数理解析研究所講究録 1327 巻 2003 年 10-20

Modular adjacency algebras of the Hamming association schemes

信州大学大学院工学系研究科
吉川　昌慶 (Masayoshi Yoshikawa)
Department of Mathematical Sciences, Faculty of Science,
Shinshu University

Abstruct

The adjacency algebra of an association scheme is defined over an arbitrary field. This is always semisimple over a field of characteristic 0, but not semisimple over a field of prime characteristic p, in general. The structure of the adjacency algebra over a field of prime characteristic was not studied enough before now. Therefore, we considered the structure of the modular adjacency algebra of the Hamming scheme $H(n,q)$, that is one of the most basic and important association schemes.

In this paper, we will decide the structure of the adjacency algebra of $H(n,q)$ over any field for any n and q, and describe the algebra as a factor algebra of a polynomial ring.

1 Introduction

In this paper, we consider the modular adjacency algebra of the Hamming association scheme $H(n,q)$. The modular adjacency algebra means an adjacency algebra over a positive characteristic field. For any prime p such that $p \nmid q$, the adjacency algebra of $H(n,q)$ over a field of characteristic p is semisimple (see [2, Theorem 2.3], [1, Theorem 1.1] and [5, Theorem 4.2]). For each prime p, the prime field $\mathbb{F}_p$ of characteristic p is a splitting field for the adjacency algebra of $H(n,p)$ over $\mathbb{F}_p$ (see [4, Theorem 3.4, Corollary 3.5]). For all prime p such that $p \mid q$, $\mathbb{F}_pH(n,p) \cong \mathbb{F}_pH(n,q)$ (see §2.3). Therefore it is enough to decide the structure of $\mathbb{F}_pH(n,p)$ for all prime p, for deciding the structure of the modular adjacency algebra of any $H(n,q)$ over any field. It is known that the algebra $\mathbb{F}_pH(n,p)$ is commutative and local, and that any local commutative algebra is isomorphic to a factor algebra of a polynomial ring.

2 Preparation

For the definitions in this section, refer to [2].

2.1 Association schemes

Let X be a finite set with cardinality n. We define $R_0 := \{ (x,x) \mid x \in X \}$. Let $R_i \subseteq X \times X$ be given. We set $R_i^* := \{ (z,y) \mid (y,z) \in R_i \}$. Let G be a partition of $X \times X$ such that $R_0 \in G$ and the empty set $\emptyset \notin G$, and assume that, $R_i^* \in G$ for each $R_i \in G$. Then, the pair (X,G) will be called an *association scheme* if, for all $R_i, R_j, R_k \in G$, there exists a cardinal number p_{ijk} such that, for all $y, z \in X$

$$(y,z) \in R_k \Rightarrow \sharp\{ x \in X \mid (y,x) \in R_i, (x,z) \in R_j \} = p_{ijk}.$$

The elements of $\{p_{ijk}\}$ will be called the *intersection numbers* of (X,G).

For each $R_i \in G$, we define the $n \times n$ matrix A_i indexed by the elements of X,

$$(A_i)_{xy} = \begin{cases} 1 & \text{if } (x,y) \in R_i, \\ 0 & \text{otherwise,} \end{cases}$$

and this matrix A_i will be called the *adjacency matrix* of R_i.

Let the cardinal number of G be $d+1$ and let J be the $n \times n$ all 1 matrix. Then, by the definition, it follows that $\sum_{i=0}^{d} A_i = J$. It follows that for all A_i, A_j,

$$A_i A_j = \sum_{k=0}^{d} p_{ijk} \; A_k.$$

From this fact, we can define an algebra naturally. For the commutative ring R with 1, we put $R(X,G) = \bigoplus_{i=0}^{d} RA_i$ as a matrix ring over R, and it will be called the *adjacency algebra* of (X,G) over R.

For all $i,j,k \in \{ 0,1,\ldots,d \}$, we define the matrix B_i by $(B_i)_{jk} = p_{ijk}$. This matrix B_i will be called the *i-th intersection matrix.* It follows that for all B_i, B_j, $B_i B_j = \sum_{k=0}^{d} p_{ijk} \; B_k$. Therefore we can define an algebra $RB = \bigoplus_{i=0}^{d} RB_i$ for a commutative ring R with 1, and it will be called the *intersection algebra* of (X,G) over R. Then the mapping from the adjacency algebra to the intersection algebra of (X,G) over R, $A_i \mapsto B_i$, is an algebra isomorphism.

2.2 P-polynomial schemes

A symmetric association scheme is called a *P-polynomial scheme* with respect to the ordering $R_0, R_1, \ldots, R_d$, if there exist some complex coefficient polynomials v_i of degree i $(0 \leq i \leq d)$ such that $A_i = v_i(A_1)$, where A_i is the adjacency matrix of R_i.

We use the following notation: a tridiagonal matrix

$$B = \begin{pmatrix} a_0 & c_1 & & & 0 \\ b_0 & a_1 & \ddots & & \\ & b_1 & \ddots & \ddots & \\ & & \ddots & \ddots & c_d \\ 0 & & & b_{d-1} & a_d \end{pmatrix}$$

is denoted by

$$\left\{ \begin{matrix} * & c_1 & \cdots & c_{d-1} & c_d \\ a_0 & a_1 & \cdots & a_{d-1} & a_d \\ b_0 & b_1 & \cdots & b_{d-1} & * \end{matrix} \right\}.$$

Then the following (i) and (ii) are equivalent to each other (see [2, Proposition 1.1]).

(i) B_1 is a tridiagonal matrix with non-zero off-diagonal entries:

$$\left\{ \begin{matrix} * & 1 & c_2 & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ b_0 & b_1 & b_2 & \cdots & b_{d-1} & * \end{matrix} \right\} \ (b_i \neq 0, c_i \neq 0).$$

(ii) $(X, \{R_i\}_{0 \leq i \leq d})$ is a P-polynomial scheme with respect to the ordering $R_0, R_1, \ldots, R_d$, i.e.,

$$A_i = v_i(A_1) \quad (i = 0, 1, \ldots, d)$$

for some polynomials v_i of degree i.

2.3 Hamming schemes

Let Σ be an alphabet of q symbols $\{ 0, 1, \ldots, q-1 \}$. We define Ω to be the set Σ^n of all n-tuples of elements of Σ, and let $\rho(x, y)$ be the number of coordinate places in which the n-tuples x and y

differ. Thus $\rho(x,y)$ is the Hamming distance between x and y. we set

$$R_i = \{\ (x,y) \in \Omega \times \Omega \mid \rho(x,y) = i\ \},$$

and then $(\Omega, \{R_i\}_{0\leq i\leq n})$ is an association scheme. This will be called the *Hamming scheme*, and denoted by $H(n,q)$.

We consider the intersection numbers $p_{ijk}^{(n,q)}$ of $H(n,q)$. For the convenience of the argument, we extend the binomial coefficient as follows.

$$\binom{0}{x} = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{otherwise,} \end{cases}$$

and for each integer x and each negative integer y,

$$\binom{x}{y} = 0, \binom{y}{x} = 0.$$

Then we can obtain that

$$p_{ijk}^{(n,q)} = \sum_{\beta=0}^{n-k} \binom{k}{k-i+\beta}\binom{i-\beta}{k-j+\beta}\binom{n-k}{\beta}(q-1)^{\beta}(q-2)^{i+j-k-2\beta}.$$

Therefore if $p|q$ for some prime number p, $p_{ijk}^{(n,q)} \equiv p_{ijk}^{(n,p)} \pmod p$. Since the intersection numbers are the structure constants of the adjacency algebra, $\mathbb{F}_pH(n,q) \cong \mathbb{F}_pH(n,p)$.

The Hamming scheme $H(n,q)$ is P-polynomial scheme (see [2]), and

$$B_1 = \begin{Bmatrix} * & 1 & \cdots & i & \cdots & n \\ 0 & q-2 & \cdots & i(q-2) & \cdots & n(q-2) \\ n(q-1) & (n-1)(q-1) & \cdots & (n-i)(q-1) & \cdots & * \end{Bmatrix}$$

In this paper, let p be a fixed prime number. Therefore we set $H(n) := H(n,p)$. And we denote the intersection numbers, the adjacency matrices, and the intersection matrices of $H(n)$ respectively by $p_{ijk}^{(n)}, A_i^{(n)}, B_i^{(n)}$ and so on.

We can consider the elements of Σ^n on $H(n)$ as the p-adic number of n figures. Therefore we index the adjacency matrices by the ordinary order on the p-adic number. Then it follows that

$$A_i^{(n+1)} = I \otimes A_i^{(n)} + K \otimes A_{i-1}^{(n)} \qquad \text{for } \forall i \in \{\, 0, 1, \ldots, n+1 \,\},$$

where I is the $p \times p$ identity matrix, K is the $p \times p$ matrix such that the diagonal entries are 0 and the others 1, $A_{-1}^{(n)} = A_{n+1}^{(n)} = O$ (the $p^n \times p^n$ zero matrix), and $\otimes$ is the Kronecker product. The Kronecker product $A \otimes B$ of matrices A and B is defined as follows. Suppose $A = (a_{ij})$. Then $A \otimes B$ is obtained by replacing the entry a_{ij} of A by the matrix $a_{ij}B$, for all i and j. The most important property of this product is that, provided the required products exist,

$$(A \otimes B)(X \otimes Y) = AX \otimes BY.$$

3 $H(p^r - 1)$

Since the intersection numbers are the structure constants of the adjacency algebra, if we consider over a field of characteristic p, we may consider the intersection numbers in modulo p. Since the size of the adjacency matrix of $H(n)$ is p^n, the adjacency algebra of $H(n)$ over a field of characteristic p is local and the unique irreducible representation is $A_i \mapsto p_{i\ i^*\ 0}$ (see [4, Theorem 3.4, Corollary 3.5]). So the prime field $\mathbb{F}_p$ of characteristic p is a splitting field for the adjacency algebra of $H(n)$ over $\mathbb{F}_p$.

In this paper, since we consider the adjacency algebras only over $\mathbb{F}_p$, we set $\mathfrak{A}_n := \mathbb{F}_p H(n)$.

By the definition,

$$B_1^{(p^r-1)} = \begin{pmatrix} B_1^{(p-1)} & & & \\ & B_1^{(p-1)} & & \\ & & \ddots & \\ & & & B_1^{(p-1)} \end{pmatrix},$$

therefore if we set $A_i^{(p-1)} = v_i(A_1^{(p-1)})$, it follows that for $0 \le \alpha \le p-1$,

$$A_{pi+\alpha}^{(p^r-1)} = v_\alpha(A_1^{(p^r-1)})A_{pi}^{(p^r-1)}.$$

Then since any $c_i^{(p-1)} \not\equiv 0 \pmod p$, we can define v_α over $\mathbb{F}_p$ for $0 \le \alpha \le p-1$. For calculating $B_{pi+\alpha}^{(p^r-1)}$, we prepare the following theorem and corollary.

Theorem 1. **(Lucas' theorem** [3, Theorem 3.4.1]) *Let p be prime, and let*

$$m = a_0 + a_1 p + \cdots + a_k p^k,$$

$$n = b_0 + b_1 p + \cdots + b_k p^k,$$

where $0 \le a_i, b_i < p$ for $i = 0, 1, \ldots, k-1$. Then

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} \quad (\text{mod p}).$$

Corollary 2. *We assume the same condition for theorem 1 and $0 \le \alpha, \beta < p$. Then*

$$\binom{pm+\alpha}{pn+\beta} \equiv \binom{m}{n}\binom{\alpha}{\beta} \quad (\text{mod p}).$$

Now we want to culculate $B_{pi+\alpha}^{(p^r-1)}$, that is the coefficients of $A_{pi+\alpha}^{(p^r-1)} A_{pj+\beta}^{(p^r-1)}$. But it is enough to investigate $A_{pi}^{(p^r-1)} A_{pj}^{(p^r-1)}$, i.e. $p_{pi\ pj\ k}^{(p^r-1)}$ because we know $v_\alpha(A_1^{(p^r-1)})v_\beta(A_1^{(p^r-1)})$.

Here we set $k = pk' + k''(0 \leq k'' \leq p-1)$. Using Lucas' theorem, we can obtain that if $p \mid k$, $p^{(p^r-1)}_{pi\ pj\ k} \equiv p^{(p^{r-1}-1)}_{ijk'}$, and if $p \nmid k$, $p^{(p^r-1)}_{pi\ pj\ k} \equiv 0$.

Thus

$$A^{(p^r-1)}_{pi+\alpha} A^{(p^r-1)}_{pj+\beta} = v_\alpha(A^{(p^r-1)}_1) v_\beta(A^{(p^r-1)}_1) A^{(p^r-1)}_{pi} A^{(p^r-1)}_{pj}$$

$$\equiv \sum_{k=0}^{p^{r-1}-1} \sum_{\gamma=0}^{p-1} p^{(p^{r-1}-1)}_{ijk} p^{(p-1)}_{\alpha\beta\gamma} A^{(p^r-1)}_{pk+\gamma}.$$

By the above argument, it follows that

$$B^{(p^r-1)}_{pi+\alpha} = B^{(p^{r-1}-1)}_i \otimes B^{(p-1)}_\alpha.$$

Repeating the same argument, we know that for all non-negative integer m such that $0 \leq m \leq p^r - 1$ and $m = m_0 p^0 + m_1 p^1 + \cdots + m_{r-1} p^{r-1}$,

$$B^{(p^r-1)}_m = B^{(p-1)}_{m_{r-1}} \otimes B^{(p-1)}_{m_{r-2}} \otimes \cdots \otimes B^{(p-1)}_{m_0}.$$

From this fact, we obtain that

$$\mathfrak{A}_{p^r-1} \cong \overbrace{\mathfrak{A}_{p-1} \otimes \mathfrak{A}_{p-1} \otimes \cdots \otimes \mathfrak{A}_{p-1}}^{r}.$$

Theorem 3. $\mathfrak{A}_{p-1} \cong \mathbb{F}_p C_p \cong \mathbb{F}_p[X]/\langle X^p \rangle$

Therefore the following theorem holds.

Theorem 4. *For all positive integer r, $\mathfrak{A}_{p^r-1}$ is isomorphic to the group algebra of the elementary abelian group of order p^r over $\mathbb{F}_p$.*

4 The structure of $\mathfrak{A}_n$

In the previous section, we considered the structure of $\mathfrak{A}_{p^r-1}$. To determine the structure of $\mathfrak{A}_n$, in general, we construct an algebra homomorphism $\mathfrak{A}_{n+1} \to \mathfrak{A}_n$.

From § 2.3, $A_i^{(n+1)} = I \otimes A_i^{(n)} + K \otimes A_{i-1}^{(n)}$. This means that $\mathfrak{A}_{n+1}$ is a subalgebra of $\mathfrak{A}_1 \otimes \mathfrak{A}_n$. The unique irreducible representation of $\mathfrak{A}_1$ is $A_0^{(1)} \mapsto 1, A_1^{(1)} \mapsto -1$.

Therefore we can define naturally the mapping f_{n+1} for each positive integer n by

$$f_{n+1} : \mathfrak{A}_{n+1} \to \mathfrak{A}_n$$
$$A_i^{(n+1)} = I \otimes A_i^{(n)} + K \otimes A_{i-1}^{(n)} \mapsto A_i^{(n)} - A_{i-1}^{(n)}.$$

Proposition 5. *For each positive integer n, $f_{n+1} : \mathfrak{A}_{n+1} \to \mathfrak{A}_n$ above is an algebra epimorphism.*

By Theorem 4, $\mathfrak{A}_{p^r-1}$ is isomorphic to $\mathbb{F}_p(\underbrace{C_p \times C_p \times \cdots \times C_p}_{r})$ for all positive integer r. Furthermore, there exists the algebra isomorphism g from the quotient ring $\mathfrak{P}_r = F_p[X_1, X_2, \ldots, X_r]/\langle X_1^p, \cdots, X_r^p\rangle$ of the polynomial ring of r variables over $\mathbb{F}_p$ to $\mathbb{F}_p(\underbrace{C_p \times C_p \times \cdots \times C_p}_{r})$ by $g(X_i) = 1 - x_i$. Therefore we can define an algebra isomorphism $s_r : \mathfrak{P}_r \to \mathfrak{A}_{p^r-1}$ by

$$s_r(X_i) = A_0^{(p^r-1)} - A_{p^{i-1}}^{(p^r-1)}.$$

We define a weight function wt on the set of the monomials of $\mathfrak{P}_r$ by

$$wt(X_i) = p^{i-1}, \; wt(\prod_j X_j^{k_j}) = \sum_j k_j p^{j-1}.$$

Proposition 6. *For all positive integers m such that $1 \le m \le p-1$,*

$$(A_0^{(p^r-1)} - A_{p^i}^{(p^r-1)})^m = m! \sum_{n=0}^{m} \binom{m}{n} (-1)^n A_{np^i}^{(p^r-1)}.$$

And if $i \neq j, 0 \le \alpha, \beta \le p-1$,

$$A_{\alpha p^i}^{(p^r-1)} A_{\beta p^j}^{(p^r-1)} = A_{\alpha p^i + \beta p^j}^{(p^r-1)}.$$

Let $Y_i = X_{i_0}^{k_0} X_{i_1}^{k_1} \cdots X_{i_s}^{k_s}$ be the monomial of $\mathfrak{P}_r$ such that $wt(Y_i) = i$. Then by the above two equations, the following Proposition holds.

Proposition 7.

$$s_r(Y_i) = (\prod_{j=0}^{s} k_j!) \sum_{n=0}^{p^r-1} \binom{i}{n} (-1)^n A_n^{(p^r-1)}.$$

Then the following theorem holds that is the main theorem in this paper.

Theorem 8. *We set* $\mathfrak{P} = \mathbb{F}_p[X_1, X_2, \cdots]/\langle X_1^p, X_2^p \cdots \rangle$, *and for all positive integer* n, *we set*

$$W_n = \langle\ x \mid x \textit{ is the monomial of } \mathfrak{P} \textit{ such that } wt(x) > n \rangle.$$

Then it holds that $\mathfrak{P}/W_n \cong \mathfrak{A}_n$ *as algebras.*

Proof. It is enough that we show that,

$$\mathfrak{P}_r/W_n \cong \mathfrak{A}_n \quad \text{for } n < p^r.$$

Furthermore it is enough that we show that for each positive integer n such that $n \leq p^r - 1$, $Y_n \in \mathrm{Ker} f_n f_{n+1} \cdots f_{p^r-1} s_r$, but $f_n f_{n+1} \cdots f_{p^r-1} s_r(Y_n) = 0$. □

Remark 1 We set $G_{n,q} = S_q\ wr\ S_n$, $H_{n,q} = S_{q-1}\ wr\ S_n$ for positive integers n, q. Let K be a field. Then $KH(n,q)$ and the Hecke algebra $\mathrm{End}_{KG_{n,q}}(1_{H_{n,q}}^{G_{n,q}})$ are isomorphic as algebras (see [2, III.2]). Therefore we also could decide the structure of $\mathrm{End}_{KG_{n,q}}(1_{H_{n,q}}^{G_{n,q}})$. In particular, Theorem 4 means that for all positive integer r, if $n = p^r - 1$, the Hecke algebra $\mathrm{End}_{\mathbb{F}_p G_{n,p}}(1_{H_{n,p}}^{G_{n,p}})$ is isomorphic to the group algebra of the elementary abelian group of order p^r.

Acknowledgement

The author thanks to A. Hanaki for valuable suggestions and comments.

References

[1] Z. Arad, E. Fisman, and M. Muzychuk, "Generalized table algebras," Israel J. Math. **144** (1999), 29-60.

[2] E. Bannai and T. Ito, Algebraic Combinatorics. I. Association Schemes, Benjamin-Cummings, Menlo Park, CA, 1984.

[3] P. -J. Cameron, Combinatorics: topics, techniques, algorithms, Cambridge University Press, 1994.

[4] A. Hanaki, "Locality of a modular adjacency algebra of an association scheme of prime power order," to appear in Arch. Math.

[5] A. Hanaki, "Semisimplicity of Adjacency Algebras of Association Schemes," J. Alg. **225** (2000), 124-129.