$$

a contradiction.

By Lemma 4.3,

$$\max\{d_S \mid S \in \mathcal{R}_{X,Y}\} \leq k^2.$$

Applying the contraposition of Lemma 4.4(iii) we have  $U_S S \cap \mathcal{S}_2 \neq \emptyset$  for each  $S \in \mathcal{R}_{X,Y}$ , and hence,  $T \in RS$  for some  $R \in U_S$  and  $T \in \mathcal{S}_2$ . Since  $d_T = k$  and  $c_{RS}^T = 1$  by Lemma 2.2,  $d_S$  divides  $k$  for each  $S \in \mathcal{R}_{X,Y}$ . This implies that  $|\mathcal{S}_3| = 0$ .

We claim  $|\mathcal{S}_1| = 1$ . Suppose not. Since  $1 + (r - 1)k = m = d_{S_1} + k(r - |\mathcal{S}_1|)$ ,

$$1 + k|\mathcal{S}_1| \leq k + \sum_{S \in \mathcal{S}_1} d_S \leq k + k/2 + k/2 + (|\mathcal{S}_1| - 2)k,$$

a contradiction. By the claim we have  $\mathcal{S}_1 = \{S\}$  for some  $S \in \mathcal{R}_{X,Y}$ . Since

$$1 + k(r - 1) = m = k|\mathcal{S}_2| + d_S = k(r - 1) + d_S,$$

we have  $d_S = 1$ . This completes the proof. □

**Lemma 4.6.** *If  $S, T \in \mathcal{R}_{X,Y}$  with  $ST^t = \{R\}$ , then*

$$c_{RR^t}^{R_1} \geq d_T \text{ for each } R_1 \in SS^t \text{ and } c_{R^tR}^{R_2} \geq d_S \text{ for each } R_2 \in TT^t.$$

*Proof.* Let  $y \in Y$ ,  $x_1, x_2 \in S^t(y)$  and  $z \in T^t(y)$ . Note that  $(x_i, z) \in R$  for  $i = 1, 2$  since  $ST^t = \{R\}$ . Since  $z \in T^t(y)$  is arbitrarily taken, we have  $T^t(y) \subseteq R(x_1) \cap R(x_2)$ , which proves the first statement. By the symmetric argument the second statement can be proved. □

**Proposition 4.7.** *There exist no  $S, T \in \mathcal{R}_{X,Y}$  such that*

$$ST^t = \{R\}, d_S + d_T \geq k + 1 \text{ and } 1 < d_S < d_T. \tag{4.3}$$

*Proof.* Suppose that  $S, T \in \mathcal{R}_{X,Y}$  satisfies (4.3).

We claim that  $SS^t = \{\Delta_X, R_1\}$  for some  $R_1 \in \mathcal{R}_X - \{\Delta_X\}$ . Suppose not, i.e.,  $SS^t - \{\Delta_X\}$  has at least two elements  $R_1, R_2$ . By Lemma 2.1(i),

$$k^2 = d_R d_{R^t} \geq k + c_{RR^t}^{R_1} d_{R_1} + c_{RR^t}^{R_2} d_{R_2} = k + c_{RR^t}^{R_1} k + c_{RR^t}^{R_2} k.$$

It follows from Lemma 4.6 and  $d_S + d_T \geq k + 1$  that

$$k^2 \geq k(k + 2),$$

a contradiction.

We claim that  $SS^t \cap TT^t = \{\Delta_X, R_1\}$ . Suppose not, i.e.,  $SS^t \cap TT^t = \{\Delta_X\}$ . Then, by Lemma 2.2,  $c_{S^t T^t}^R = 1$ . It follows from Lemma 2.1(i) that  $k = d_R = d_S d_T$ , which contradicts  $d_S + d_T \geq k + 1$  and  $1 < d_S < d_T$ .

We claim that  $R = R^t$ . Suppose not, i.e.,  $R \neq R^t$ . Then, by Lemma 2.3(ii),

$$k - 1 = \sum_{R_2 \in \mathcal{R}_X} c_{R_2 R_2^t}^{R_1} \geq c_{R R^t}^{R_1} + c_{R^t R}^{R_1} \geq d_S + d_T \geq k + 1,$$

a contradiction.

We claim that  $TT^t = \{\Delta_X, R_1\}$ . If  $R_2 \in TT^t - \{\Delta_X, R_1\}$ , then  $c_{R_2 R_2}^{R_1} \geq d_S$  by Lemma 4.6 with  $R = R^t$ . By Lemma 2.1(i),

$$k^2 = d_R d_R \geq k + c_{R R}^{R_1} k + c_{R R}^{R_2} k,$$

which implies that  $k \geq 1 + d_T + d_S$ , a contradiction to  $d_S + d_T \geq k + 1$ .

We claim that  $c_{R_1 R_1^t}^{R_1} \geq d_T - 2$ . By the previous claim, for all  $z_1, z_2 \in T^t(y)$  with  $z_1 \neq z_2$  we have  $(z_1, z_2) \in R_1$ . Thus,

$$c_{R_1 R_1^t}^{R_1} = |R_1(z_1) \cap R_1(z_2)| \geq |T^t(y) - \{z_1, z_2\}| \geq d_T - 2.$$

Since  $c_{R_1 R_1^t}^{R_1} + c_{R R^t}^{R_1} \geq d_T - 2 + d_T \geq k$  by Lemma 4.6, it follows from Lemma 2.3(ii) that  $R = R_1$ . Thus,  $c_{R R^t}^R = k - 1$  since  $1 < d_S$  and

$$S^t(y) \cup T^t(y) \setminus \{x_1, x_2\} \subseteq R(x_1) \cap R(x_2) \text{ for } x_1, x_2 \in S^t(y).$$

Since  $\{\Delta_X, R\}$  is closed under the complex product,  $1 + k$  divides  $|X|$ . Since  $|X|$  is a prime, it follows that  $\{\Delta_X, R\} = \mathcal{R}_X$ , and hence  $|\mathcal{R}_X| = 2$ , a contradiction.  $\square$

**Lemma 4.8.** *Suppose that  $k = 4q$  for some prime power  $q$  and  $1 \notin \{d_S \mid S \in \mathcal{R}_{X,Y}\}$ . Then  $|\mathcal{S}_3| = 0$ ,  $|\mathcal{S}_1| = 2$ , and  $\{d_S \mid S \in \mathcal{S}_1\} = \{3q, q + 1\}$ .*

*Proof.* By Lemma 4.2(iii) and the assumption,  $|\mathcal{S}_3| = 0$ . By Lemma 4.2(ii),  $|\mathcal{S}_1| \leq 2$ . Let  $S \in \mathcal{S}_1$ . Then, by Lemma 4.1,  $d_S \equiv 1 \pmod q$ . By the assumption,  $1 < d_S < 4q$ . Since  $d_S \leq d_{S_1} \leq 1 + 4q$  Lemma 4.2(iii), it follows from Lemma 4.1 that

$$d_S \in \{q + 1, 3q + 1\}.$$

Let  $T \in \mathcal{R}_{X,Y}$  with  $S \neq T$ . Since  $d_S d_T \equiv 0 \pmod{4q}$  by Lemma 4.1,  $q \mid d_T$ . Since  $m = 1 + k(r - 1) = d_{S_1} + d_{S_2} = d_S + d_T + k(r - 2)$ , we have  $d_S + d_T = k + 1$ . Therefore, we conclude from Proposition 4.7 that  $\{d_S \mid S \in \mathcal{S}_1\} = \{3q, q + 1\}$ .  $\square$

**Proof of Theorem 1.3.** (i) is a direct consequence of Proposition 4.5.

(ii) Suppose on the contrary that

$$1 \notin \{d_S \mid S \in \mathcal{R}_{X,Y}\}.$$

Note that  $e \leq 2$  if  $k \in \{q, 2q, 3q\}$  for some prime power  $q$ . By Lemma 4.2(iii),  $|\mathcal{S}_3| = 0$ , and  $d_{S_1} \leq k + 1$ . Since

$$1 + k(r - 1) = d_{S_1} + d_{S_2} \leq k + 1 + d_{S_2},$$

we have  $d_{S_2} \geq k(r - 2)$ , and, hence,  $|S_2| \geq r - 2$ .

Suppose  $k = q$ . Then the statement follows from Lemma 4.2(iii) since  $e = 1$ .

Suppose  $k = 2q$ . Then  $|S_1| \leq 2$  and  $\{d_S \mid S \in \mathcal{S}_1\} = \{q, q + 1\}$  by Lemma 4.2(ii),(iii) and Lemma 4.1. Without loss of generality we assume that

$$\mathcal{S}_1 = \{S, T\}, d_S = q + 1 \text{ and } d_T = q.$$

Since  $q$  and  $q + 1$  are relatively prime, it follows from Lemma 2.1(iii) that  $ST^t = \{R\}$  for some  $R \in \mathcal{R}$ , which contradicts Proposition 4.7.

Suppose  $k = 3q$ . Then we have either

$$\{d_S \mid S \in \mathcal{S}_1\} = \{q, 2q + 1\} \text{ or } \{d_S \mid S \in \mathcal{S}_1\} = \{2q, q + 1\}.$$

The first case is done by Proposition 4.7.

For the last case we assume that  $\mathcal{S}_1 = \{S, T\}$ ,  $d_S = q + 1$  and  $d_T = 2q$ . By Lemma 2.1(i),(ii),  $SS^t = \{\Delta_X, R\}$  for some  $R \in \mathcal{R}$  with  $R = R^t$ . This implies that  $k = d_R$  is even since  $|X|$  is an odd prime, so  $q$  is a power of two. Thus,  $d_S$  and  $d_T$  are relatively prime. Therefore, the statement follows from Lemma 2.1(iii) and Proposition 4.7.

(iii) Suppose  $k = 4q$ . Then, by Lemma 4.8,  $\{d_S \mid S \in \mathcal{R}_{X,Y}\} = \{q, 3q + 1\}$  or  $\{d_S \mid S \in \mathcal{R}_{X,Y}\} = \{3q, q + 1\}$ . The statement follows from the assumption and Proposition 4.7. □

## 5 Appendix

In this section we show how Theorem 1.3 is applied to small configurations  $\mathcal{C}_{X \cup Y}$  with  $|X| = |Y| < 100$ .

First, we denote by  $\mathcal{M}$  the set of primes  $m$  less than 100.

Second, we take the set  $\mathcal{K}$  of positive integers  $k$  such that

$$k \mid m - 1 \text{ for some } m \in \mathcal{M} \text{ with } k < m - 1 \text{ and}$$

$$k \notin \{q, 2q, 3q \mid q \text{ is a prime power}\} \cup \{4q \mid q \text{ is a prime power with } 3 \nmid q + 1\}.$$

Then  $\mathcal{K} = \{20, 30, 35, 44\}$ .

**Lemma 5.1.** *If  $k = 20$ , then  $1 \in \{d_S \mid S \in \mathcal{R}_{X,Y}\}$ .*

*Proof.* Suppose not. By Lemma 4.8,  $\{d_S \mid S \in \mathcal{S}_1\} = \{15, 6\}$ . Let  $S \in \mathcal{R}_{X,Y}$  with  $d_S = 6$ . By Lemma 2.1(ii),  $6 \mid c_{SS^t}^R k$  for  $R \in SS^t \setminus \{\Delta_X\}$ . Thus,  $3 \mid c_{SS^t}^R$ , which contradicts Lemma 2.1(ii). □

**Lemma 5.2.** *Suppose that each element of  $\mathcal{R}_Y = \{\Delta_Y, R, R'\}$  is symmetric and  $\Pi_x = \{C_1, C_2, C_3\}$  is the equitable partition of  $(Y, \mathcal{R}_Y)$  as in Section 2 for  $x \in X$ . We define*

$$\{\beta_{ij}\}_{1 \leq i, j \leq 3} \text{ and } \{\gamma_{ij}\}_{1 \leq i, j \leq 3}$$

*such that  $\beta_{ij} = |R(y) \cap C_j|$  with  $y \in C_i$  and  $\gamma_{ij} := |R'(y) \cap C_j|$  with  $y \in C_i$ . Then we have the following:*

1. *For each  $i$  we have  $\sum_{j=1}^3 \beta_{ij} = k$ ;*
2. *For all  $i, j$  with  $i \neq j$  we have  $\beta_{ij} + \gamma_{ij} = |C_j|$ ;*

3. For each  $i$  we have  $\beta_{ii} + \gamma_{ii} = |C_i| - 1$ ;
4. For all  $i, j$  we have  $|C_i|\beta_{ij} = \beta_{ji}|C_j|$ ;
5. We have  $\beta_{11} + \beta_{22} + \beta_{33} = k - 1$ .

*Proof.* The first four statements can be proved by checking the definition of equitable partitions and using a double-way counting for  $(C_i \times C_j) \cap R$ .

Let  $\mathcal{A}$  be the adjacency algebra of  $\mathcal{C}_Y$  and  $W$  the subspace spanned by the characteristic vectors of the cells of  $\Pi_x$ . Then  $W$  is a left  $\mathcal{A}$ -module corresponding to the algebra homomorphism defined by  $A_R \mapsto (\beta_{ij}), A_{R'} \mapsto (\gamma_{ij})$ .

We claim that  $W$  affords the regular character. Let  $\chi$  be the character afforded by  $W$ , i.e., the value of the adjacency matrix of  $R$  is equal to  $\sum_{i=1}^3 \beta_{ii}$ . Note that the character afforded by  $W$  is integral valued but not a sum of principal character. Since  $\dim(W) = 3$ , it follows that  $\chi$  is the sum of irreducible characters of  $\mathcal{A}$ . This implies that  $\chi$  is the regular character of  $\mathcal{A}$ , and, hence, the trace of the matrix  $(\beta_{ij})$  is equal to  $k - 1$  by Lemma 2.3(ii) with Lemma 2.1(ii).  $\square$

**Proposition 5.3.** *If  $(k, m) = (30, 61)$ , then  $1 \in \{d_S \mid S \in \mathcal{R}_{X,Y}\}$ .*

*Proof.* Suppose not.

By Lemma 4.2(ii),(iii),  $|\mathcal{S}_1| \leq 3$  and  $|\mathcal{S}_3| \leq 1$ . if  $|\mathcal{S}_3| = 1$ , then  $2k \leq d_{\mathcal{S}_3} < m = 2k + 1$ , a contradiction. Thus,  $|\mathcal{S}_3| = 0$ .

Since  $|\mathcal{S}_2| \leq 1$ , it follows from Lemma 4.1 that the following are only possible cases of  $\{d_S \mid S \in \mathcal{R}_{X,Y}\}$ :

$$\{30, 25, 6\}; \{30, 15, 16\}; \{30, 10, 21\}; \{15, 36, 10\}; \{15, 6, 40\}.$$

The first three cases do not occur by Proposition 4.7 since each of them contains a pair of relatively prime numbers.

Note that  $\{|C_i| \mid i = 1, 2, 3\} = \{d_S \mid S \in \mathcal{R}_{X,Y}\}$  where  $\Pi_x = \{C_1, C_2, C_3\}$  as in Lemma 5.2. Without loss of generality we may assume that

$$C_i = S_i(x) \text{ for } i = 1, 2, 3.$$

From now on we shall use Lemma 5.2 many times without mentioning.

Suppose that

$$(|C_1|, |C_2|, |C_3|) = (10, 15, 36).$$

Since  $|C_2|\beta_{23} = |C_3|\beta_{32}$ , we have  $12 \mid \beta_{23}$ . If  $\beta_{23} \in \{0, 36\}$ , then  $|S_2S_3^t| = 1$ , which contradicts Proposition 4.5. Replacing  $R \in \mathcal{R}_Y$  by  $R'$  if necessary we may assume that  $\beta_{23} = 24$ , and hence,  $\beta_{32} = 10$ .

Since

$$|C_1|\beta_{13} = |C_3|\beta_{31},$$

we have  $18 \mid \beta_{13}$ . If  $\beta_{13} \in \{0, 36\}$ , then  $|S_3S_1^t| = 1$ , which contradicts Proposition 4.7. Thus,  $\beta_{13} = 18$ , and, hence,  $\beta_{31} = 5$ .

By Lemma 5.2(i),

$$\beta_{33} = 15, \beta_{21} + \beta_{22} = 6 \text{ and } \beta_{11} + \beta_{12} = 12.$$

By Lemma 5.2(v),  $\beta_{11} + \beta_{22} = 23$ . Thus,  $\beta_{12} + \beta_{21} = 19$ , which contradicts  $10\beta_{12} = 15\beta_{21}$ . Therefore,  $(d_S, d_T, d_U) = (10, 15, 36)$  does not occur.

Suppose

$$(|C_1|, |C_2|, |C_3|) = (15, 6, 40).$$

Since  $|C_2|\beta_{23} = |C_3|\beta_{32}$ , we have  $20 \mid \beta_{23}$ . If  $\beta_{23} \in \{0, 40\}$ , then  $|S_2S_3^t| = 1$ , which contradicts Proposition 4.7. We may assume that  $\beta_{23} = 20$ , and hence,  $\beta_{32} = 3$ .

Since

$$|C_1|\beta_{12} = |C_2|\beta_{21},$$

we have  $5 \mid \beta_{21}$ . By Lemma 5.2(i),

$$\beta_{21} + \beta_{22} + 20 = 30.$$

Thus,  $5 \mid \beta_{22}$ . Replacing  $R \in \mathcal{R}_Y$  by  $R'$  if necessary we may assume that  $\beta_{22} = 5$ , and hence,  $\beta_{21} = 5$  and  $\beta_{12} = 2$ .

By Lemma 5.2(i),(v), we have

$$\beta_{11} + \beta_{13} = 28, \beta_{31} + \beta_{33} = 27 \text{ and } \beta_{11} + \beta_{33} = 24.$$

Thus,  $\beta_{13} + \beta_{31} = 31$ , which contradicts  $15\beta_{13} = 40\beta_{31}$ .

This completes the proof. □

**Proposition 5.4.** *If  $(k, m) = (44, 89)$ , then  $1 \in \{d_S \mid S \in \mathcal{R}_{X,Y}\}$ .*

*Proof.* Suppose not. By Lemma 4.8, the following is a unique possible case of  $\{d_S \mid S \in \mathcal{R}_{X,Y}\}$ :

$$\{12, 33, 44\}.$$

Without loss of generality we may assume that

$$C_i = S_i(y) \text{ for } i = 1, 2, 3 \text{ and } (|C_1|, |C_2|, |C_3|) = (12, 33, 44).$$

Since  $12\beta_{12} = 33\beta_{21}$ ,  $\beta_{12} \in \{0, 11, 22, 33\}$ . Proposition 4.7 forces  $\beta_{12} \in \{11, 22\}$ , and we may assume that  $\beta_{12} = 22$  by replacing  $R \in \mathcal{R}_Y$  by  $R'$ . Then  $\beta_{21} = 8$ .

Note that 11 divides  $\beta_{13}$  and so does  $\beta_{11}$  by Lemma 5.2(i). We divide our consideration into the following two cases  $\beta_{11} = 11$  or 0.

Suppose  $\beta_{11} = 11$ . Then  $\beta_{13} = 11$  and  $\beta_{31} = 3$ . By Lemma 5.2(i),(v),

$$\beta_{22} + \beta_{23} = 36, \beta_{32} + \beta_{33} = 41 \text{ and } \beta_{22} + \beta_{33} = 32.$$

Therefore,  $\beta_{23} + \beta_{32} = 45$ , which contradicts  $33\beta_{23} = 44\beta_{32}$ .

Suppose  $\beta_{11} = 0$ . Then

$$\beta_{13} = 22 \text{ and } \beta_{31} = 6.$$

By Lemma 5.2(i),(v),

$$\beta_{22} + \beta_{23} = 36, \beta_{32} + \beta_{33} = 38 \text{ and } \beta_{22} + \beta_{33} = 43.$$

Therefore,  $\beta_{23} + \beta_{32} = 34$ , which contradicts  $33\beta_{23} = 44\beta_{32}$ .

This completes the proof. □

**Lemma 5.5.** *If  $(k, m) = (35, 71)$  then  $\{d_S \mid S \in \mathcal{R}_{X,Y}\} = \{15, 21, 35\}$ .*

*Proof.* Applying Lemma 4.2(i),(iii) and Lemma 4.1 we conclude that  $\{15, 21, 35\}$  is a unique case of  $\{d_S \mid S \in \mathcal{R}_{X,Y}\}$ . □

We notice that the lemmata given in this section justify the elimination given in Introduction.

## Acknowledgements

First, the authors would like to express gratitude to Professor Akihiro Munemasa for his valuable suggestions in revising Theorem 1.3.

Second, the authors are grateful to anonymous referees for their kind attention to our work, carefully checking and error corrections.

The introduction of the current article was revised according to comments and suggestions of one of the referees. We greatly appreciate his/her contribution helped clarify and improve our article.

The first author was supported by the Persian Gulf University Research Council under the contract No: **PGU/FS/49-1/1390/1468**.

## References

- [1] E. Ademaj and M. Essert, Classification of symmetric block design for  $(71, 21, 6)$  with non-abelian group of order 21, *Math. Commun.* **9** (2004), 45–49.
- [2] E. Bannai and T. Ito, *Algebraic combinatorics. I*, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984, association schemes.
- [3] H. Beker and W. Haemers, 2-designs having an intersection number  $k - n$ , *J. Combin. Theory Ser. A* **28** (1980), 64–81, doi:10.1016/0097-3165(80)90059-X, [http://dx.doi.org/10.1016/0097-3165\(80\)90059-X](http://dx.doi.org/10.1016/0097-3165(80)90059-X).
- [4] C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of combinatorial designs*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2nd edition, 2007.
- [5] D. Crnković and D. Held, Some Hadamard designs with parameters  $(71, 35, 17)$ , *J. Combin. Des.* **10** (2002), 144–149, doi:10.1002/jcd.996, <http://dx.doi.org/10.1002/jcd.996>.
- [6] J. D. Dixon and B. Mortimer, *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1996, doi:10.1007/978-1-4612-0731-3, <http://dx.doi.org/10.1007/978-1-4612-0731-3>.
- [7] S. Evdokimov and I. Ponomarenko, Permutation group approach to association schemes, *European J. Combin.* **30** (2009), 1456–1476, doi:10.1016/j.ejc.2008.11.005, <http://dx.doi.org/10.1016/j.ejc.2008.11.005>.
- [8] C. D. Godsil and W. J. Martin, Quotients of association schemes, *J. Combin. Theory Ser. A* **69** (1995), 185–199, doi:10.1016/0097-3165(95)90050-0, [http://dx.doi.org/10.1016/0097-3165\(95\)90050-0](http://dx.doi.org/10.1016/0097-3165(95)90050-0).
- [9] W. H. Haemers, *Eigenvalue techniques in design and graph theory*, volume 121 of *Mathematical Centre Tracts*, Mathematisch Centrum, Amsterdam, 1980, dissertation, Technische Hogeschool Eindhoven, Eindhoven, 1979.
- [10] A. Hanaki and K. Uno, Algebraic structure of association schemes of prime order, *J. Algebraic Combin.* **23** (2006), 189–195, doi:10.1007/s10801-006-6923-7, <http://dx.doi.org/10.1007/s10801-006-6923-7>.
- [11] D. Higman, Coherent configurations. I: Ordinary representation theory, *Geom. Dedicata* **4** (1975), 1–32, doi:10.1007/BF00147398.
- [12] D. Higman, Coherent configurations. II: Weights., *Geom. Dedicata* **5** (1976), 413–424, doi:10.1007/BF00150773.

- [13] D. G. Higman, Coherent algebras, *Linear Algebra Appl.* **93** (1987), 209–239, doi:10.1016/S0024-3795(87)90326-0, [http://dx.doi.org/10.1016/S0024-3795\(87\)90326-0](http://dx.doi.org/10.1016/S0024-3795(87)90326-0).
- [14] D. G. Higman, Strongly regular designs of the second kind, *European J. Combin.* **16** (1995), 479–490, doi:10.1016/0195-6698(95)90003-9, [http://dx.doi.org/10.1016/0195-6698\(95\)90003-9](http://dx.doi.org/10.1016/0195-6698(95)90003-9).
- [15] M. Hirasaka, H. Kang and K. Kim, Equitable partitions of flat association schemes, *Graphs Combin.* **24** (2008), 81–89, doi:10.1007/s00373-008-0777-9, <http://dx.doi.org/10.1007/s00373-008-0777-9>.
- [16] M. Hirasaka and R. Sharafadini, Characterization of balanced coherent configurations, *J. Algebra* **324** (2010), 2025–2041, doi:10.1016/j.jalgebra.2010.05.015, <http://dx.doi.org/10.1016/j.jalgebra.2010.05.015>.
- [17] Z. Janko and T. v. Trung, Construction of two symmetric block designs for  $(71, 21, 6)$ , *Discrete Math.* **55** (1985), 327–328, doi:10.1016/S0012-365X(85)80011-X, [http://dx.doi.org/10.1016/S0012-365X\(85\)80011-X](http://dx.doi.org/10.1016/S0012-365X(85)80011-X).
- [18] M. Muzychuk and I. Ponomarenko, On pseudocyclic association schemes, *Ars Math. Contemp.* **5** (2012), 1–25.
- [19] M. Muzychuk and I. Ponomarenko, On quasi-thin association schemes, *J. Algebra* **351** (2012), 467–489, doi:10.1016/j.jalgebra.2011.11.012, <http://dx.doi.org/10.1016/j.jalgebra.2011.11.012>.
- [20] P.-H. Zieschang, *Theory of association schemes*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.