ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 19 (2020) 51–60
https://doi.org/10.26493/1855-3974.2034.dad
(Also available at http://amc-journal.eu)

Association schemes with a certain type of p-subschemes[*]

Wasim Abbas[†], Mitsugu Hirasaka

Department of Mathematics, College of Sciences, Pusan National University,
63 Beon-gil 2, Busandaehag-ro, Geumjung-gu, Busan 609-735, Korea

Received 4 July 2019, accepted 16 July 2020, published online 2 November 2020

Abstract

In this article, we focus on association schemes with some properties derived from the orbitals of a transitive permutation group G with a one-point stabilizer H satisfying $H < N_G(H) < N_G(N_G(H)) \trianglelefteq G$ and $|N_G(N_G(H))| = p^3$ where p is a prime. By a corollary of our main result we obtain some inequality which corresponds to the fact $|G : N_G(N_G(H))| \leq p + 1$.

Keywords: Association schemes, p-schemes.

Math. Subj. Class. (2020): 05E15, 05E30

1 Introduction

Let G be a finite group with a subgroup H which satisfies

$$H < N_G(H) < N_G(N_G(H)) \trianglelefteq G \quad \text{and} \quad |N_G(N_G(H))| = p^3 \tag{1.1}$$

where p is a prime. In this article we focus on association schemes axiom-zing some properties derived from the orbitals of the action of G on G/H.

We shall recall some terminologies to show that the definition of coherent configurations is derived from properties of the binary relations obtained from a permutation group. Let G be a permutation group of a finite set Ω. Then G acts on $\Omega \times \Omega$ by its entry-wise action, i.e.,

$$(\alpha, \beta)^x := (\alpha^x, \beta^x) \quad \text{for } \alpha, \beta \in \Omega \text{ and } x \in G.$$

We denote the set of orbits of the action of G on $\Omega \times \Omega$ by $\mathrm{Inv}(G)$, which satisfies the following conditions:

[*] This work was supported by BK21 Dynamic Math Center, Department of Mathematics at Pusan National University.

[†] Corresponding author.

E-mail addresses: wasimabbas@pusan.ac.kr (Wasim Abbas), hirasaka@pusan.ac.kr (Mitsugu Hirasaka)

(i) The diagonal relation 1_Ω is a union of elements of $\mathrm{Inv}(G)$;

(ii) For each $s \in \mathrm{Inv}(G)$ we have $s^* \in \mathrm{Inv}(G)$ where $s^* := \{(\alpha, \beta) \mid (\beta, \alpha) \in s\}$;

(iii) For all $s, t, u \in \mathrm{Inv}(G)$ we have $\sigma_s\sigma_t = \sum_{u\in S} c_{st}^u \sigma_u$ for $c_{st}^u \in \mathbb{N}$ uniquely determined by s, t, u where σ_u is the adjacency matrix of u, i.e., $(\sigma_u)_{\alpha,\beta} = 1$ if $(\alpha, \beta) \in u$ and $(\sigma_u)_{\alpha,\beta} = 0$ if $(\alpha, \beta) \notin u$.

A *coherent configuration* is a pair (Ω, S) of a finite set Ω and a partition S of $\Omega \times \Omega$ which satisfies the conditions obtained from the above by replacing $\mathrm{Inv}(G)$ by S. We say that a coherent configuration (Ω, S) is *schurian* if $S = \mathrm{Inv}(G)$ for some permutation group G of Ω, and it is *homogeneous* or an *association scheme* if $1_\Omega \in S$ (see [2] and [3] for its background).

Suppose that G has a subgroup H which satisfies (1.1). Then $|H| = p$, $|N_G(H)| = p^2$ and for each $g \in G$ we have the following:

(i) $|HgH|/|H| \in \{1, p\}$ and $|N_G(H)gN_G(H)|/|N_G(H)| \in \{1, p\}$;

(ii) $|HgH|/|H| = 1$ if and only if $g \in N_G(H)$;

(iii) $|N_G(H)gN_G(H)|/|N_G(H)| = 1$ if and only if $g \in N_G(N_G(H))$;

(iv) $N_G(N_G(H))$ is the smallest normal subgroup of G containing H.

Since G acts faithfully and transitively on the set of right cosets of H in G by its right multiplication, it induces a schurian association scheme (Ω, S) where $\Omega = \{Hx \mid x \in G\}$ and $S = \mathrm{Inv}(G)$ such that, for each $s \in S$ we have the following:

(i) $n_s \in \{1, p\}$ where $n_s := c_{ss^*}^{1_\Omega}$;

(ii) $\mathbf{O}_\theta(S)$ forms a group of order p where $\mathbf{O}_\theta(S) := \{s \in S \mid n_s = 1\}$;

(iii) $\mathbf{O}^\theta(S) = \{s \in S \mid ss^*s = s\}$ where $\mathbf{O}^\theta(S)$ is the thin residue of S (see Section 2, [9] or [10] for its definition).

The following is our main result:

Theorem 1.1. *Let (Ω, S) be an association scheme with $\mathbf{O}_\theta(S) < \mathbf{O}^\theta(S)$ such that $n_s \in \{1, p\}$ for each $s \in S$ and $n_{\mathbf{O}^\theta(S)} = p^2$ where p is a prime. Then $|\Omega| \le p^2(p + 1)$.*

In [4] they give a criterion on association schemes whose thin residue $\mathbf{O}^\theta(S)$ induces the subschemes isomorphic to either

$$C_{p^2}, \quad C_p \times C_p \quad \text{or} \quad C_p \wr C_p.$$

Here we denote $(G, \mathrm{Inv}(G))$ by G when G acts on itself by its right multiplication and we denote the wreath product of one scheme (Δ, U) by another scheme (Γ, V) by $(\Delta, U) \wr (\Gamma, V)$, i.e.,

$$(\Delta, U) \wr (\Gamma, V) := (\Delta \times \Gamma, \{1_\Gamma \otimes u \mid u \in U\} \cup \{v \otimes U \mid v \in V \setminus \{1_\Gamma\}\})$$

where

$$1_\Gamma \otimes u := \{((\delta_1, \gamma), (\delta_2, \gamma)) \mid (\delta_1, \delta_2) \in u, \gamma \in \Gamma\} \quad \text{and}$$
$$v \otimes U := \{((\delta_1, \gamma_1), (\delta_2, \gamma_2)) \mid \delta_1, \delta_2 \in \Delta, (\gamma_1, \gamma_2) \in v\}.$$

For the case of $\mathbf{O}^\theta(S) \simeq C_{p^2}$ we can apply the main result in [7] to conclude that (Ω, S) is schurian. For the case of $\mathbf{O}^\theta(S) \simeq C_p \times C_p$ we can say that $|\Omega| \leq p^2(p^2+p+1)$ under the assumption that $n_s = p$ for each $s \in S \setminus \mathbf{O}^\theta(S)$. For the case of $\mathbf{O}^\theta(S) \simeq C_p \wr C_p$ we had no progression for the last five years.

In [6] all association schemes of degree 27 are classified by computational enumeration, and there are three pairs of non-isomorphic association schemes with $\mathbf{O}^\theta(S) \simeq C_3 \wr C_3$ which are algebraic isomorphic. These examples had given an impression that we need some complicated combinatorial argument to enumerate p-schemes (Ω, S) with $\mathbf{O}^\theta(S) \simeq C_p \wr C_p$ and $\{n_s \mid s \in S \setminus \mathbf{O}^\theta(S)\} = \{p\}$. The following reduces our argument to the p-schemes of degree p^3 where an association scheme (Ω, S) is called a p-scheme if $|s|$ is a power of p for each $s \in S$:

Corollary 1.2. *For each p-scheme (Ω, S) with $\mathbf{O}^\theta(S) \simeq C_p \wr C_p$, if $n_s = p$ for each $s \in S \setminus \mathbf{O}^\theta(S)$, then $|\Omega| = p^3$.*

In the proof of Theorem 1.1 the theory of coherent configurations plays an important role through the thin residue extension which is a way of construction of coherent configurations from association schemes (see [5, Theorem 2.1] or [8]) . The following is the kernel of our paper:

Theorem 1.3. *For each coherent configuration (Ω, S) whose fibers are isomorphic to $C_p \wr C_p$, if $|s| = p^3$ for each $s \in S$ with $\sigma_s\sigma_s = 0$, then either $|\Omega| \leq p^2(p+1)$ or $ss^*s = s$ for each $s \in S$.*

In Section 2 we prepare necessary terminologies on coherent configurations. In Section 3 we prove our main results.

2 Preliminaries

Throughout this section, we assume that (Ω, S) is a coherent configuration. An element of Ω and an element of S are called a *point* and a *basis relation*, respectively. Furthermore, $|\Omega|$ and $|S|$ are called the *degree* and *rank* of (Ω, S), respectively. For all $\alpha, \beta \in \Omega$ the unique element in S containing (α, β) is denoted by $r(\alpha, \beta)$. For $s \in S$ and $\alpha \in \Omega$ we set

$$\alpha s := \{\beta \in \Omega \mid (\alpha, \beta) \in s\}.$$

A subset Δ of Ω is called a *fiber* of (Ω, S) if $1_\Delta \in S$. For each $s \in S$, there exists a unique pair (Δ, Γ) of fibers such that $s \subseteq \Delta \times \Gamma$. For fibers Δ, Γ of (Ω, S) we denote the set of $s \in S$ with $s \subseteq \Delta \times \Gamma$ by $S_{\Delta,\Gamma}$, and we set $S_\Delta := S_{\Delta,\Delta}$. It is easily verified that (Δ, S_Δ) is a homogeneous coherent configuration. Now we define the *complex product* on the power set of S as follows: For all subsets T and U of S we set

$$TU := \{s \in S \mid c_{tu}^s > 0 \text{ for some } t \in T \text{ and } u \in U\}$$

where the singleton $\{t\}$ in the complex product is written without its parenthesis.

The following equations are frequently used without any mention:

Lemma 2.1. *Let (Ω, S) be a coherent configuration. Then we have the following:*

(i) *For all $r, s \in S$, if $rs \neq \emptyset$, then $n_r n_s = \sum_{t \in S} c_{rs}^t n_t$;*

(ii) *For all $r, s, t \in S$ we have $|t|c_{rs}^{t^*} = |r|c_{st}^{r^*} = |s|c_{tr}^{s^*}$;*

(iii) *For all* $r, s \in S$ *we have* $|\{t \in S \mid t \in rs\}| \leq \gcd(n_r, n_s)$.

For $T \subseteq S_{\Delta,\Gamma}$ we set

$$n_T := \sum_{t \in T} n_t.$$

Here we mention closed subsets, their subschemes and factor scheme according to the terminologies given in [10]. Let (Ω, S) be an association scheme and $T \subseteq S$. We say that a non-empty subset T of S is *closed* if $TT^* \subseteq T$ where

$$T^* := \{t^* \mid t \in T\},$$

equivalently $\bigcup_{t \in T} t$ is an equivalence relation on Ω whose equivalence classes are

$$\{\alpha T \mid \alpha \in \Omega\}$$

where $\alpha T := \{\beta \in \Omega \mid (\alpha, \beta) \in t \text{ for some } t \in T\}$. Let T be a closed subset of S and $\alpha \in \Omega$. It is well-known (see [9]) that

$$(\Omega, S)_{\alpha T} := (\alpha T, \{t \cap (\alpha T \times \alpha T) \mid t \in T\})$$

is an association scheme, called the *subscheme* of (Ω, S) induced by αT, and that

$$(\Omega, S)^T := (\Omega/T, S/\!\!/T)$$

is also an association scheme where

$$\Omega/T := \{\alpha T \mid \alpha \in \Omega\}, \quad S/\!\!/T = \{s^T \mid s \in S\} \quad \text{and}$$
$$s^T := \{(\alpha T, \beta T) \mid (\gamma, \delta) \in s \text{ for some } (\gamma, \delta) \in \alpha T \times \beta T\},$$

which is called the *factor scheme* of (Ω, S) over T.

We say that a closed subset T is *thin* if $n_t = 1$ for each $t \in T$, and $\mathbf{O}_\theta(S)$ is called the *thin radical* of S, and the smallest closed subset T such that $S/\!\!/T$ is thin is called the *thin residue* of S, which is denoted by $\mathbf{O}^\theta(S)$.

3 Proof of the main theorem

Let (Ω, S) be a coherent configuration whose distinct fibers are $\Omega_1, \Omega_2, \dots, \Omega_m$. For all integers i, j with $1 \leq i, j \leq m$ we set

$$S_{ij} := S_{\Omega_i, \Omega_j} \quad \text{and} \quad S_i := S_{ii}.$$

Throughout this section we assume that $(\Omega_i, S_i) \simeq C_p \wr C_p$ for $i = 1, 2, \dots, m$ where p is a prime and $C_p \wr C_p$ is a unique non-thin p-scheme of degree p^2 up to isomorphism.

For $s \in S$ we say that s is *regular* if $ss^*s = \{s\}$ and we denote by R the set of regular elements in S.

Lemma 3.1. *For each regular element* $s \in S_{ij}$ *with* $n_s = p$ *we have*

$$\sigma_s \sigma_{s^*} = p(\textstyle\sum_{t \in \mathbf{O}_\theta(S_i)} \sigma_t) \quad \textit{and} \quad \sigma_{s^*} \sigma_s = p(\textstyle\sum_{t \in \mathbf{O}_\theta(S_j)} \sigma_t).$$

In particular, $ss^* = \mathbf{O}_\theta(S_i)$ *and* $s^*s = \mathbf{O}_\theta(S_j)$.

Proof. Notice that $\{1_{\Omega_i}\} \subsetneq ss^* \subset S_i$ and $ts = \{s\}$ for each $t \in ss^*$. Since $\{t \in S_i \mid ts = \{s\}\}$ is a closed subset of valency at most n_s, it follows from $(\Omega_i, S_i) \simeq C_p \wr C_p$ that $ss^* = \mathbf{O}_\theta(S_i)$, and hence for each $t \in ss^*$

$$c_{ss^*}^t = c_{st}^s n_{s^*}/n_{t^*} = p.$$

This implies that $\sigma_s\sigma_{s^*} = p(\sum_{t\in\mathbf{O}_\theta(S_i)} \sigma_t)$. By the symmetric argument we have $\sigma_{s^*}\sigma_s = p(\sum_{t\in\mathbf{O}_\theta(S_j)} \sigma_t)$. □

Lemma 3.2. *For each non-regular element $s \in S_{ij}$ with $n_s = p$ we have*

$$\sigma_s\sigma_{s^*} = p\sigma_{1_{\Omega_i}} + \sum_{u\in S_i\setminus\mathbf{O}_\theta(S_i)} \sigma_u \quad \textit{and} \quad \sigma_{s^*}\sigma_s = p\sigma_{1_{\Omega_j}} + \sum_{u\in S_j\setminus\mathbf{O}_\theta(S_j)} \sigma_u.$$

Proof. Notice that $\{t \in S_i \mid ts = \{s\}\} = \{1_{\Omega_i}\}$, otherwise, s is regular or $n_s = p^2$, a contradiction. This implies that the singletons ts with $t \in \mathbf{O}_\theta(S_i)$ are distinct elements of valency p. Since

$$p^2 = |\Omega_j| = \sum_{s\in S_{ij}} n_s \geq \sum_{t\in\mathbf{O}_\theta(S_i)} n_{ts} = p + p + \cdots + p = p^2,$$

it follows that $\mathbf{O}_\theta(S_i)s = S_{ij}$.

We claim that $S_i \setminus \mathbf{O}_\theta(S_i) \subseteq ss^*$. Let $u \in S_i \setminus \mathbf{O}_\theta(S_i)$. Then there exists $t \in \mathbf{O}_\theta(S_i)$ such that $u \in tss^*$ since $u \in S_{ij}s^* = \mathbf{O}_\theta(S_i)ss^*$. This implies that $u = t^*u \subseteq t^*(tss^*) = ss^*$.

By the claim with $p^2 = n_s n_{s^*} = \sum_{t\in S_i} c_{ss^*t} n_t$ and $c_{ss^*1_{\Omega_i}} = n_s = p$ we have the first statement, and the second statement is obtained by the symmetric argument. □

For the remainder of this section we assume that $n_s = p$ for each $s \in \bigcup_{i\neq j} S_{ij}$.

Lemma 3.3. *The set $\bigcup_{s\in R} s$ is an equivalence relation on Ω.*

Proof. Since $1_{\Omega_i} \in S_i \subseteq R$ for $i = 1, 2, \ldots, m$, $\bigcup_{s\in R} s$ is reflexive. Since $ss^*s = \{s\}$ is equivalent to $s^*ss^* = \{s^*\}$, $\bigcup_{s\in R} s$ is symmetric.

Let $\alpha \in \Omega_i$, $\beta \in \Omega_j$ and $\gamma \in \Omega_k$ with $r(\alpha,\beta), r(\beta,\gamma) \in R$. Then we have

$$r(\alpha,\gamma)r(\alpha,\gamma)^* \subseteq r(\alpha,\beta)r(\beta,\gamma)r(\beta,\gamma)^*r(\alpha,\beta)^*.$$

If one of $r(\alpha,\beta)$, $r(\beta,\gamma)$ is thin, then $(\alpha,\gamma)r(\alpha,\gamma)^*$, and hence $r(\alpha,\gamma) \in R$. Now we assume that both of them are non-thin. Since $r(\beta,\gamma)r(\beta,\gamma)^* = \mathbf{O}_\theta(S_j) = r(\alpha,\beta)^*r(\alpha,\beta)$, it follows that

$$r(\alpha,\gamma)r(\alpha,\gamma)^* \subseteq r(\alpha,\beta)r(\alpha,\beta)^* = \mathbf{O}_\theta(S_i).$$

Applying Lemma 3.1 and 3.2 we obtain that $r(\alpha,\gamma)$ is regular, and hence $\bigcup_{s\in R} s$ is transitive. □

Lemma 3.4. *The set $\bigcup_{s\in N} s$ is an equivalence relation on Ω where $N := \bigcup_{i=1}^m S_i \cup (S \setminus R)$.*

Proof. Since $1_{\Omega_i} \in S_i \subseteq N$ for $i = 1, 2, \dots, m$, $\bigcup_{s\in N} s$ is reflexive. By Lemma 3.3, $\bigcup_{s\in R}$ is symmetric, so that $\bigcup_{s\in N} s$ is symmetric.

Let $\alpha \in \Omega_i$, $\beta \in \Omega_j$ and $\gamma \in \Omega_k$ with $r(\alpha, \beta), r(\beta, \gamma) \in N$. Since $\bigcup_{i=1}^m S_i \subseteq R$, it follows from Lemma 3.3 that it suffices to show that

$$r(\alpha, \gamma) \in S \setminus R$$

under the assumption that

$$r(\alpha, \beta), r(\beta, \gamma) \in S \setminus R \quad \text{with } i \neq k.$$

Suppose the contrary, i.e., $r(\alpha, \gamma) \in R$. Then, by Lemma 3.3, $S_{ik} \subseteq R$. Since

$$r(\alpha, \beta)r(\beta, \gamma) \subseteq S_{ik} \subseteq R,$$

it follows that

$$\mathbf{O}_\theta(S_i)r(\alpha, \beta)r(\beta, \gamma) = r(\alpha, \beta)r(\beta, \gamma).$$

On the other hand, we have

$$\mathbf{O}_\theta(S_i)r(\alpha, \beta)r(\beta, \gamma) = S_{ij}r(\beta, \gamma) = S_{ik}.$$

Thus, $r(\alpha, \beta)r(\beta, \gamma) = S_{ik}$. Since $i \neq k$, each element of S_{ik} has valency p, and hence,

$$\sigma_{s_1}\sigma_{s_2} = \sum_{u\in S_{ik}} \sigma_u$$

where $s_1 := r(\alpha, \beta)$ and $s_2 := r(\beta, \gamma)$. By Lemma 3.2,

$$p^2 = \langle \sigma_{s_1}\sigma_{s_2}, \sigma_{s_1}\sigma_{s_2}\rangle = \langle \sigma_{s_1}^*\sigma_{s_1}, \sigma_{s_2}\sigma_{s_2}^*\rangle = p^2 + p(p-1),$$

a contradiction where $\langle\ ,\ \rangle$ is the inner product defined by

$$\langle A, B\rangle := 1/p^2 \mathrm{tr}(AB^*) \quad \text{for all } A, B \in M_\Omega(\mathbb{C}).$$

Therefore, $\bigcup_{s\in N} s$ is transitive. □

Lemma 3.5. *We have either $R = S$ or $N = S$.*

Proof. Suppose $R \neq S$. Let $\alpha, \beta \in \Omega$ with $r(\alpha, \beta) \in R$. Since $R \neq S$, there exists $\gamma \in \Omega$ with $r(\alpha, \gamma) \in N$. Notice that $r(\beta, \gamma) \in R \cup N$. By Lemma 3.3, $r(\beta, \gamma) \in N$, and hence, by Lemma 3.4,

$$r(\alpha, \beta) \in R \cap N = \bigcup_{i=1}^m S_i.$$

Since $\alpha, \beta \in \Omega$ are arbitrarily taken, it follows that

$$R = \bigcup_{i=1}^m S_i \quad \text{and} \quad N = S.$$ □

Lemma 3.6. *Suppose that $S = N$ and $s_1 \in S_{ij}, s_2 \in S_{jk}$ and $s_3 \in S_{ik}$ with distinct i, j, k. Then $\sigma_{s_1}\sigma_{s_2} = \sigma_{s_3}(\sum_{t\in\mathbf{O}_\theta(S_k)} a_t\sigma_t)$ for some non-negative integers a_t with $\sum_{t\in\mathbf{O}_\theta(S_k)} a_t = p$, $\sum_{t\in\mathbf{O}_\theta(S_k)} a_t^2 = 2p - 1$ and for each $u \in \mathbf{O}_\theta(S_k) \setminus \{1_{\Omega_k}\}$, $\sum_{t\in\mathbf{O}_\theta(S_k)} a_t a_{tu} = p - 1$.*

Proof. Since $s_1s_2 \subseteq S_{ij} = s_3\mathbf{O}_\theta(S_k)$, $\sigma_{s_1}\sigma_{s_2} = \sum_{t\in\mathbf{O}_\theta(S_k)} a_t\sigma_{s_3t}$ for some non-negative integers a_t. Since $\sigma_{s_3t} = \sigma_{s_3}\sigma_t$ and

$$p^2 = n_{s_1}n_{s_2} = \sum_{t\in\mathbf{O}_\theta(S_k)} a_t n_{s_3t} = p\sum_{t\mathbf{O}_\theta(S_j)} a_t,$$

it remains to show the last two equalities on a_t with $t \in \mathbf{O}_\theta(S_j)$. Expanding $\sigma^*_{s_2}\sigma^*_{s_1}\sigma_{s_1}\sigma_{s_2}$ by two ways we obtain from Lemma 3.2 that

$$(2p^2-p)\sigma_{1_{\Omega_j}} + (p^2-p)\sum_{t\in\mathbf{O}_\theta(S_j)\setminus\{1_{\Omega_j}\}} \sigma_t + (p^2-2p)\sum_{u\in S_j\setminus\mathbf{O}_\theta(S_j)} \sigma_u$$
$$= \sum_{t\in\mathbf{O}_\theta(S_k)} a_t\sigma^*_t\sigma^*_{s_3}\sigma_{s_3}\sum_{t\in\mathbf{O}_\theta(S_k)} a_t\sigma_t.$$

Therefore, we conclude from Lemma 3.2 that

$$p\sum_{t\in\mathbf{O}_\theta(S_k)} a_t^2 = 2p^2 - p \quad\text{and}\quad p\sum_{t\in\mathbf{O}_\theta(S_k)} a_t a_{tu} = p^2 - p$$

for each $u \in \mathbf{O}_\theta(S_k)$ with $u \neq 1_{\Omega_k}$. □

For the remainder of this section we assume that

$$S = N.$$

For $i = 1, 2, \ldots, m$ we take $\alpha_i \in \Omega_i$ and we define $t_i \in S_i$ such that $t_1 \in \mathbf{O}_\theta(S_1)\setminus\{1_{\Omega_1}\}$, and for $i = 2, 3, \ldots, m$, t_i is a unique element in $\mathbf{O}_\theta(S_i)$ with $r(\alpha_1t_1, \alpha_it_i) = r(\alpha_1, \alpha_i)$. Then C_p acts semi-regularly on Ω such that

$$\Omega \times C_p \to \Omega, \quad (\beta_i, t^j) \mapsto \beta_i t_i^j,$$

where $C_p = \langle t\rangle$ and β_i is an arbitrary element in Ω_i.

Lemma 3.7. *The above action acts semi-regularly on Ω as an automorphism of* (Ω, S).

Proof. Since C_p acts regularly on each of geometric coset of $\mathbf{O}_\theta(S_i)$ for $i = 1, 2, \ldots, m$, the action is semi-regular on Ω. By the definition of $\{t_i\}$, it is straightforward to show that $r(\alpha_1, \alpha_i)$ is fixed by the action on $\Omega \times \Omega$, and hence each element of $\bigcup_{j=2}^m S_{1j} \cup S_{j1}$ is also fixed since $S_{1j} = \mathbf{O}_\theta(S_1)r(\alpha_1, \alpha_j)$. Let $s \in S_{ij}$with $2 \leq i, j$. Notice that $r(\alpha_i, \alpha_1)r(\alpha_1, \alpha_j)$ is a proper subset of S_{ij} by Lemma 3.6. This implies that s is obtained as the intersection of some of $t_i^k r(\alpha_i, \alpha_1)r(\alpha_1, \alpha_j)$ with $0 \leq k \leq p-1$, and hence s is fixed. □

For each $i = 1, 2, \ldots, m$ we take $\{\alpha_{ik} \mid k = 1, 2, \ldots, m\}$ to be a complete set of representatives with respect to the equivalence relation $\bigcup_{t\in\mathbf{O}_\theta(S_i)} t$ on Ω_i.

Lemma 3.8. *For each $s \in S_{ij}$ with $i \neq j$ and all $k, l = 1, 2, \ldots, p$ there exists a unique $h(s)_{kl} \in \mathbb{Z}_p$ such that $r(\alpha_{ik}, \alpha_{jl}t^{h(s)_{kl}}) = s$. Moreover, if $s_1 \in S_{ij}$ and $t^a \in \mathbf{O}_\theta(S_k)$ with $s_1 = st^a$, then $h(s_1)_{kl} = h(s)_{kl} + a$ for all $k, l = 1, 2, \ldots, m$.*

Proof. Since $\mathbf{O}_\theta(S_j)$ acts regularly on S_{ij} by its right multiplication, the first statement holds. The second statement is obtained by a direct computation. □

Lemma 3.9. *For each $s \in S_{ij}$ with $i \neq j$ and all $k, l = 1, 2, \ldots, p$ we have*

$$s \cap (\alpha_{ik}\mathbf{O}_\theta(S_i) \times \alpha_{jl}\mathbf{O}_\theta(S_j)) = \{(\alpha_{ik}t_i^a, \alpha_{jl}t_j^b) \mid b - a = h(s)_{kl}\}.$$

Proof. Notice that

$$r(\alpha_{ik}t_i^a, \alpha_{jl}t_j^b) = (t_i^a)^* r(\alpha_{ik}, \alpha_{jl}) t_j^b = r(\alpha_{ik}, \alpha_{jl}) t_j^{b-a}.$$

Since $r(\alpha_{ik}, \alpha_{jl}t^{h(s)_{kl}}) = s$ by Lemma 3.8, it follows that $r(\alpha_{ik}t_i^a, \alpha_{jl}t_j^b) = s$ if and only if $b - a = h(s)_{kl}$. □

Proposition 3.10. *For each $s \in S_{ij}$ with $i \neq j$ the matrix $(h(s)_{kl}) \in M_{p\times p}(\mathbb{Z}_p)$ satisfies that, for all distinct $k_1, k_2 \in \{1, 2, \ldots, p\}$,*

$$\{h(s)_{k_1,l} - h(s)_{k_2,l} \mid l = 1, 2, \ldots, p\} = \mathbb{Z}_p.$$

In other word the matrix is a generalized Hadamard matrix of degree p over $\mathbb{Z}_p$, equivalently, the matrix $(\xi^{h(s)_{kl}}) \in M_{p\times p}(\mathbb{C})$ is a complex Hadamard matrix of Butson type (p, p) where ξ is a primitive p-th root of unity.

Proof. Notice that, for all distinct k, l, by Lemma 3.9,

$$\{\gamma \in \Omega \mid r(\alpha_{ik}t_i^a, \gamma) = r(\alpha_{il}t_i^b, \gamma) = s\}$$

equals

$$\bigcup_{r=1}^{p} \{\alpha_{jr}t_j^c \mid c - a = h(s)_{kr}, c - b = h(s)_{lr}\}.$$

Since the upper one is a singleton by Lemma 3.2, there exists a unique $r \in \{1, 2, \ldots, p\}$ such that $b - a = h(s)_{kr} - h(s)_{lr}$. Since a and b are arbitrarily taken, the first statement holds.

The second statement holds since $\sum_{i=0}^{p-1} x^i$ is the minimal polynomial of ξ over $\mathbb{Q}$. □

We shall write the matrix $(\xi^{h(s)_{kl}})$ as $H(s)$. For $s \in S_{ij}$ with $i \neq j$, the restriction of σ_s to $\Omega_i \times \Omega_j$ can be viewed as a $(p \times p)$-matrix whose (k, l)-entry is the matrix $P_i^{h(s)_{kl}}$ where P_i is the permutation matrix corresponding to the mapping $\beta_i \mapsto \beta_i t_i$ where we may assume that $P_i = P_j$, say P, for all $i, j = 1, 2, \ldots, m$ by Lemma 3.7. Notice that $H(s)$ is obtained from $(P^{h(s)_{kl}})$ by sending $P^{h(s)_{kl}}$ to $\xi^{h(s)_{kl}}$.

Proposition 3.11. *For all $s_1 \in S_{ij}$, $s_2 \in S_{jk}$ and $s_3 \in S_{ik}$ with distinct i, j, k we have $H(s_1)H(s_2) = \alpha H(s_3)$ for some $\alpha \in \mathbb{C}$ with $|\alpha| = \sqrt{p}$.*

Proof. By Lemma 3.6, $H(s_1)H(s_2) = H(s_3)(\sum_{i=0}^{p-1} a_i\xi^i)$ for some $a_i \in \mathbb{Z}$ where $a_i = c_{t_k^i}$. Thus, it suffices to show that $|(\sum_{i=0}^{p-1} a_i\xi^i)|^2 = p$. By Lemma 3.6, the left hand side equals

$$\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_i a_j \xi^{i-j} = \sum_{i=0}^{p-1} a_i^2 + \sum_{i=1}^{p-1}\sum_{j=0}^{p-1} a_j a_{i+j}\xi^i = (2p-1) + (p-1)(-1) = p. \qquad \square$$

Corollary 3.12. *Let $s_i := r(\alpha_1, \alpha_i)$ for $i = 2, 3, \ldots, m$ and $\mathbf{B}_i$ denote the basis consisting of the rows of $H(s_i)$, $i = 2, 3, \ldots, m$, and $\mathbf{B}_1$ be the standard basis. Then $\{\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m\}$ is a mutually unbiased bases for $\mathbb{C}^p$, and $m \leq p + 1$.*

Proof. The first statement is an immediate consequence of Proposition 3.10, and the second statement follows from a well-known fact that the number of mutually unbiased bases for $\mathbb{C}^n$ is at most $n + 1$ (see [1]). □

Proof of Theorem 1.3. Suppose that $R \neq S$. Then $N = S$ and the theorem follows from Corollary 3.12. □

Proof of Theorem 1.1. Since $n_{\mathbf{O}^\theta(S)} = p^2$ and $\mathbf{O}_\theta(S) < \mathbf{O}^\theta(S)$, it follows from [5, Theorem 2.1] (or see [8]) that the thin residue extension of (Ω, S) is a coherent configuration with all fibers isomorphic to $C_p \wr C_p$ such that each basic relation out of the fibers has valency p.

We claim that $S = N$. Otherwise, $S = R$, which implies that $\langle ss^* \mid s \in S \rangle$ has valency p. Since $\mathbf{O}^\theta(S) = \langle ss^* \mid s \in S \rangle$ (see [9]), it contradicts that $\mathbf{O}^\theta(S)$ has valency p^2.

By the claim, $S = N$. Since the number of fibers of the thin residue extension of (Ω, S) equals $|\Omega / \mathbf{O}^\theta(S)|$, the theorem follows from Theorem 1.3. □

Proof of Corollary 1.2. Since (Ω, S) is a p-scheme and $\mathbf{O}^\theta(S) \simeq C_p \times C_p$, $|\Omega|$ is a power of p greater than p^2. By Theorem 1.1, $|\Omega| \leq (p + 1)p^2$, and hence, $|\Omega| = p^3$. □

ORCID iDs

Wasim Abbas https://orcid.org/0000-0002-1706-1462

References

[1] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, A new proof for the existence of mutually unbiased bases, *Algorithmica* **34** (2002), 512–528, doi:10.1007/s00453-002-0980-7.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*, The Benjamin/Cummings Publishing, Menlo Park, CA, 1984.

[3] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Springer-Verlag, Berlin, 1989, doi:10.1007/978-3-642-74341-2.

[4] J. R. Cho, M. Hirasaka and K. Kim, On p-schemes of order p^3, *J. Algebra* **369** (2012), 369–380, doi:10.1016/j.jalgebra.2012.06.026.

[5] S. A. Evdokimov and I. N. Ponomarenko, Schemes of relations of the finite projective plane, and their extensions, *Algebra i Analiz* **21** (2009), 90–132, http://mi.mathnet.ru/aa996, *St. Petersburg Math. J.* **21** (2010), 65–93, doi:10.1090/s1061-0022-09-01086-3.

[6] A. Hanaki and I. Miyamoto, Classification of association schemes of small order, *Discrete Math.* **264** (2003), 75–80, doi:10.1016/s0012-365x(02)00551-4.

[7] M. Hirasaka and P.-H. Zieschang, Sufficient conditions for a scheme to originate from a group, *J. Comb. Theory Ser. A* **104** (2003), 17–27, doi:10.1016/s0097-3165(03)00104-3.

[8] M. Muzychuk and I. Ponomarenko, On quasi-thin association schemes, *J. Algebra* **351** (2012), 467–489, doi:10.1016/j.jalgebra.2011.11.012.

[9] P.-H. Zieschang, *An Algebraic Approach to Association Schemes*, volume 1628 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1996, doi:10.1007/bfb0097032.

[10] P.-H. Zieschang, *Theory of Association Schemes*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005, doi:10.1007/3-540-30593-9.