Association Schemes of Prime Order and Related Topics

Akihide Hanaki (Shinshu University)
joint work with
Katsuhiro Uno (Osaka Kyoiku University)

July 6, 2005

Let X be a finite set, G a collection of subsets of $X \times X$. For $g \in G$, define $\sigma_g \in M_X(\mathbb{Z})$ by

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

(X, G) is called an *association scheme* (or briefly a scheme) if
(1) $\bigcup_{g \in G} g = X \times X$ (disjoint),
(2) $G \ni 1 = \{(x,x) \mid x \in X\}$,
(3) if $g \in G$, then $G \ni g^* = \{(y,x) \mid (x,y) \in g\}$,
(4) and $\sigma_f \sigma_g = \sum_{h \in G} p_{fg}^h \sigma_h$ for some $p_{fg}^h \in \mathbb{Z}_{\geq 0}$.

This is also called a *homogenious coherent configulation*.

An association scheme (X, G) is said to be *commutative* if

$$p_{fg}^h = p_{gf}^h$$

for all $f, g, h \in G$.

We can define a $\mathbb{Z}$-algebra $\mathbb{Z}G = \bigoplus_{g \in G} \mathbb{Z}\sigma_g$. For any commutative ring R with identity, we can define

$$RG = R \otimes_{\mathbb{Z}} \mathbb{Z}G$$

and call this the *adjacency algebra* of G over R. It is clear that (X, G) is commutative if and only if the algebra $\mathbb{Z}G$ is commutative.

It is well known that $\mathbb{C}G$ is a semisimple algebra. We denote the set of irreducible characters of $\mathbb{C}G$ by $\mathrm{Irr}(G)$. The *character table* of G means the table of entries $\chi(\sigma_g)$ ($\chi \in \mathrm{Irr}(G)$, $g \in G$).

It is easy to see that $\chi(\sigma_g)$ is an algebraic integer.

Motivation.

For $f, g \in G$, put $fg = \{h \in G \mid p_{fg}^h > 0\}$. For $H, K \subset G$, put $HK = \bigcup_{h \in H} \bigcup_{k \in K} hk$. These are called the *complex products*. A non-empty subset H of G is called *closed* if

$$HH \subset H.$$

A scheme (X, G) is said to be *primitive* if it has no non-trivial closed subset.

If H is a closed subset of G, then we can define subschemes and the quotient scheme, and G can be regarded as a extension of them. So primitive schemes are important in the theory of schemes, like as simple groups in group theory.

Especially, if $|X|$ is a prime number, then (X, G) is primitive. But the classification of such schemes is unknown.

p	$\sharp$	p	$\sharp$	p	$\sharp$(Schurian)
2	1	11	4	23	22(4)
3	2	13	6	29	26(6)
5	3	17	5	31	$\geq 1,000$(8)
7	4	19	7(6)		

Schurian schemes (association schemes defined by transitive permutation groups) of prime order must be cyclotomic and easily we can classify them. For order up to 17, there are only Schurian schemes. There are many non-Schurian schemes of order greater than 17. But their adjacency algebras are algebraically isomorphic to Schurian schemes for known schemes. So we want to classify the structure of adjacency algebras and the character tables.

Main Result.

Theorem. Let (X, G) be an association scheme with $|X| = p$ a prime and $|G| = d + 1$. Then (X, G) is commutative. Moreover, if we suppose that the minimal splitting field of it is abelian, then the character table of it is same as that of the cyclotomic scheme $Cyc(p, d)$.

Remark. In the famous book by Bannai-Ito, they asked whether the minimal splitting field of a commutative scheme is abelian. If this is true, then the character table of an association scheme of prime order is completely determined.

Commutativity.

We denote the *valency* of $g \in G$ by n_g, namely $n_g = p^1_{gg^*}$. For $S \subset G$, we write $n_S = \sum_{g \in S} n_g$. Especially $n_G = |X|$. The map $\sigma_g \mapsto n_g$ is a character of G. It is called the *trivial charcter* of G and denoted by 1_G.

Fix a prime number p.

Lemma [Ha 2002]. Suppose that n_G is a p-power. Let K be a field of characteristic zero containing all character values $\chi(\sigma_g)$, and let $\mathfrak{P}$ be a prime ideal of K lying above $p\mathbb{Z}$. Then

$$\chi(\sigma_g) \equiv \chi(1) n_g \pmod{\mathfrak{P}}$$

for all $g \in G$ and $\chi \in \mathrm{Irr}(G)$.

Lemma. Suppose that $n_G = p$. Then all nontrivial irreducible characters of G are algebraically conjugate.

Proof. Let χ be a nontrivial irreducible character of G. Note that an algebraic conjugate of an irreducible character is again an irreducible character. Put Φ the sum of all algebraic conjugates of χ, and Ψ the sum of all nontrivial irreducible characters which are not algebraically conjugate to χ. Then the values of Φ and Ψ are rational integers. If Ψ is zero, then the assertion holds, so we assume that $\Psi \neq 0$.

By the previous lemma, there exist rational integers u_g $(g \in G)$ such that $\Phi(\sigma_g) = \Phi(1)n_g - u_g p$. Similarly there exist rational integers v_g $(g \in G)$ such that $\Psi(\sigma_g) = \Psi(1)n_g - v_g p$.

By the orthogonality relation, we have

$$\begin{aligned} 0 &= \sum_{g\in G} \frac{1}{n_g} 1_G(\sigma_{g^*})\Phi(\sigma_g) = \sum_{g\in G} \Phi(\sigma_g) \\ &= \sum_{g\in G} (\Phi(1)n_g - u_g p) = p\left(\Phi(1) - \sum_{g\in G} u_g\right). \end{aligned}$$

We have

$$\sum_{g\in G} u_g = \Phi(1)$$

and similarly

$$\sum_{g\in G} v_g = \Psi(1).$$

Again by the orthogonality relation,

$$
\begin{aligned}
0 &= \sum_{g\in G}\frac{1}{n_g}\Phi(\sigma_{g^*})\Psi(\sigma_g) = \sum_{g\in G}\frac{1}{n_g}(\Phi(1)n_{g^*} - u_{g^*}p)(\Psi(1)n_g - v_g p)\\
&= \sum_{g\in G}\Phi(1)\Psi(1)n_g - \sum_{g\in G}\Phi(1)v_g p - \sum_{g\in G}\Psi(1)u_{g^*}p + \sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g p^2\\
&= p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) + \sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g p^2\\
&= -p\Phi(1)\Psi(1) + \sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g p^2,
\end{aligned}
$$

so we have

$$\Phi(1)\Psi(1) = p\sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g.$$

But $\Phi(1)\Psi(1)$ is relatively prime to p and $\sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g$ is a p-integer, namely every n_g is relatively prime to p. So this is a contradiction. $\square$

Since the Frame number

$$\mathcal{F}(G) = |X|^{|G|} \frac{\prod_{g \in G} n_g}{\prod_{\chi \in \mathrm{Irr}(G)} m_\chi{}^{(\chi(1)^2)}}$$

is a rational integer, we have the following.

Lemma [Bannai-Ito's book]. If the multiplicities of all nontrivial irreducible characters of G are constant, then so are the valencies of all nontrivial relations.

Lemma [Arad-Fisman-Muzychuk 1999].
Suppose $n_G = p$ is a prime number. If the valencies of all nontrivial relations are constant, then (X, G) is commutative.

Theorem. Suppose $n_G = p$ is a prime number. Then (X, G) is commutative, and the Frame number is a p-power.

Discriminants and Frame numbers

For a $\mathbb{Z}$-free $\mathbb{Z}$-algebra A, we define the *discriminant* as follows. Let $\{a_1, a_2, \cdots, a_r\}$ be a $\mathbb{Z}$-basis of A. Then we put

$$d(A) = \det(\mathrm{Tr}(a_i a_j))$$

and call this the discriminant of A. Here Tr is the trace of the regular representation of A. If B is a subalgebra of A with the same rank, then $|d(A)|$ is a divisor of $|d(B)|$.

For an algebraic number field K, the ring of integers $\mathcal{O}_K$ is a $\mathbb{Z}$-free $\mathbb{Z}$-algebra and we have $d(\mathcal{O}_K)$ is the same as the discriminant $d(K)$ of K in algebraic number theory.

For a commutative scheme (X, G), it is known that

$$\mathcal{F}(G) = |d(\mathbb{Z}G)|.$$

Let K be the minimal splitting field of (X, G). Fix $\chi \in \mathrm{Irr}(G) \setminus \{1_G\}$ and put $K' = \chi(\mathbb{Q}G)$. Then $\mathbb{Q}G \cong \mathbb{Q} \oplus K'$ and K' is a subfield of K. Also we can say that K is generated by K' and its conjugates.

We can see that $\mathbb{Z}G$ is a $\mathbb{Z}$-subalgebra of $\mathbb{Z} \oplus \mathcal{O}_{K'}$. So $|d(K')|$ divides the Frame quotient $\mathcal{F}(G)$. Since $\mathcal{F}(G)$ is a p-power, $|d(K')|$ and $|d(K)|$ are also p-powers.

We assume that

Assumption A. The minimal splitting field K is an abelian extension of $\mathbb{Q}$.

By Kronecker-Weber's theorem, K is a subfield of some cyclotomic field. Let N be the conductor of K, namely N is the

smallest positive integer such that K is a subfield of $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive N-th root of unity. It is known that a prime number ℓ ramifies in $K/\mathbb{Q}$ if and only if ℓ is a divisor of N. Also ℓ ramifies in $K/\mathbb{Q}$ if and only if ℓ is a divisor of $|d(K)|$. So we can say that $N = p^a$ for some non-negative integer a. Then, since $Gal(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}) \cong (\mathbb{Z}/p^a\mathbb{Z})^\times$ has the unique subgroup of index d, we can say that $N = p$ and we have the following.

Lemma. Suppose Assumption A. Then K is the unique subfield of $\mathbb{Q}(\zeta_p)$ with $\dim_{\mathbb{Q}} K = d$ and $Gal(K/\mathbb{Q})$ is a cyclic group of order d.

Remark. Assumption A is equivalent to that $K = K'$.

Question. Suppose d is a divisor of $p-1$. Is there a non-normal extension K' of $\mathbb{Q}$ such that $\dim_{\mathbb{Q}} K' = d$ and $|d(K')| = p^{d-1}$?

Put $k = (p-1)/d$. Then $n_g = k$ for all $1 \neq g \in G$, and $m_\chi = k$ for all $1_G \neq \chi \in \mathrm{Irr}(G)$.

Put $\alpha = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$.

Let τ is a generator of the cyclic group $Gal(K/\mathbb{Q})$.

The character table of $Cyc(p,d)$ is as follows.

1	1	k	k	$\cdots$	k	1
φ	1	α	α^τ	$\cdots$	$\alpha^{\tau^{d-1}}$	k
φ^τ	1	α^τ	α^{τ^2}	$\cdots$	α	k
		$\cdots$	$\cdots$	$\cdots$		
$\varphi^{\tau^{d-1}}$	1	$\alpha^{\tau^{d-1}}$	α	$\cdots$	$\alpha^{\tau^{d-2}}$	k

Lemma. Use the above notations, then we have $\sum_{i=0}^{d-1} \alpha^{\tau^i} = -1$ and

$$\sum_{i=0}^{d-1} \alpha^{\tau^i} \overline{\alpha}^{\tau^{i+j}} = \begin{cases} p-k & \text{if } j \equiv 0 \pmod{d}, \\ 0 & \text{otherwise.} \end{cases}$$

Now we consider the character table of (X, G). It looks like the following.

	1	g_1	g_2		g_d	
1_G	1	k	k	$\cdots$	k	1
χ	1	β_1	β_2	$\cdots$	β_d	k
χ^τ	1	β_1^τ	β_2^τ	$\cdots$	β_d^τ	k
		$\cdots$	$\cdots$	$\cdots$		
$\chi^{\tau^{d-1}}$	1	$\beta_1^{\tau^{d-1}}$	$\beta_2^{\tau^{d-1}}$	$\cdots$	$\beta_d^{\tau^{d-1}}$	k

We fix $g_j \in G$ for a while. Since $\{\alpha^{\tau^i} \mid i = 0, 1, \cdots, d-1\}$ is an

integral basis of $\mathcal{O}_K$ and $\beta_j \in \mathcal{O}_K$, there exist $b_s \in \mathbb{Z}$ such that

$$\beta_j = \sum_{s=0}^{d-1} b_s \alpha^{\tau^s}.$$

By the second orthogonality relation with respect to g_j and 1, we have

$$0 = k\left(1 + \sum_{i=0}^{d-1} \beta_j^{\tau^i}\right) = k\left(1 - \sum_{s=0}^{d-1} b_s\right).$$

So we have $\sum_{s=0}^{d-1} b_s = 1$.

Again by the second orthogonality relation with respect to g_j and itself, we have

$$pk = k\left(k + \sum_{i=0}^{d-1} \beta_j^{\tau^i} \overline{\beta_j}^{\tau^i}\right) = k\left(k + (p-k)\sum_{s=0}^{d-1} {b_s}^2\right).$$

This means $\sum_{s=0}^{d-1} {b_s}^2 = 1$, and consequently we have that the only one $b_s = 1$ and the others are zero. Namely, $\beta_j = \alpha^{\tau^s}$ for some $0 \leq s < d$.

The character table does not contain the identical columns. This shows that the character table of (X, G) is the same as that of $Cyc(p, d)$ by a suitable reordering of G.

Theorem. Let (X, G) be an association scheme of prime order p with $|G| = d + 1$. Under Assumption A, the character table of (X, G) is the same as that of the cyclotomic scheme $Cyc(p, d)$.

The idea of our consideration is based on the theory of p-blocks with cyclic defect groups. We generalize it.

Let (X, G) be a commutative scheme, K a Galois field of finite degree, and $\mathfrak{P}$ a prime ideal of K lying above $p\mathbb{Z}$. We suppose K is large enough. The *inertia group* of $\mathfrak{P}$ is defined by

$$T := \{\tau \in Gal(K/\mathbb{Q}) \mid \mathfrak{P}^\tau = \mathfrak{P}, \text{ and } \alpha^\tau - \alpha \in \mathfrak{P}\ \forall \alpha \in \mathcal{O}_K\}.$$

The *inertia field* of $\mathfrak{P}$ is the Galois correspondence of T, and it will be denoted by L. It is known that p is unramified in $L/\mathbb{Q}$. Namely $p \notin \mathfrak{p}^2$ for a prime ideal $\mathfrak{p}$ of L lying above $p\mathbb{Z}$.

The discrete valuation ring defined by K and $\mathfrak{P}$ will be denoted by $\mathcal{O}_{\mathfrak{P}}$, and the quotient field will be denoted by $K_{\mathfrak{P}}$.

For $\chi, \varphi \in \mathrm{Irr}(G)$, we say that they belong to the same $\mathfrak{P}$-*block* if

$$\chi(\sigma_g) \equiv \varphi(\sigma_g) \pmod{\mathfrak{P}}.$$

Of cource, this is an equivalent relation, and an equivalent class will be denoted by $\mathrm{Irr}_{\mathfrak{P}}(B)$ or briefly by $\mathrm{Irr}(B)$.

Proposition. The set $\mathrm{Irr}(B)$ is a minimal subset of $\mathrm{Irr}(G)$ such that $e_B = \sum_{\chi \in \mathrm{Irr}(B)} e_\chi \in \mathcal{O}_{\mathfrak{P}} G$.

Let ν_p denote the valuation on $K_{\mathfrak{P}}$ with $\nu_p(p) = 1$.

Proposition. $\nu_p(n_G) \leq \nu_p(\sum_{\chi \in \mathrm{Irr}(B)} m_\chi)$.

For $\chi,\ \varphi \in \mathrm{Irr}(G)$, we say that χ and φ are $\mathfrak{P}$-*conjugate* if there exists $\tau \in Gal(K/L)$ such that $\chi^\tau = \varphi$, where L is the inertia field of $\mathfrak{P}$. Though $\mathrm{Irr}(B)$ is not closed by algebraically conjugate, we have the following.

Proposition. For $\chi \in \mathrm{Irr}(G)$ and $\tau \in Gal(K/L)$, χ and χ^τ belong to the same block. Namely, $\mathrm{Irr}(B)$ is closed by $\mathfrak{P}$-conjugate.

We say that (X, G) is p'-*valenced* if $p \nmid n_g$ for all $g \in G$. If (X, G) is p'-valenced, then the adjacency algebra $F_{\mathfrak{P}}G$ is a symmetric algebra, where $F_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$.

Now we are interested in the number of $Gal(K/L)$-orbits of $\mathrm{Irr}(B)$. For $\chi \in \mathrm{Irr}(G)$, we denote r_χ for the length of the $Gal(K/L)$-orbit of $\mathrm{Irr}(G)$ containing χ. We fix $\chi \in \mathrm{Irr}(B)$.

Proposition. Suppose (X, G) is a commutative p'-valenced scheme. If $\nu_p(m_\chi) \geq \nu_p(n_G)$, then $\mathrm{Irr}(B) = \{\chi\}$. Moreover, $\nu_p(m_\chi) = \nu_p(n_G)$ in this case.

Proposition. Let (X, G) be a commutative scheme. If $\nu_p(m_\chi) < \nu_p(n_G)$, then $|\mathrm{Irr}(B)| \geq 2$.

Proposition. Suppose (X, G) is a commutative p'-valenced scheme. If $\nu_p(m_\chi) + 1 = \nu_p(n_G)$ and $\nu_p(r_\chi) \geq 1$, then $\mathrm{Irr}(B) = \{\chi^\tau \mid \tau \in Gal(K/L)\}$.

Proposition. Let (X, G) be a commutative p'-valenced scheme. Suppose $\chi \in \mathrm{Irr}(B)$ satisfies $\nu_p(m_\chi) + 1 = \nu_p(n_G)$. Then the number of $Gal(K/L)$-orbits of $\mathrm{Irr}(B)$ is at most two, and $\nu_p(m_\varphi) + 1 = \nu_p(n_G)$ for every $\varphi \in \mathrm{Irr}(B)$.

Example (Shimabukuro). Let (X, G) be the Johnson scheme $J(2(p-1), p-1)$. Then it is p'-valenced and $\nu_p(n_G) = 1$. Moreover all character values are rational. So we can conclude that $|\mathrm{Irr}(B)| \leq 2$ for any $B \in \mathrm{Bl}(G)$.

The block containing the trivial character $1_G : \sigma_g \mapsto n_g$ is called the *principal block* of G and denoted by $B_0(G)$ or B_0.

Corollary. Suppose (X, G) is a commutative p'-valenced scheme with $\nu_p(n_G) = 1$. Then $\mathrm{Irr}(B_0)$ has exactly two $Gal(K/L)$-orbits. Moreover, these $Gal(K/L)$-orbits are $Gal(K/\mathbb{Q})$-orbits. (Of course, one of them is $\{1_G\}$.) Namely, all nontrivial characters in $\mathrm{Irr}(B_0)$ are algebraically conjugate.

Our key lemma is a special case of this fact.

END.