J Algebr Comb (2008) 27: 307–316
DOI 10.1007/s10801-007-0090-3

Commutativity of association schemes of prime square order having non-trivial thin closed subsets

Akihide Hanaki · Mitsugu Hirasaka · Katsuhiro Uno

Received: 26 December 2006 / Accepted: 24 July 2007 / Published online: 1 September 2007

Abstract Through a study of the structure of the modular adjacency algebra over a field of positive characteristic p for a scheme of prime order p and utilizing the fact that every scheme of prime order is commutative, we show that every association scheme of prime square order having a non-trivial thin closed subset is commutative.

Keywords Association scheme · Closed subset · Character

Mathematics Subject Classification (2000) Primary 05E30

1 Introduction

In [7], the first and the third authors proved that all association schemes of prime order are commutative. It is natural to ask whether association schemes of prime square order are commutative. To our knowledge, there is no known non-commutative association scheme of prime square order. Only a certain class of association schemes of

The second author was supported by Korea Research Foundation Grant (KRF-2006-003-00008).

A. Hanaki (✉)
Faculty of Science, Shinshu University, Matsumoto, 390-8621, Japan
e-mail: hanaki@math.shinshu-u.ac.jp

M. Hirasaka
Department of Mathematics, College of Science, Pusan National University Kumjung, Pusan 609-735, Republic of Korea
e-mail: hirasaka@pusan.ac.kr

K. Uno
Department of Mathematical Sciences, Osaka Kyoiku University, Kashiwara, Osaka, 582-8582, Japan
e-mail: uno@cc.osaka-kyoiku.ac.jp

prime square order has been shown to be commutative. If a scheme of prime square order is Schurian, then the scheme is commutative (Theorem 4.6). Also if a scheme of prime square order has a proper strongly normal closed subset, then the first author showed in [6] that it is commutative. In this article, we consider a scheme of prime square order having a non-trivial thin closed subset, and show that the scheme is commutative (Theorem 5.4). The assumption is very strong and we can use many facts on finite groups since a thin closed subset can be considered as a finite group.

In Section 3, we determine the structure of the modular adjacency algebra, that is the adjacency algebra over a field of positive characteristic p, of a scheme of prime order p. In Section 4, we consider a combinatorial structure of schemes of prime square order having non-trivial thin closed subsets. We show that there are two types of structures, and that one of them gives commutative schemes. In Section 5, we prove that the other type gives also commutative schemes. To see this, the results in modular representation theory obtained in Section 3 are useful.

2 Preliminaries

Throughout this paper, let (X, S) denote an *association scheme* in the sense of a finite scheme in [9]. An association scheme is called a *scheme* in short. All unexplained notations and symbols used in what follows may be found in [9] or [7]. For $s \in S$, we put $s^* = \{(y, x) \mid (x, y) \in s\}$. Then s^* is also an element of S. The *adjacency matrix* of $s \in S$ will be denoted by σ_s. Namely σ_s is a matrix whose rows and columns are indexed by the elements of X and $(\sigma_s)_{xy} = 1$ if $(x, y) \in s$ and $(\sigma_s)_{xy} = 0$ otherwise. For $s, t, u \in S$, the *structure constant* will be denoted by a_{stu}, namely $\sigma_s\sigma_t = \sum_{u\in S} a_{stu}\sigma_u$. The *valency* of $s \in S$ will be denoted by n_s, which is given by a_{ss^*1}. We call the cardinality of X the *order* of (X, S). For $s, t \in S$, we define the *complex product* of s and t by $st = \{u \in S \mid a_{stu} \neq 0\}$.

Let A and B be subsets of S. We write σ_A for $\sum_{s\in A} \sigma_s$, n_A for $\sum_{s\in A} n_s$, and a_{ABu} for $\sum_{s\in A}\sum_{t\in B} a_{stu}$. We also use $a_{A,B,u}$ instead of a_{ABu}. Obviously $\sigma_A\sigma_B = \sum_{u\in S} a_{ABu}\sigma_u$. The complex product of A and B is defined by $AB = \{u \in S \mid a_{ABu} \neq 0\} = \bigcup_{s\in A}\bigcup_{t\in B} st$. We also use the notations sA and As instead of $\{s\}A$ and $A\{s\}$ for $s \in S$, respectively. Since the associative law holds for complex products [9, Lemma 1.3.1], we can use the notation AsB, and so on. A nonempty subset T of S is called a *closed subset* if $TT = T$. A closed subset T of S is called a *normal closed subset* if $sT = Ts$ for any $s \in S$.

An element $s \in S$ is said to be *thin* if $n_s = 1$. A closed subset T of S is called a *thin closed subset* if every element of T is thin. A thin closed subset can be considered as a finite group (see [9, Preface]).

By the definition of a scheme, $\bigoplus_{s\in S} \mathbb{Z}\sigma_s$ is a matrix ring. For any commutative unitary ring R, we can define an R-algebra $R \otimes_{\mathbb{Z}} (\bigoplus_{s\in S} \mathbb{Z}\sigma_s)$. We call this R-algebra the *adjacency algebra* of (X, S) over R and write it RS (In [9], Zieschang calls this ring the *scheme ring*). A scheme (X, S) is said to be *commutative* if the ring $\mathbb{Z}S$ is a commutative ring.

Now we consider the complex adjacency algebra $\mathbb{C}S$. It is known that $\mathbb{C}S$ is a semisimple algebra [9, Theorem 9.1.5(ii)]. We write $\mathrm{Irr}(S)$ for the set of all irreducible characters of $\mathbb{C}S$. Every scheme (X, S) has the *trivial character* $1_S : \sigma_s \mapsto n_s$.

We write $\mathrm{Irr}^*(S)$ for $\mathrm{Irr}(S) - \{1_S\}$. The matrix $(\chi(\sigma_s))_{\chi\in\mathrm{Irr}(S), s\in S}$ is called the *character table* of (X, S). We say that a field K of characteristic zero is a *splitting field* of (X, S) if K is a splitting field of the $\mathbb{Q}$-algebra $\mathbb{Q}S$. If (X, S) is commutative, then K is a splitting field if and only if K contains all character values $\chi(\sigma_s)$, $\chi \in \mathrm{Irr}(S)$, $s \in S$. So $\mathbb{Q}(\chi(\sigma_s) \mid \chi \in \mathrm{Irr}(S), s \in S)$ is the minimal splitting field of (X, S).

3 Modular adjacency algebras of schemes of prime order

In this section, we suppose (X, S) is a scheme of prime order p and determine the structure of the adjacency algebra of (X, S) over a field of characteristic p. Put $|S| = d + 1$ and $k = (p-1)/d$. Then, it is shown in [7] that $n_s = k$ for every $1 \neq s \in S$. Also all non-trivial irreducible characters of S are algebraically conjugate. Let K be the minimal splitting field of (X, S). Since (X, S) is commutative, we have $K = \mathbb{Q}(\chi(\sigma_s) \mid \chi \in \mathrm{Irr}(S), s \in S)$. Obviously $K/\mathbb{Q}$ is a Galois extension and we put G the Galois group of this extension. Then [7, Lemma 3.1] shows that G acts on $\mathrm{Irr}^*(S)$ transitively. Let $\mathfrak{P}$ be a prime ideal of the ring of integers of K lying above $p\mathbb{Z}$. In this section, the letter T is used to denote the inertia group of $\mathfrak{P}$, whereas T denotes a subset of S in the other sections. Let K_T be the inertia field of $\mathfrak{P}$. Since p is unramified in $K_T/\mathbb{Q}$, the same argument as [7, Lemma 3.1] shows that T acts on $\mathrm{Irr}^*(S)$ transitively.

Lemma 3.1 *The following statements hold*:

(1) *The Galois group G acts on* $\mathrm{Irr}^*(S)$ *faithfully.*
(2) *The Galois group G is a p'-group, a finite group of order not divisible by p.*
(3) *The inertia group T is cyclic.*

Proof If an element in G stabilizes all irreducible characters, then it stabilizes all elements in K. This shows that (1) holds. By (1), G is isomorphic to a subgroup of the symmetric group on $\mathrm{Irr}^*(S)$. Since $|\mathrm{Irr}^*(S)| = d < p$, it is a p'-group and (2) holds. In general, the inertia group T has a normal Sylow p-subgroup with a cyclic quotient group [8, Theorem 5.34 and Proposition 6.6]. But, in our case, T is a p'-group, so it is a cyclic group and (3) holds. □

We fix $\chi \in \mathrm{Irr}^*(S)$, and put $H = \{\tau \in G \mid \chi^\tau = \chi\}$. Then $K_H = \mathbb{Q}(\chi(\sigma_s) \mid s \in S)$ is the Galois correspondent of H.

Lemma 3.2 *The following statements hold*:

(1) $HT = G$.
(2) $H \cap T = 1$.
(3) $|T| = \dim_{\mathbb{Q}} K_H = d$. *Thus the ramification index of $\mathfrak{P}$ in $K/\mathbb{Q}$ is d.*
(4) *The prime ideal $\mathfrak{P}$ is unramified in the extension K/K_H.*

Proof For any $\rho \in G$, there exists $\tau \in T$ such that $\chi^\rho = \chi^\tau$. Then $\rho = (\rho\tau^{-1})\tau$ and $\rho\tau^{-1} \in H$. This means (1) holds. Suppose $\rho \in H \cap T$. For any $\varphi \in \mathrm{Irr}^*(S)$, there exists $\tau \in T$ such that $\varphi = \chi^\tau$. Then, since T is cyclic,

$$\varphi^\rho = \chi^{\tau\rho} = \chi^{\rho\tau} = \chi^\tau = \varphi.$$

This means that ρ stabilizes all irreducible characters and it must be the identity. This shows (2) holds. By (1) and (2), we have $|T| = |G|/|H|$. Since G is a permutation group on d elements and H is a stabilizer, we have $|T| = d$ and (3) holds. Now (4) is clear since the inertia group of $\mathfrak{P}$ in K/K_H is $H \cap T = 1$. □

We write the $\mathfrak{P}$-valuation of K by $\nu_{\mathfrak{P}}$. Since the ramification index of $\mathfrak{P}$ is d, we have $\nu_{\mathfrak{P}}(p) = d$. Let P denote the character table of (X, S). Note that we regard P as a matrix.

Lemma 3.3 *We have* $\nu_{\mathfrak{P}}(\det P) = d(d+1)/2$.

Proof By [7], the Frame number $\mathcal{F}(S)$ is equal to p^{d+1}. Also, by [1, p. 74], $(\det P)\overline{(\det P)} = \mathcal{F}(S)$. The complex conjugate induces a permutation of the rows of P. So $\det P$ is real or purely imaginary. This shows the statement. □

Consider the localization of K by $\mathfrak{P}$, and write the ring of $\mathfrak{P}$-integers by $\mathcal{O}_{\mathfrak{P}}$.

Lemma 3.4 *There exists an element* $s \in S$ *such that* $\nu_{\mathfrak{P}}(\chi(\sigma_s) - k) = 1$.

Proof Let τ be a generator of the cyclic group T. Since the action of T on $\mathrm{Irr}^*(S)$ is regular, we can write

$$P = \begin{pmatrix} 1 & k & k & \cdots & k \\ 1 & \beta_1 & \beta_2 & \cdots & \beta_d \\ 1 & {\beta_1}^\tau & {\beta_2}^\tau & \cdots & {\beta_d}^\tau \\ & \cdots & \cdots & \cdots & \\ 1 & {\beta_1}^{\tau^{d-1}} & {\beta_2}^{\tau^{d-1}} & \cdots & {\beta_d}^{\tau^{d-1}} \end{pmatrix},$$

for some $\beta_i \in \mathcal{O}_{\mathfrak{P}}$ $(i = 1, \ldots, d)$. Put $\gamma_i = \beta_i - k$. Then

$$\det P = \begin{vmatrix} 1 & k & k & \cdots & k \\ 0 & \beta_1 - k & \beta_2 - k & \cdots & \beta_d - k \\ 0 & {\beta_1}^\tau - k & {\beta_2}^\tau - k & \cdots & {\beta_d}^\tau - k \\ & \cdots & \cdots & \cdots & \\ 0 & {\beta_1}^{\tau^{d-1}} - k & {\beta_2}^{\tau^{d-1}} - k & \cdots & {\beta_d}^{\tau^{d-1}} - k \end{vmatrix}$$

$$= \begin{vmatrix} \gamma_1 & \gamma_2 & \cdots & \gamma_d \\ {\gamma_1}^\tau & {\gamma_2}^\tau & \cdots & {\gamma_d}^\tau \\ & \cdots & \cdots & \\ {\gamma_1}^{\tau^{d-1}} & {\gamma_2}^{\tau^{d-1}} & \cdots & {\gamma_d}^{\tau^{d-1}} \end{vmatrix}.$$

We fix $\pi \in \mathcal{O}_{\mathfrak{P}}$ such that $\nu_{\mathfrak{P}}(\pi) = 1$. Since τ is contained in the inertia group of $\mathfrak{P}$, we have $\nu_{\mathfrak{P}}(\pi^{\tau^j}) = 1$ for $j \in \{0, 1, \ldots, d-1\}$. Define $\gamma_{i,1}$ by $\pi\gamma_{i,1} = \gamma_i$.

By [4], β_i is congruent to k modulo $\mathfrak{P}$. This means that $\gamma_{i,1} \in \mathcal{O}_{\mathfrak{P}}$. Since τ is in the inertia group, we can define $\gamma_{i,j} \in \mathcal{O}_{\mathfrak{P}}$ inductively by

$$\pi \gamma_{i,j+1} = {\gamma_{i,j}}^{\tau} - \gamma_{i,j} \quad (j = 1, 2, \ldots, d-1).$$

Then

$$\begin{vmatrix} \gamma_1 & \gamma_2 & \cdots & \gamma_d \\ {\gamma_1}^{\tau} & {\gamma_2}^{\tau} & \cdots & {\gamma_d}^{\tau} \\ & \cdots & \cdots & \\ {\gamma_1}^{\tau^{d-1}} & {\gamma_2}^{\tau^{d-1}} & \cdots & {\gamma_d}^{\tau^{d-1}} \end{vmatrix}$$

$$= \prod_{i=0}^{d-1} \pi^{\tau^i} \begin{vmatrix} \gamma_{1,1} & \gamma_{2,1} & \cdots & \gamma_{d,1} \\ {\gamma_{1,1}}^{\tau} & {\gamma_{2,1}}^{\tau} & \cdots & {\gamma_{d,1}}^{\tau} \\ & \cdots & \cdots & \\ {\gamma_{1,1}}^{\tau^{d-1}} & {\gamma_{2,1}}^{\tau^{d-1}} & \cdots & {\gamma_{d,1}}^{\tau^{d-1}} \end{vmatrix}$$

$$= \prod_{i=0}^{d-1} \pi^{\tau^i} \begin{vmatrix} \gamma_{1,1} & \gamma_{2,1} & \cdots & \gamma_{d,1} \\ {\gamma_{1,1}}^{\tau} - \gamma_{1,1} & {\gamma_{2,1}}^{\tau} - \gamma_{2,1} & \cdots & {\gamma_{d,1}}^{\tau} - \gamma_{d,1} \\ & \cdots & \cdots & \\ {\gamma_{1,1}}^{\tau^{d-1}} - {\gamma_{1,1}}^{\tau^{d-2}} & {\gamma_{2,1}}^{\tau^{d-1}} - {\gamma_{2,1}}^{\tau^{d-2}} & \cdots & {\gamma_{d,1}}^{\tau^{d-1}} - {\gamma_{d,1}}^{\tau^{d-2}} \end{vmatrix}$$

$$= \prod_{i=0}^{d-1} \pi^{\tau^i} \begin{vmatrix} \gamma_{1,1} & \gamma_{2,1} & \cdots & \gamma_{d,1} \\ \pi \gamma_{1,2} & \pi \gamma_{2,2} & \cdots & \pi \gamma_{d,2} \\ & \cdots & \cdots & \\ \pi^{\tau^{d-2}} {\gamma_{1,2}}^{\tau^{d-2}} & \pi^{\tau^{d-2}} {\gamma_{2,2}}^{\tau^{d-2}} & \cdots & \pi^{\tau^{d-2}} {\gamma_{d,2}}^{\tau^{d-2}} \end{vmatrix}$$

$$= \prod_{i=0}^{d-1} \pi^{\tau^i} \prod_{i=0}^{d-2} \pi^{\tau^i} \begin{vmatrix} \gamma_{1,1} & \gamma_{2,1} & \cdots & \gamma_{d,1} \\ \gamma_{1,2} & \gamma_{2,2} & \cdots & \gamma_{d,2} \\ & \cdots & \cdots & \\ {\gamma_{1,2}}^{\tau^{d-2}} & {\gamma_{2,2}}^{\tau^{d-2}} & \cdots & {\gamma_{d,2}}^{\tau^{d-2}} \end{vmatrix}.$$

Repeat this process. Then we have

$$\det P = \begin{vmatrix} \gamma_1 & \gamma_2 & \cdots & \gamma_d \\ {\gamma_1}^{\tau} & {\gamma_2}^{\tau} & \cdots & {\gamma_d}^{\tau} \\ & \cdots & \cdots & \\ {\gamma_1}^{\tau^{d-1}} & {\gamma_2}^{\tau^{d-1}} & \cdots & {\gamma_d}^{\tau^{d-1}} \end{vmatrix} = \prod_{\ell=0}^{d-1} \prod_{i=0}^{\ell} \pi^{\tau^i} \begin{vmatrix} \gamma_{1,1} & \gamma_{2,1} & \cdots & \gamma_{d,1} \\ \gamma_{1,2} & \gamma_{2,2} & \cdots & \gamma_{d,2} \\ & \cdots & \cdots & \\ \gamma_{1,d} & \gamma_{2,d} & \cdots & \gamma_{d,d} \end{vmatrix}.$$

By Lemma 3.3, $\nu_{\mathfrak{P}}(\det P) = d(d+1)/2$. So, if $\nu_{\mathfrak{P}}(\gamma_i) > 1$ for all $i \in \{1, \cdots, d\}$, then we can write $\gamma_i = \pi^2 \gamma'_{i,1}$ for some $\gamma'_{i,1} \in \mathcal{O}_{\mathfrak{P}}$ for every $i \in \{1, 2, \cdots, d\}$. This gives a contradiction. We have $\nu_{\mathfrak{P}}(\gamma_i) = 1$ for some i. The corresponding element in S satisfies the required condition. □

Now we can show the main theorem in this section.

Theorem 3.5 *Let F be a field of positive characteristic p, and (X, S) an association scheme of order p. Then there exists $s \in S$ such that $FS = F[\overline{\sigma_s}] \cong F[x]/(x^{d+1})$, where $\overline{\sigma_s}$ is the natural image of σ_s in FS.*

Proof Let $\chi \in \mathrm{Irr}^*(S)$. By Lemma 3.4, there exists $s \in S$ such that $\nu_{\mathfrak{P}}(\chi(\sigma_s) - k) = 1$. Put $\gamma = \sigma_s - k\sigma_1 \in \mathbb{Z}S$. Then $\nu_{\mathfrak{P}}(\chi(\gamma)^{d-1}) = d - 1$, so $\gamma^{d-1} \notin p\mathbb{Z}S$. This means $\overline{\gamma}^{d-1} \neq 0$ in FS. By [4], $\overline{\gamma}$ is contained in the Jacobson radical of FS. So, if we prove $\overline{\gamma}^d \neq 0$, then the statement holds.

By [4], FS is a local symmetric algebra, so its socle is $F(\sum_{s\in S} \sigma_s)$. If FS is not a serial algebra, then $\overline{\gamma}^{d-1}$ is in the socle. This means $\gamma^{d-1} \in \mathbb{Z}(\sum_{s\in S} \sigma_s) + p\mathbb{Z}S$. But then $\chi(\gamma)^{d-1} \in p\mathcal{O}_{\mathfrak{P}}$ and this is a contradiction. So FS is serial and $\overline{\gamma}^d \neq 0$. □

4 Combinatorial structures

In this section, we consider combinatorial structures of schemes of prime square order having nontrivial thin closed subsets. We show that there are two types of structures and for one of them the scheme is commutative. Commutativity of the other type is considered in the next section. First, we give a general fact.

Theorem 4.1 *Let (X, S) be an association scheme having a closed subset T. Suppose n_S/n_T is the smallest prime divisor of n_S. Then T is a normal closed subset.*

Proof By [9, Lemma 2.3.1(1)], we have $\sigma_T\sigma_s = a_{T,s,s}\sigma_{Ts}$ and $\sigma_{Ts}\sigma_T = a_{Ts,T,s}\sigma_{TsT}$ for any $s \in S$. These show that $n_T n_s n_T = a_{T,s,s} a_{Ts,T,s} n_{TsT}$. So we have

$$n_{s^T} = \frac{n_{TsT}}{n_T} = \frac{n_T n_s}{a_{T,s,s} a_{Ts,T,s}}.$$

For any $x \in X$, xs^* is partitioned into $xs^* \cap yT$ where y ranges in xs^* and $|xs^* \cap yT| = a_{s^*,T,s^*} = a_{T,s,s}$. This shows that $a_{T,s,s} \mid n_s$. Since $n_{s^T} < n_{S/\!/T} = n_S/n_T$ and we are assuming that n_S/n_T is the smallest prime divisor of n_S, we have $n_T \mid a_{Ts,T,s}$. Especially $n_T \le a_{Ts,T,s}$. For $x, y \in X$ such that $(x, y) \in s$, $a_{Ts,T,s} = |xTs \cap yT| \le |yT| = n_T$. So $xTs \supset \bigcup_{y\in xs} yT \supset xsT$. By using the equation $n_T n_s n_T = a_{s,T,s} a_{T,sT,s} n_{TsT}$, we have $xsT \supset xTs$ similarly. Hence $xsT = xTs$ and $sT = Ts$. Since $s \in S$ is arbitrarily taken, we can conclude that T is a normal closed subset. □

In what follows in this section, we consider a scheme (X, S) of prime square order p^2 which has a nontrivial thin closed subset T. If $n_T = p^2$, namely S is thin, then obviously (X, S) is commutative. So we assume $n_T = p$. Then T is normal by Theorem 4.1.

In general, for $s, t \in S$, the complex product st is a subset of S. But in our case, for $t \in T$ and $s \in S$, $|st| = 1$ and $|ts| = 1$ since t is thin. So we regard st and ts as elements of S. We note that $n_s = n_{st} = n_{ts}$ in this case. Also T can be considered as a group of order p. Then T acts on S from left and right. We consider T-orbits of S. Since T is normal, every T-orbit of the left action is also a T-orbit of the right action. So every T-orbit is of the form TsT for some $s \in S$. The length of every T-orbit is 1 or p since the order of T is p.

Lemma 4.2 *If there exists $s \in S$ such that $|TsT| = 1$, then $|Ts'T| = 1$ for every $s' \in S - T$.*

Proof Suppose there exists $s' \in S - T$ such that $|Ts'T| = p$. Then $n_{s'} < p$ by $n_S = p^2$. Since the quotient scheme $S/\!/T$ is primitive, there exists a positive integer i such that $s^T \in (s'^T)^i$. Then $s \in (s')^i$ by $TsT = \{s\}$. Note that $p \mid n_{TsT} = n_s$. This contradicts to [9, Theorem 3.1.6]. □

Now we have the following.

Proposition 4.3 *Let p be a prime number, (X, S) an association scheme of order p^2. Suppose that (X, S) has a thin closed subset T with $n_T = p$. Put $k = (p-1)/(|S/\!/T| - 1)$. Then one of the following holds.*

(1) *Every T-orbit by the right or left action of $S - T$ has length 1. Moreover, we have $n_s = kp$ for every $s \in S - T$ and $|S| = |S/\!/T| + p - 1$.*
(2) *Every T-orbit by the right or left action of $S - T$ has length p. Moreover, we have $n_s = k$ for every $s \in S - T$ and $|S| = p|S/\!/T|$.*

Proof By Lemma 4.2, it is enough to determine the valencies. By [7], $n_{s^T} = k$ for every $s \in S - T$. So the result is clear by $n_{TsT} = n_{s^T} n_T = kp$. □

We show that (X, S) is commutative for the case (1) in Proposition 4.3. In this case, easily we can see that the scheme is isomorphic to the wreath product of the thin scheme of order p and a scheme of order p. This fact shows the commutativity of the scheme. But we will give an elementary proof. Commutativity for the case (2) will be proved in the next section.

Proposition 4.4 *In the case (1) in Proposition 4.3, the scheme (X, S) is commutative.*

Proof For $s \in S$ and $t \in T$, $\sigma_s \sigma_t = \sigma_t \sigma_s$ since $TsT = s$ or $s \in T$.

Let $s, s' \in S - T$. We know that the quotient scheme $S/\!/T$ is commutative. So, by [9, Theorem 4.1.3(ii)], we have

$$a_{ss'w} = n_T a_{s^T s'^T w^T} = n_T a_{s'^T s^T w^T} = a_{s'sw}$$

for any $w \in S$. This means that (X, S) is commutative. □

We note that the case (2) in Proposition 4.3, the scheme (X, S) is p'-valenced, namely the valency of every $s \in S$ is a p'-number.

Proposition 4.5 *In the case (2) in Proposition 4.3, $\mathbb{Z}T$ is in the center of $\mathbb{Z}S$.*

Proof Fix $s \in S$ and define a group homomorphism $\rho : T \to T$ by $ts = s\rho(t)$. Then

$$\sigma_t \sigma_s \sigma_{s^*} \sigma_{t^*} = \sigma_s \sigma_{\rho(t)} \sigma_{\rho(t)^*} \sigma_{s^*} = \sigma_s \sigma_{s^*}.$$

So we have

$$\sum_{u \in S} a_{s,s^*,u} \sigma_u = \sigma_s \sigma_{s^*} = \sigma_t \sigma_s \sigma_{s^*} \sigma_{t^*} = \sum_{u \in S} a_{s,s^*,u} \sigma_{tut^*} = \sum_{u \in S} a_{s,s^*,t^*ut} \sigma_u$$

for $t \in T$. This means $a_{s,s^*,u} = a_{s,s^*,tut^*}$ for any $s, u \in S$ and $t \in T$. So we have $a_{u^*,s,s} = a_{tu^*t^*,s,s}$ by [9, Lemma 1.1.3(ii)].

Suppose $tu^* \neq u^*t$ for some $u \in S$ and $t \in T$. Then u^*, tu^*t^*, $\ldots$, and $t^{p-1}u^*(t^*)^{p-1}$ are all different. So, if $u \in ss^*$ for some $s \in S$, then $a_{u^*,s,s} > 0$ and

$$p \leq \sum_{v \in S} a_{v,s,s} = n_s < p.$$

This is a contradiction. So we can say that $tu = ut$ if $u \in ss^*$ for some $s \in S$.

If $ss^* \subset T$ for any $s \in S$, then T is in the thin residue of (X, S). So (X, S) is commutative by [6] in this case. So we may assume that there exists $v \in S - T$ such that $v \in ss^*$ for some $s \in S$. Then $\sigma_t \sigma_v \sigma_v \sigma_{t^*} = \sigma_v \sigma_v$. Similar argument as above shows that any $u \in vv$ satisfies $tu = ut$ for any $t \in T$. Repeat this process, and we can show that, for any positive integer i, any $u \in v^i$ satisfies $tu = ut$ for any $t \in T$.

Let u be an arbitrary element in S. Since $S/\!/T$ is primitive, there exists a positive integer i such that $TuT \cap v^i \neq \phi$. Take $u' \in TuT \cap v^i$. Then $u' = ut'$ for some $t' \in T$. So u also satisfies $tu = ut$ for any $t \in T$. This completes the proof. □

Now we show that any Schurian scheme of prime square order is commutative. An association scheme induced by a transitive permutation group [1, Example II.2.1(1)] is said to be *Schurian*. This definition seems to be different from that in [9], but they are equivalent [9, Corollary 6.3.2]. Permutation groups of prime square degree are considered, for example, in [3]. The next theorem follows from the results in [3] but we give a proof.

Theorem 4.6 *Every Schurian scheme of prime square order is commutative.*

Proof Let p be a prime number, G a transitive permutation group of degree p^2, H a stabilizer of a point, and let P be a Sylow p-subgroup of G. Put $|G| = p^a q$ where a and q are rational integers and $p \nmid q$. Then

$$|G| \geq |HP| = \frac{|H| \cdot |P|}{|H \cap P|} = \frac{p^{a-2}}{|H \cap P|} |G|.$$

Of course, $|H \cap P| \leq p^{a-2}$. This shows that $HP = G$, and so P is transitive. This means that the adjacency algebra of the scheme induced by G is a subalgebra of that induced by P. So it is enough to show that the scheme induced by P is commutative.

Let (X, S) be the scheme induced by P. Then the valency of every element of S is a p-power, since P is a p-group. If (X, S) is thin, then obviously it is commutative since a finite group of prime square order is commutative. If (X, S) is not thin, then it satisfies the condition of the case (1) in Proposition 4.3. So the result holds by Proposition 4.4. □

We can identify a thin scheme with the corresponding finite group. So there are two isomorphism classes of thin schemes of order p^2 and they are commutative. We can see that any Schurian scheme of order p^2 is a fusion scheme of one of them by the above arguments.

5 Commutativity

In this section, we will prove the commutativity of a scheme of order p^2 with a non-trivial thin closed subset satisfying (2) in Proposition 4.3. So we may assume (X, S) is p'-valenced and every valency is less than p.

Let F be a field of characteristic p. By Theorem 3.5, there exists $s \in S$ such that $F(S/\!/T) = F[\overline{\sigma_{sT}}]$. We will fix such $s \in S$. Let t be a generator of the cyclic group T. We write the Jacobson radical of FT by $\mathrm{Rad}(FT)$. Then it is proved in [2, Theorem 5.24] that $\mathrm{Rad}(FT) = \bigoplus_{j=1}^{p-1} F(1 - \sigma_t{}^j)$.

By [5], there exists an algebra homomorphism

$$\pi : \mathbb{Z}S \to \mathbb{Z}(S/\!/T), \qquad \sigma_s \mapsto \frac{n_s}{n_{s^T}} \sigma_{s^T}.$$

This induces an F-algebra homomorphism $\overline{\pi} : FS \to F(S/\!/T)$. Since (X, S) is p'-valenced, $\overline{\pi}$ is an epimorphism.

Lemma 5.1 *In the above notations, the kernel of* $\overline{\pi}$ *is* $(FS)\mathrm{Rad}(FT)$ *and its dimension is* $|S|(p-1)/p$.

Proof By the definition of $\overline{\pi}$, it is easy to see that $(FS)\mathrm{Rad}(FT)$ is contained in the kernel. Also $\dim_F (FS)\mathrm{Rad}(FT) = |S|(p-1)/p$ is clear by the structure of (X, S). Since $\overline{\pi}$ is an epimorphism and $\dim_F F(S/\!/T) = |S|/p$, the kernel is $(FS)\mathrm{Rad}(FT)$. □

Lemma 5.2 *We have* $FS = F[\overline{\sigma_s}](FT)$. *Especially,* FS *is commutative.*

Proof Since $\overline{\pi}(F[\overline{\sigma_s}](FT)) = F[\overline{\sigma_{sT}}] = F(S/\!/T)$ and $\ker(\overline{\pi}) = (FS)\mathrm{Rad}(FT)$, we have

$$FS = F[\overline{\sigma_s}](FT) + (FS)\mathrm{Rad}(FT).$$

Regard both sides of this equation as FT-modules. Then Nakayama's Lemma [2, Lemma 5.7] shows that $FS = F[\overline{\sigma_s}](FT)$.

Since FT is contained in the center of FS by Proposition 4.5, FS is commutative. □

Proposition 5.3 *Under the above assumptions,* (X, S) *is commutative.*

Proof Note that every valency of an element of S is less than p. For $s, t, u \in S$, it holds that $\sum_{t \in S} a_{stu} = n_s$ by [9, Lemma 1.1.3(iii)] and $a_{stu} \geq 0$. So we have $0 \leq a_{stu} \leq n_s < p$, and similarly $0 \leq a_{tsu} \leq n_s < p$. Since FS is commutative, we have $a_{stu} \equiv a_{tsu} \pmod{p}$ for any $s, t, u \in S$. This means that $a_{stu} = a_{tsu}$ and (X, S) is commutative. □

Now we have proved all parts of our main result.

Theorem 5.4 *Let p be a prime number, and (X, S) an association scheme of order p^2 having a non-trivial thin closed subset T. Then (X, S) is commutative. Moreover, if $n_T = p$, then $|S| = |S/\!\!/T| + p - 1$ or $|S| = p|S/\!\!/T|$ holds.*

Acknowledgements The authors thank Paul-Hermann Zieschang who pointed out some mistakes of the manuscript.

References

1. Bannai, E., Ito, T.: Algebraic Combinatorics I. Benjamin/Cummings, Menlo Park (1984)
2. Curtis, C.W., Reiner, I.: Methods of Representation Theory, vol. I. Wiley, New York (1981)
3. Dobson, E., Witte, D.: Transitive permutation groups of prime-squared degree. J. Algebr. Comb. **16**(1), 43–69 (2002)
4. Hanaki, A.: Locality of a modular adjacency algebra of an association scheme of prime power order. Arch. Math. (Basel) **79**(3), 167–170 (2002)
5. Hanaki, A.: Representations of association schemes and their factor schemes. Graphs Comb. **19**(2), 195–201 (2003)
6. Hanaki, A.: Characters of association schemes containing a strongly normal closed subset of prime index. Proc. Am. Math. Soc. **135**(9), 2683–2687 (2007)
7. Hanaki, A., Uno, K.: Algebraic structure of association schemes of prime order. J. Algebr. Comb. **23**(2), 189–195 (2006)
8. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers. Springer Monographs in Mathematics. Springer, Berlin (2004)
9. Zieschang, P.-H.: Theory of Association Schemes. Springer Monographs in Mathematics. Springer, Berlin (2005)