Hokkaido Mathematical Journal Vol. 45 (2016) p. 75–91

Zeta functions of adjacency algebras of association schemes of prime order or rank two

Akihide Hanaki and Mitsugu Hirasaka

(Received September 17, 2013; Revised January 6, 2014)

Abstract. For a module L which has only finitely many submodules with a given finite index we define the zeta function of L to be a formal Dirichlet series $\zeta_L(s) = \sum_{n\geq 1} a_n n^{-s}$ where a_n is the number of submodules of L with index n. For a commutative ring R and an association scheme (X, S) we denote the adjacency algebra of (X, S) over R by RS. In this article we aim to compute $\zeta_{\mathbb{Z}S}(s)$, where $\mathbb{Z}S$ is viewed as a regular $\mathbb{Z}S$-module, under the assumption that $|X|$ is a prime or $|S| = 2$.

Key words: zeta functions, adjacency algebras, association schemes.

1. Introduction

For a module L which has only finitely many submodules with a given finite index we define the *zeta function* of L to be a formal Dirichlet series

$$\zeta_L(s) = \sum_{n\geq 1} a_n n^{-s}$$

where a_n is the number of submodules of L with index n. In [8], L. Solomon established several important methods in computing the zeta function of a lattice over a group ring $\mathbb{Z}[G]$ where G is a finite group, and he found the following zeta function of $\mathbb{Z}[G]$ being viewed as a regular $\mathbb{Z}[G]$-module when the order of G is a prime p:

$$\zeta_{\mathbb{Z}[G]}(s) = (1 - p^{-s} + p^{1-2s})\zeta_{\mathbb{Q}}(s)\zeta_{\mathbb{Q}(\varepsilon)}(s)$$

where $\zeta_k(s)$ is the Dedekind zeta function of an algebraic field k and ε is a primitive p-th root of unity (see [6], [7] and [9] for other group rings).

2010 Mathematics Subject Classification : 05E30.

This research was supported by Basic Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (grant number NRF-2013R1A1A2012532).

In this article we are concerned with adjacency algebras of association schemes. Let X be a finite set and S a partition of $X \times X$. Then an element r of S is a binary relation on X and its adjacency matrix σ_r is defined to be a $\{0,1\}$-matrix whose rows and columns are indexed by the elements of X such that

$$(\sigma_r)_{x,y} = \begin{cases} 1 & \text{if } (x,y) \in r, \\ 0 & \text{if } (x,y) \notin r. \end{cases}$$

We say that the pair (X,S) is an *association scheme* if it satisfies the following conditions (see [1] or [11] a background for the theory of associations schemes):

(i) The identity matrix is contained in $\{\sigma_r \mid r \in S\}$;
(ii) $\{\sigma_r \mid r \in S\}$ is closed under the transposed map;
(iii) $\sum_{r\in S} \mathbb{Z}\sigma_r$ is closed under the matrix product.

For an association scheme (X,S) we denote $\sum_{r\in S} \mathbb{Z}\sigma_r$ by $\mathbb{Z}S$ so that $\mathbb{Z}S$ is a $\mathbb{Z}$-algebra. For a commutative ring R we denote the tensor product $R \otimes_{\mathbb{Z}} \mathbb{Z}S$ by RS, which is called the *adjacency algebra* of (X,S) over R.

For a finite group G we set

$$\hat{G} = \{\hat{g} \mid g \in G\}$$

where $\hat{g} = \{(a,b) \in G \times G \mid a^{-1}b = g\}$. It is well-known (see [10, Theorem A]) that $(G,\hat{G})$ is an association scheme and the adjacency algebra $R\hat{G}$ is identified with the group ring $R[G]$ for a commutative ring R. At this point it is natural to ask whether the same attempt as in [8] can be done for adjacency algebras generalizing group rings. In this article we deal with association schemes (X,S) of prime order or rank two, i.e., $|X|$ is a prime or $|S| = 2$, and we obtain the zeta function of $\mathbb{Z}S$ being viewed as a regular $\mathbb{Z}S$-module for each of the two cases. It should be mentioned that the proofs owe much to the methods given in [8]. But, we would like to stress that this is the first attempt to find zeta functions of adjacency algebras of association schemes except for group rings. The following are our main theorems:

Theorem 1.1 *Let (X,S) be an association scheme of prime order p. Then*

$$\zeta_{\mathbb{Z}S}(s) = (1 - p^{-s} + p^{1-2s})\zeta_{\mathbb{Q}}(s)\zeta_F(s)$$

where F is the minimal splitting field of a non-principal character of $\mathbb{C}S$.

Theorem 1.2 *Let (X, S) be an association scheme of rank two and $|X| = \prod_{i=1}^{k} {p_i}^{m_i}$ where $p_1, p_2, \dots, p_k$ are the prime divisors of $|X|$ and $m_1, m_2, \dots, m_k$ are positive integers. Then*

$$\zeta_{\mathbb{Z}S}(s) = \prod_{i=1}^{k} \delta_{p_i,m_i}({p_i}^{-s}) \cdot \zeta_{\mathbb{Q}}(s)^2$$

where $\delta_{p_i,m_i}(t) = {p_i}^{m_i} t^{2m_i} + \sum_{j=0}^{m_i-1} {p_i}^j t^{2j}(1-t)$.

In Section 2 we prepare basic results to make this article as self-contained as possible. In Sections 3, 4, we reveal the structure of the poset consisting of submodules of $\mathbb{Z}_p S$ with finite index where p is a prime divisor of $|X|$ and $\mathbb{Z}_p$ is the localization of $\mathbb{Z}$ at p. In Section 5 we prove our main theorems.

2. Preliminaries

We use the same notation for association schemes as in [2] and for integral representations as in [8]. Throughout this article we assume the following:

(i) (X, S) is an association scheme;
(ii) p is a prime;
(iii) $\mathbb{Z}_p$ is the localization of $\mathbb{Z}$ at p;
(iv) A module means a finitely generated unitary left module.

For a ring R and an R-module L we will write $\mathrm{Rad}(L)$ for the intersection of all maximal submodules of L, so that $\mathrm{Rad}(R)$ is the Jacobson radical of R.

Lemma 2.1 *For every module L over a $\mathbb{Z}_p$-algebra we have $pL \subseteq \mathrm{Rad}(L)$.*

Proof. Assume the contrary, i.e., $pL \not\subseteq M$ for a maximal submodule M of L. Then $M + pL = L$. Since M, pL and L are viewed as $\mathbb{Z}_p$-modules and $pL = (p\mathbb{Z}_p)L = \mathrm{Rad}(\mathbb{Z}_p)L$, it follows from Nakayama's lemma that $M = L$, which contradicts the maximality of M. □

Lemma 2.2 *Let L be a module over a $\mathbb{Z}_p$-algebra R and B a subset of L. Then we have the following*:

(i) *pR is an ideal of R and L/pL is an R/pR-module;*
(ii) *B generates L as an R-module if and only if $\{b+pL \mid b \in B\}$ generates L/pL as an R/pR-module.*

Proof. (i) Since p is in the center of R, pR is a two-sided ideal of R. Since $(pR)L \subseteq pL$, the function $R/pR \times L/pL \to L/pL$, $(r+pR, x+pL) \mapsto rx+pL$, is well-defined and it is easily checked that L/pL is an R/pR-module.

(ii) "only if" part is trivial. Suppose that $\{b + pL \mid b \in B\}$ generates L/pL as an R/pR-module. Then $L = RB + pL$, and by Lemma 2.1,

$$RB + pL \subseteq RB + \mathrm{Rad}(R)L.$$

By Nakayama's lemma, $L = RB$. □

Lemma 2.3 *Let L be a torsion-free $\mathbb{Z}_p$-module and B a subset of L. If $\{b + pL \mid b \in B\}$ is $\mathbb{Z}_p/p\mathbb{Z}_p$-linearly independent in L/pL, then B is $\mathbb{Z}_p$-linearly independent.*

Proof. Suppose that

$$\sum_{i=0}^{n} a_i b_i = 0 \text{ for } a_0, a_1, \ldots, a_d \in \mathbb{Z}_p \text{ and distinct } b_1, b_2, \ldots, b_n \in B.$$

The assumption implies that $a_i \in p\mathbb{Z}_p$ for $i = 1, 2, \ldots, n$. Since L is torsion-free, it follows that $a_i \in p^j\mathbb{Z}_p$ for $i = 1, 2, \ldots, n$ and each positive integer j. This implies that $a_i = 0$ for $i = 1, 2, \ldots, n$. Therefore, B is linearly independent. □

We can weaken the assumption given in [8, Lemma 12] as follows:

Lemma 2.4 *Suppose that Λ is a local $\mathbb{Z}_p$-order with the unique maximal ideal of index p, and L is a Λ-lattice. Then all maximal Λ-submodules of L have the form $\ker f$ where*

$$f \in \mathrm{Hom}_\Lambda(L, K) \text{ and } K = \Lambda/\mathrm{Rad}(\Lambda) \cong \mathbb{Z}/p\mathbb{Z}.$$

If $f, g \in \mathrm{Hom}_\Lambda(L, K)$, then $\ker f = \ker g$ if and only if f is a K-multiple of g. Thus the number of maximal Λ-modules of L is

$$1 + p + \cdots + p^{n-1} \text{ where } n = \dim_K \mathrm{Hom}_\Lambda(L, K).$$

Proof. The proof is parallel to that as in [8, Lemma 12]. □

Recall that the adjacency algebra of an association scheme over the complex number field is semisimple. We denote by $\mathrm{Irr}(S)$ the set of irreducible characters of $\mathbb{C}S$. We shall write the set of non-principal irreducible characters of $\mathbb{C}S$ as $\mathrm{Irr}(S)^\times$, and the set of non-diagonal relations of S as $S^\times$. For $s \in S$ we denote by σ_s the adjacency matrix of s. For $\chi \in \mathrm{Irr}(S)$ we denote the multiplicity of χ by m_χ. For a matrix a over $\mathbb{Z}_p$, we will write $\overline{a}$ for the image by the projection $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p$.

Theorem 2.5 ([2], [3], [4] and [5]) *Suppose that $|X|$ is a prime p and K is a field of characteristic p. Then we have the following*:

- (i) *All elements in* $\mathrm{Irr}(S)^\times$ *are algebraic conjugate*;
- (ii) $\mathbb{Q}S \simeq \mathbb{Q} \oplus F$ *where F is the minimal splitting field of $\chi \in \mathrm{Irr}(S)^\times$, namely $F = \mathbb{Q}(\chi(\sigma_s) \mid s \in S)$, and p is totally ramified in the ring of algebraic integers of F*;
- (iii) *There exists $s \in S$ such that $KS = K[\overline{\sigma_s}]$ and*

$$\{\overline{v}^i \mid i = 0, 1, 2, \ldots, |S| - 1\}$$

  is a basis for KS where $v = \sigma_s - n_s\sigma_1$;
- (iv) *KS is a local algebra and $(KS)\overline{v}$ is the unique maximal ideal of KS.*

Lemma 2.6 *Let Γ be a maximal $\mathbb{Z}$-order in $\mathbb{Q}S$ containing $\mathbb{Z}S$. Suppose $n_s \mid m_\chi$ for all $\chi \in \mathrm{Irr}(S)^\times$ and $s \in S^\times$. Then each prime divisor of the index $|\Gamma : \mathbb{Z}S|$ divides $|X|$.*

Proof. For short we denote $|X|$ by n. Let $x \in \Gamma$. Then

$$x = \sum_{s \in S} b_s\sigma_s \text{ for some } b_s \in \mathbb{Q} \text{ with } s \in S.$$

We set $T : \mathbb{C}S \to \mathbb{C}$ as the trace map. Since $T(x\sigma_{s^*}) = b_s n_s n$ for each $s \in S$, it follows that

$$nx = \sum_{s \in S} \frac{1}{n_s} T(x\sigma_{s^*})\sigma_s.$$

Since $x, \sigma_{s^*} \in \Gamma$, it follows that $x\sigma_{s^*} \in \Gamma$. Note that $T(y) \in \mathbb{Z}$ for each $y \in \Gamma$

since $T(y) \in \mathbb{Q}$, $T(y)$ is a sum of eigenvalues of y and y is integral over $\mathbb{Z}$. Recall that $T = \sum_{\chi\in \mathrm{Irr}(S)} m_\chi \chi$. We shall write the principal character of $\mathbb{C}S$ as χ_0. Thus,

$$\begin{aligned} nx &= \sum_{s\in S}\sum_{\chi} \frac{m_\chi \chi(x\sigma_{s^*})\sigma_s}{n_s} \\ &= \sum_{s\in S^\times}\sum_{\chi} \frac{m_\chi \chi(x\sigma_{s^*})\sigma_s}{n_s} + \sum_{\chi} m_\chi\chi(x)\sigma_1 \\ &= \sum_{s\in S^\times}\sum_{\chi\neq\chi_0} \frac{m_\chi \chi(x\sigma_{s^*})\sigma_s}{n_s} + \sum_{\chi} m_\chi\chi(x)\sigma_1 + \sum_{s\in S^\times} \frac{\chi_0(x\sigma_{s^*})\sigma_s}{n_s} \\ &\quad \text{since } \chi_0 \text{ is a ring homomorphism such that } \chi_0(\sigma_s) = n_s \\ &= \sum_{s\in S^\times}\sum_{\chi\neq\chi_0} \frac{m_\chi \chi(x\sigma_{s^*})\sigma_s}{n_s} + \sum_{\chi} m_\chi\chi(x)\sigma_1 + \sum_{s\in S^\times} \chi_0(x)\sigma_s. \end{aligned}$$

Therefore, $nx \in \mathbb{Z}S$ whenever $n_s \mid m_\chi$ for all $\chi \in \mathrm{Irr}(S)^\times$ and $s \in S^\times$.

Let q be a prime divisor of $|\Gamma : \mathbb{Z}S|$. Since $\Gamma/\mathbb{Z}S$ is a finite group, there exists an element of order q in $\Gamma/\mathbb{Z}S$. Since we have already proved that $n\Gamma \subseteq \mathbb{Z}S$, q divides n. □

3. Submodules of $\mathbb{Z}_p S$ where $|X| = p$

Throughout this section we assume that (X, S) is an association scheme of prime order p, and we denote by Λ the adjacency algebra of (X, S) over $\mathbb{Z}_p$.

Lemma 3.1 *The $\mathbb{Z}_p$-algebra Λ is commutative and local with the unique maximal ideal of index p.*

Proof. By Theorem 2.5(ii), $\mathbb{Q}S$ is commutative, and hence, Λ is also commutative. Let M be a maximal ideal of Λ. Applying Lemma 2.1 for Λ we have $p\Lambda \subseteq M$. Since $\Lambda/p\Lambda \simeq (\mathbb{Z}_p/p\mathbb{Z}_p)S$, it follows from Theorem 2.5(iv) that Λ is local with the unique maximal ideal of index p. □

We shall denote the unique maximal ideal of Λ as in Lemma 3.1 by M, and Λ/M by K where K is viewed as a field or a simple Λ-module for the remainder of this article. For short we shall write σ_1, $\sigma_S := \sum_{s\in S}\sigma_s$ and

$\sigma_s - n_s\sigma_1$ as e, u and v, respectively, where $\sigma_s \in \mathbb{Z}S$ is as in Theorem 2.5. For short we shall write $|S|$ as $d+1$.

Lemma 3.2 *$\{v^i \mid i = 0, 1, \ldots, d\}$ is a $\mathbb{Z}_p$-basis for Λ.*

Proof. By Theorem 2.5(iii), $\{\bar{v}^i \mid i = 0, 1, \ldots, d\}$ is a basis for KS. Thus, this lemma follows from Lemma 2.2 and Lemma 2.3. $\square$

By Lemma 3.2,

$$u = \sum_{i=0}^{d} a_i v^i \text{ for some } a_0, a_1, \ldots, a_d \in \mathbb{Z}_p. \tag{1}$$

Multiplying u to both sides of (1) we obtain from $uv = 0$ and $uu = pu$ that

$$a_0 = p. \tag{2}$$

We claim that $\bar{v}^d$ is a nonzero scalar multiple of $\bar{u}$. By Theorem 2.5(iii), the annihilator of $\bar{v}$ in KS is exactly $K\bar{v}^d$. Since $vu = 0$ by the definition of u and v, the claim follows. Therefore,

$$a_1 \equiv a_2 \equiv \cdots \equiv a_{d-1} \equiv 0 \mod p, \quad a_d \not\equiv 0 \mod p. \tag{3}$$

Multiplying v to both sides of (1) we obtain from (2) that

$$pv + \sum_{i=1}^{d} a_i v^{i+1} = 0. \tag{4}$$

Lemma 3.3 *We have $M = \Lambda u \oplus \Lambda v$.*

Proof. We claim that $\Lambda u \cap \Lambda v = \{0\}$. Note that $\Lambda u = \mathbb{Z}_p u$ by the definition of u and Λ. Suppose $x \in \Lambda u \cap \Lambda v$. Then $x = ru = tv$ for some $r \in \mathbb{Z}_p$ and $t \in \Lambda$. Now since $uv = 0$, we have

$$ux = u(ru) = pru, \quad ux = u(tv) = t(uv) = 0.$$

This means $r = 0$ and $x = 0$. Therefore, we conclude from the claim that $\Lambda u + \Lambda v$ is a direct sum. Clearly, $\Lambda u + \Lambda v$ is a Λ-submodule, which is a free $\mathbb{Z}_p$-module with the ordered $\mathbb{Z}_p$-basis $(u, v, v^2, \ldots, v^d)$. By (2), $(pe, v, v^2, \ldots, v^d)$

is an ordered $\mathbb{Z}_p$-basis for $\Lambda u + \Lambda v$, which implies $|\Lambda : \Lambda u + \Lambda v| = p$. Since M is a unique maximal Λ-submodule of Λ, $M = \Lambda u \oplus \Lambda v$. □

Lemma 3.4 *We have* $\dim_K \operatorname{Hom}_\Lambda(M, K) = 2$.

Proof. By Lemma 2.4 and Lemma 3.3, $M/pM \simeq K \oplus U$ as $\Lambda/p\Lambda$-modules, where $U = (\Lambda/p\Lambda)(v + pM)$ is a uniserial module. So,

$$(\operatorname{Rad}(\Lambda/p\Lambda))(M/pM) = \bigoplus_{i=2}^{d} K(v^i + pM) \text{ and}$$

$$(M/pM)/(\operatorname{Rad}(\Lambda/p\Lambda))(M/pM) \simeq K \oplus K \text{ as } \Lambda/p\Lambda\text{-modules.}$$

Since K is a simple Λ-module, we have

$$\begin{aligned}\operatorname{Hom}_\Lambda(M, K) &\simeq \operatorname{Hom}_{\Lambda/p\Lambda}(M/pM, K)\\ &\simeq \operatorname{Hom}_{\Lambda/p\Lambda}((M/pM)/\operatorname{Rad}(\Lambda/p\Lambda)(M/pM)), K)\\ &\simeq \operatorname{Hom}_{\Lambda/p\Lambda}(K \oplus K, K).\end{aligned}$$

Thus, $\dim_K \operatorname{Hom}_\Lambda(M, K) = 2$. □

Proposition 3.5 *Suppose $d > 1$. Then M has exactly $p + 1$ maximal Λ-submodules, exactly two of which are isomorphic to M and exactly $p - 1$ of which are isomorphic to Λ.*

Proof. By Lemma 2.4 and Lemma 3.4, M has exactly $p+1$ Λ-submodules of index p. Thus, the first assertion holds. By Lemma 3.3,

$$\Lambda pu + \Lambda v^2 \subseteq MM = \operatorname{Rad}(\Lambda)M.$$

By Nakayama's lemma, $\operatorname{Rad}(\Lambda)M \subseteq \operatorname{Rad}(M)$. This implies that each maximal Λ-submodule of M contains $\sum_{i=2}^{d} \mathbb{Z}_p v^i$. Thus, by the theory of elementary divisors, the set of $\mathbb{Z}_p$-submodules being viewed as Λ-submodules of M with index p coincides with

$$\{N_a \mid a = 0, 1, \ldots, p-1, \infty\}$$

where $N_\infty = \mathbb{Z}_p u + \mathbb{Z}_p(pv) + \sum_{i=2}^{d} \mathbb{Z}_p v^i$ and for $a = 0, 1, \ldots, p-1$

$$N_a = \mathbb{Z}_p(pu) + \mathbb{Z}_p(au+v) + \sum_{i=2}^{d} \mathbb{Z}_p v^i.$$

We shall write the representation matrix of the multiplication of v in the ordered $\mathbb{Z}_p$-basis β for a Λ-module as T_β. Note that, for all Λ-modules M_1, M_2, $M_1 \simeq M_2$ as Λ-modules if and only if $T_{\beta_1} = T_{\beta_2}$ for some ordered $\mathbb{Z}_p$-basis β_i of M_i with $i = 1, 2$ since v generates Λ by Lemma 3.2.

We claim that $N_0 \simeq N_\infty \simeq M$. By Lemma 3.3, $\beta_1 = (u, v, v^2, \dots, v^d)$ is an ordered basis for M. By the definition of N_0, $\beta_2 = (pu, v, v^2, \dots, v^d)$ is an ordered basis for N_0. By (3) and (4), $\beta_3 = (u, v^2, \dots, v^d, v^{d+1})$ is an ordered basis for N_∞. The claim holds since

$$T_{\beta_1} = T_{\beta_2} = T_{\beta_3} = \left(\begin{array}{c|c|c|c|c} 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & (-a_d^{-1})p \\ \hline 0 & 1 & 0 & \cdots & (-a_d^{-1})a_1 \\ \hline 0 & 0 & 1 & \ddots & (-a_d^{-1})a_2 \\ \hline \cdots & \cdots & \cdots & \cdots & \cdots \\ \hline 0 & 0 & 0 & \cdots & (-a_d^{-1})a_{d-1} \end{array}\right).$$

We claim that $N_a \simeq \Lambda$ for $a = 1, 2, \dots, p-1$. By Lemma 3.2, $\gamma = (e, v, v^2, \dots, v^d)$ is an ordered basis for Λ. By (3) and (4), $\gamma_a = (au + v, v^2, \dots, v^d, v^{d+1})$ is an ordered basis for N_a. The claim holds since

$$T_\gamma = T_{\gamma_a} = \left(\begin{array}{c|c|c|c|c} 0 & 0 & 0 & \cdots & 0 \\ \hline 1 & 0 & 0 & \cdots & (-a_d^{-1})p \\ \hline 0 & 1 & 0 & \cdots & (-a_d^{-1})a_1 \\ \hline 0 & 0 & 1 & \ddots & (-a_d^{-1})a_2 \\ \hline \cdots & \cdots & \cdots & \cdots & \cdots \\ \hline 0 & 0 & 0 & \cdots & (-a_d^{-1})a_{d-1} \end{array}\right).$$

The two claims complete the proof of the second assertion. □

4. Submodules of $\mathbb{Z}_p S$ with $|S| = 2$ and $p \mid |X|$

Throughout this section we assume that (X, S) is an association scheme with $|S| = 2$ and $|X| = n$, p is a prime divisor of n and m is the least positive integer with $p^{m+1} \nmid n$. For short we denote $\mathbb{Z}_p S$ by Λ. For non-negative integers i, a we define

$$N_{i,a} = \mathbb{Z}_p(p^{i+1}e) + \mathbb{Z}_p(p^i ae + u) \text{ and } N_{i,\infty} = \mathbb{Z}_p(p^i e) + \mathbb{Z}_p(pu)$$

where $e = \sigma_1$ and $u = \sigma_S$.

Lemma 4.1 *We have the following*:

(i) $N_{i,a}$ *is a free* $\mathbb{Z}_p$*-module of rank* 2;
(ii) $\{N_{i,a} \mid a = 0, 1, \ldots, p-1, \infty\}$ *are the distinct maximal* $\mathbb{Z}_p$*-submodules of* $N_{i-1,0}$ *where* $N_{-1,0} = \Lambda$.

Proof. (i) follows since $\{xe, ye + zu\}$ are linearly independent for all $x, y, z \in \mathbb{Z}_p$ with $xz \neq 0$.

(ii) follows from the theory of elementary divisors since $\mathbb{Z}_p$ is a principal ideal domain and $N_{i,a}$ is a $\mathbb{Z}_p$-submodule of $N_{i-1,0}$ with index p. □

Lemma 4.2 *For each* $i = 0, 1, \ldots, m$ *and* $a = 0, 1, \ldots, p-1$, $N_{i,a}$ *is a* Λ*-submodule if and only if* $i \neq 0$ *or* $a = 0$.

Proof. Suppose that $N_{i,a}$ is a Λ-submodule. Then

$$u(ap^i e + u) = x(p^{i+1}e) + y(p^i ae + u)$$

for some $x, y \in \mathbb{Z}_p$. Since the left hand side is equal to $(ap^i + n)u$ and $\{e, u\}$ are linearly independent, it follows that

$$xp^{i+1} = -y(ap^i), \;\; y = ap^i + n.$$

Since $\mathbb{Z}_p$ is an integral domain, $xp = -a(ap^i + n)$. Since $p\mathbb{Z}_p$ is a prime ideal, $a \in p\mathbb{Z}_p$ or $(ap^i + n) \in p\mathbb{Z}_p$. Thus, if $a \neq 0$, then $ap^i + n \in p\mathbb{Z}_p$, and hence, $i \neq 0$. Therefore, "only if" part holds.

Suppose $i \neq 0$ or $a = 0$. Then there exists $x \in \mathbb{Z}_p$ such that $xp = -a(ap^i + n)$ since $p \mid n$, and

$$u(p^{i+1}e) = (-p^i a)(p^{i+1}e) + p^{i+1}(p^i ae + u),$$

$$u(p^i ae + u) = x(p^{i+1}e) + (p^i a + n)(p^i ae + u).$$

This implies that $N_{i,a}$ is a Λ-submodule. Therefore, "if" part holds. □

Lemma 4.3 *For each $i = 0, 1, \ldots, m$, $N_{i,\infty}$ is a Λ-submodule if and only if $i \neq 0$.*

Proof. Since $ue = u \notin \mathbb{Z}_p e + \mathbb{Z}_p(pu)$, $N_{0,\infty}$ is not a Λ-submodule. This implies that "only if" part holds.

Suppose $i > 0$. Then

$$u(p^i e) = 0(p^i e) + p^{i-1}(pu), \;\; u(pu) = npu = 0(p^i e) + n(pu).$$

This implies that $N_{i,\infty}$ is a Λ-submodule. Therefore, "if" part holds. $\square$

For each $i = 1, \ldots, m$ and $a = 1, \ldots, p-1$, $(ap^{i+1}e, p^i ae + u)$ is an ordered basis for $N_{i,a}$ and $(pu, p^i ae + u)$ so is. There exists $c \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ such that $c(a + n/p^i) = 1$ whenever $a + n/p^i \notin p\mathbb{Z}_p$. Then $(pu, c(p^i ae + u))$ is also an ordered basis for $N_{i,a}$. Thus, the representation matrix of u by $(pu, c(p^i ae + u))$ is equal to

$$\begin{pmatrix} n & p^{i-1} \\ 0 & 0 \end{pmatrix} \text{ unless } i = m \text{ and } a \not\equiv \tfrac{-n}{p^m} \pmod{p}. \tag{5}$$

If $i = m$ and $a \equiv (-n)/p^m \pmod{p}$, then there exists $c \in \mathbb{Z}_p$ such that $cpn + n + p^m a = p^{m+1}$. Since $(pu, p^m ae + c(pu) + u)$ is an ordered basis for $N_{m,a}$, the representation matrix of u by the ordered basis $(pu, p^m ae + c(pu) + u)$ for $N_{m,a}$ with $a \equiv (-n)/p^m \pmod{p}$ is equal to

$$\begin{pmatrix} n & p^{m+1} \\ 0 & 0 \end{pmatrix}. \tag{6}$$

The representation matrix of u by the ordered basis $(pu, p^i e)$ for $N_{i,\infty}$ is equal to

$$\begin{pmatrix} n & p^{i-1} \\ 0 & 0 \end{pmatrix}. \tag{7}$$

For each nonnegative integer i the representation matrix of u by the ordered basis $(u, p^{i+1}e)$ for $N_{i,0}$ is equal to

$$\begin{pmatrix} n & p^{i+1} \\ 0 & 0 \end{pmatrix}. \tag{8}$$

Lemma 4.4 *For all distinct i, j, we have $N_{i,0} \simeq N_{j,0}$ as Λ-modules if and only if $i, j \geq m-1$.*

Proof. Suppose $N_{i,0} \simeq N_{j,0}$. We may assume that $i < j$. Then, by (8), there exist $a, b, c, d \in \mathbb{Z}_p$ such that $ad - bc \notin p\mathbb{Z}_p$.

$$\begin{pmatrix} n & p^{i+1} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} n & p^{j+1} \\ 0 & 0 \end{pmatrix}. \tag{9}$$

Comparing the entries we obtain

$$c = 0 \text{ and } p^{i+1}d + bn = p^{j+1}a.$$

Since $ad = ad - bc \notin p\mathbb{Z}_p$, we have $a, d \notin p\mathbb{Z}_p$. Since $p^{i+1}(d - ap^{j-i}) = -bn$, it follows from $i < j$ that $i + 1 \geq m$. Thus, $j > i \geq m - 1$.

Suppose $m - 1 \leq i < j$. Then, we can take

$$(a, b, c, d) = (1, (p^{j+1} - p^{i+1})/n, 0, 1)$$

so that (9) holds. Therefore, $N_{i,0} \simeq N_{j,0}$. □

Proposition 4.5 *We have the following:*

- (i) *$N_{0,0}$ is a unique maximal Λ-submodule of Λ and* $\mathrm{Rad}(\Lambda) = N_{0,0}$;
- (ii) *For each $i = 1, 2, \ldots, m-1$, $\{N_{i,a} \mid a = 0, 1, \ldots, p-1, \infty\}$ are the distinct maximal Λ-submodules of $N_{i-1,0}$ and $N_{i,a} \simeq N_{i-2,0}$ for each $a = 1, 2, \ldots, p-1, \infty$;*
- (iii) *$\{N_{m,a} \mid a = 0, 1, \ldots, p-1, \infty\}$ are the distinct maximal Λ-submodules of $N_{m-1,0}$, $N_{m,0} \simeq N_{m,b} \simeq N_{m-1,0}$, and $N_{m,a} \simeq N_{m-2,0}$ for each $a = 1, 2, \ldots, p-1, \infty$ with $a \neq b$ where b is a unique element of $\{1, 2, \ldots, p-1\}$ such that*

$$b \equiv \frac{-n}{p^m} \pmod{p};$$

- (iv) *For each $i = 1, 2, \ldots, m$,* $\mathrm{Rad}(N_{i-1,0}) = N_{i+1,\infty} \simeq N_{i-1,0}$.

Proof. The first statement of (i), (ii) and (iii) follows from Lemma 4.1, Lemma 4.2 and Lemma 4.3.

(i) The second statement follows from the first one.

(ii) The second statement follows from (5), (7) and (8).

(iii) The second statement follows from Lemma 4.4 and (6), and the third one follows from (5) and (8).

(iv) follows from Lemma 2.1, since $pN_{i-1,0} = N_{i+1,\infty} \simeq N_{i-1,0}$. $\square$

5. Proof of main theorems

We will apply [8, Theorem 3] for $\mathbb{Z}S$ with [8, Remark p. 320]. Whichever $|X|$ is a prime or $|S| = 2$, $\mathbb{Q}S$ is commutative, in particular, $\mathbb{Q}S$ is isomorphic to a direct sum of the full matrix algebras over fields. Moreover, the assumption as in Lemma 2.6 holds, so the set B given in [8, Theorem 3] coincides with the set of prime divisors of $|X|$. Therefore, we obtain

$$\zeta_{\mathbb{Z}S}(s) = \prod_{p||X|} \delta_p(p^{-s}) \cdot \zeta_{\mathbb{Q}S}(s) \quad \text{where} \quad \delta_p(p^{-s}) = \frac{\zeta_{\mathbb{Z}_pS}(s)}{\zeta_{\mathbb{Q}S}(s)_p}$$

and the definition of $\zeta_{\mathbb{Q}S}(s)_p$ is the same as in [8]. Note that $\mathbb{Q}S \simeq \mathbb{Q} \oplus F$ for an algebraic field F of degree $|S|-1$ whichever $|X|$ is a prime or $|S| = 2$.

We claim that

$$\zeta_{\mathbb{Q}S}(s)_p = (1 - p^{-s})^{-2}. \tag{10}$$

For an algebraic field E and a prime p, the definition of $\zeta_E(s)_p$ is the same as in [8]. Since $\zeta_{\mathbb{Q}S}(s)_p = \zeta_{\mathbb{Q}}(s)_p \zeta_F(s)_p$ and $\zeta_{\mathbb{Q}}(s)_p = (1 - p^{-s})^{-1}$, it suffices to show that

$$\zeta_F(s)_p = (1 - p^{-s})^{-1} \text{ when } |X| = p.$$

By Theorem 2.5(ii) and the definition of being totally ramified, there exists a unique prime ideal dividing p with norm p. Therefore, $\zeta_F(s)_p = (1-p^{-s})^{-1}$.

Following [8] we define a set of polynomials $\{A_{ij}(t)\}_{i,j}$ as follows: We assume the conditions (2.1), (2.2) and (2,3) given in [8] holds. Let $L_0, L_1, \ldots, L_h$ represent the isomorphism classes of submodules of L_0 with finite index. Let Φ_{ij} be the set of submodules of L_i which include $\mathrm{Rad}(L_i)$ and are isomorphic to L_j. For submodules N, L with $\mathrm{Rad}(L) \subseteq N \subseteq L$ we define

$$\mu(N, L) = \sum_J (-1)^{|J|}$$

where the sum is over all subsets J of the maximal submodules of L with $N = \bigcap_{M \in J} M$. For $i, j = 0, 1, \ldots, h$ we define

$$A_{ij}(t) = \sum_{N \in \Phi_{ij}} \mu(N, L_i)[L_i : N]$$

where $[L_i : N] = t^i$ whenever $|L_i : N| = p^i$. Let $Z_0(t)$ be the sum of the first row of the inverse matrix of $(A_{ij}(t))_{0 \le i,j \le h}$. Then, by [8, Lemma 3],

$$\zeta_{\mathbb{Z}_p S}(s) = Z_0(p^{-s}).$$

Suppose that $|X|$ is a prime p and $|S| > 2$. Then Proposition 3.5 shows that we have exactly two isomorphism classes of submodules of $\mathbb{Z}_p S$ with finite index and the matrix $(A_{ij}(t))_{0 \le i,j \le 1}$ is the same as in [8, Lemma 14]. Therefore, we obtain from (10)

$$\delta_p(t) = 1 - p^{-s} + p^{1-2s}.$$

Suppose that $|S| = 2$ and p is a prime divisor of $|X|$ and m is the least positive integer with $p^{m+1} \nmid |X|$. Then Proposition 4.5 shows that $L_0, L_1, \ldots, L_m$ represent the isomorphism classes of $\mathbb{Z}_p S$-submodules of $\mathbb{Z}_p S$ with finite index where $L_i = N_{i-1,0}$ for $i = 0, 1, \ldots, m$, and

$$\Phi_{00} = \{L_0\},\ \Phi_{01} = \{L_1\},\ \Phi_{0j} = \emptyset \text{ for each } j \text{ with } 2 \le j \le m,$$

$$\Phi_{10} = \{N_{1,a} \mid a = 1, 2, \ldots, p-1, \infty\},\ \Phi_{11} = \{L_1, N_{2,\infty}\},\ \Phi_{12} = \{L_2\},$$

$$\Phi_{1j} = \emptyset \text{ for each } j \text{ with } 2 \le j \le m$$

$$\cdots$$

$$\Phi_{mj} = \emptyset \text{ for each } j \text{ with } 0 \le j \le m-2,$$

$$\Phi_{m,m-1} = \{N_{m,a} \mid a \ne b\},\ \Phi_{mm} = \{N_{m+1,\infty}, L_m, N_{m,b}\}$$

where b is a unique element as in Proposition 4.5.

Thus, $(A_{ij}(t))_{0 \le i,j \le m}$ is equal to the following tridiagonal matrix:

$$A_{ij}(t) = \begin{cases} -t & \text{if } j = i+1 \text{ and } i = 0, 1, \ldots, m-1, \\ 1 & \text{if } j = i = 0, \\ 1 + pt^2 & \text{if } j = i \text{ and } i = 1, \ldots, m-1, \\ 1 - 2t + pt^2 & \text{if } j = i = m, \\ -pt & \text{if } j = i-1 \text{ and } i = 1, \ldots, m-1, \\ -(p-1)t & \text{if } j = m-1 \text{ and } i = m. \end{cases}$$

Namely,

$$(A_{ij}(t)) = \left(\begin{array}{c|c|c|c|c} 1 & -t & 0 & \cdots & 0 \\ \hline -pt & 1+pt^2 & -t & 0 & \cdots \\ \hline 0 & -pt & 1+pt^2 & -t & \cdots \\ \hline \ddots & \ddots & \ddots & \ddots & \ddots \\ \hline 0 & \cdots & -pt & 1+pt^2 & -t \\ \hline 0 & \cdots & 0 & -(p-1)t & 1-2t+pt^2 \end{array}\right).$$

We shall denote $(A_{ij}(t))_{0 \le i,j \le m}$ by A. Note that

$$\det(A) = (t-1)^2$$

and if Ax is the all one vector, then the first entry of $x = A^{-1}Ax$ is the sum of the first row of A^{-1}, that is exactly what we need. Thus, it suffices to find the first entry of the solution of $Ax = b$ where b is the all one vector.

By Cramer's Rule, it is equal to

$$\frac{\det(A_1)}{\det(A)}$$

where A_1 is the matrix obtained from A by replacing the first column of A by b. For $k = 2, 3, \ldots, m+1$ we denote by a_k the determinant of the square matrix of degree k whose first column is the all one vector and the rest of the matrix is equal to the lower right $k \times (k-1)$ submatrix of A_1. Note that, for $k = 2, 3, \ldots, m$,

$$a_{k+1} = ta_k + b_k$$

where b_k is the determinant of the lower right $k \times k$ submatrix of A for

$k = 2, 3, \ldots, m$. Note that

$$b_k = (1 + pt^2)b_{k-1} - pt^2 b_{k-2}.$$

Therefore,

$$a_{k+1} - ta_k = (1 + pt^2)(a_k - ta_{k-1}) - pt^2(a_{k-1} - ta_{k-2}),$$

equivalently,

$$a_{k+1} - pt^2 a_k = (t + 1)(a_k - pt^2 a_{k-1}) - t(a_{k-1} - pt^2 a_{k-2}). \qquad (11)$$

We claim that

$$a_{k+1} = p^k t^{2k} + \sum_{j=0}^{k-1}(-p^j t^{2j+1} + p^j t^{2j}).$$

We denote the right hand side by c_{k+1}. It suffices to show that $a_k = c_k$ for $k = 2, 3, 4$ and c_k and a_k satisfy the same recursive equation. It is easy to show that, for each k, $c_{k+1} - pt^2 c_k = 1 - t$, and (11) hold with replacing $a_{k+1} - pt^2 a_k$ by $1 - t$. Therefore, we obtain from (10) that

$$\delta_p(t) = \frac{Z_0(t)}{(1-t)^{-2}} = \frac{a_{m+1}}{(1-t)^2}(1-t)^2 = a_{m+1}.$$

This completes the proof of Theorem 1.2. Note that $a_2 = 1 - t + pt^2$. This implies that Theorem 1.1 holds also when $|S| = 2$. This completes the proof of Theorem 1.1.

References

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

[2] Hanaki A., *Representations of finite association schemes.* European J. Combin. **30** (2009), 1477–1496.

[3] Hanaki A., *Locality of a modular adjacency algebra of an association scheme of prime power order.* Arch. Math. (Basel) **79** (2002), 167–170.

[4] Hanaki A. and Uno K., *Algebraic structure of association schemes of prime order.* J. Algebraic Combin. **23** (2006), 189–195.

[5] Hanaki A., Hirasaka M. and Uno K., *Commutativity of association schemes of prime square order having non-trivial thin closed subsets*. J. Algebraic Combin. **27** (2008), 307–316.
[6] Hironaka Y., *Zeta functions of integral group rings of metacyclic groups*. Tsukuba J. Math. **5** (1981), 267–283.
[7] Reiner I., *Zeta functions of integral representations*. Comm. Algebra **8** (1980), 911–925.
[8] Solomon L., *Zeta functions and integral representation theory*. Advances in Math. **26** (1977), 306–326.
[9] Takegahara Y., *Zeta functions of integral group rings of abelian* (p, p)*-groups*. Comm. Algebra **15** (1987), 2565–2615.
[10] Zieschang P.-H., *An algebraic approach to association schemes*, Lecture Notes in Mathematics, vol. 1628, Springer-Verlag, Berlin, 1996.
[11] Zieschang P.-H., *Theory of association schemes*, Springer Monograph in Mathematics, Springer-Verlag, Berlin, 2005.

Akihide Hanaki
Department of Mathematical Sciences
Faculty of Science
Shinshu University
Matsumoto 390-8621, Japan
E-mail: hanaki@shinshu-u.ac.jp

Mitsugu Hirasaka
Department of Mathematics
Pusan National University
Busan 609–735, Korea
E-mail: hirasaka@pusan.ac.kr