Davenport-Hasse theorem and cyclotomic association schemes

E. Bannai
Department of Mathematics
Kyushu University

A. Munemasa
Department of Mathematics
Osaka Kyoiku University

July 24, 1990

1 Cyclotomic association schemes

In this section, we define cyclotomic association scheme (or cyclotomic scheme) of class e on $GF(q)$. We shall establish the relationship with its character table and Gauss sums.

Definition. Let q be a prime power and e be a divisor of $q-1$. Fix a generator α of the multiplicative group of $GF(q)$. Then $\langle\alpha^e\rangle$ is a subgroup of index e and its cosets are $\langle\alpha^e\rangle\alpha^i$, $i = 0, \dots, e-1$. Define

$$R_0 = \{(x,x) | x \in GF(q)\}$$
$$R_i = \{(x,y) | x, y \in GF(q), x - y \in \langle\alpha^e\rangle\alpha^{i-1}\},\ (1 \le i \le e)$$
$$\mathcal{R} = \{R_i | 0 \le i \le e\}$$

Then $(GF(q), \mathcal{R})$ forms an association scheme and is called the cyclotomic scheme of class e on $GF(q)$. The character table of the cyclotomic scheme is the first eigenmatrix of the association scheme. We will not give a formal definition here, instead, we show how to construct the character table of cyclotomic scheme from the character table of elementary abelian group. For a discussion of association scheme in general and the definition of the character table, see [2].

Consider the character table T of the additive group of $F = GF(q)$:

$$T = (\chi(a))_{\chi \in \hat{F}, a \in F}$$

The rows of T are indexed by the set of additive characters, the columns of T are indexed by F. The coset decomposition by the subgroup $\langle\alpha^e\rangle$ is a partition of $F - \{0\}$. Consider the q by $e+1$ matrix T' whose rows are

$$(1, \sum_{\beta \in \langle\alpha^e\rangle} \chi(\beta), \sum_{\beta \in \langle\alpha^e\rangle\alpha} \chi(\beta), \dots, \sum_{\beta \in \langle\alpha^e\rangle\alpha^{e-1}} \chi(\beta))$$

where χ runs through $\hat{F}$. Then T' has exactly $e+1$ distinct rows. The character table P of the cyclotomic scheme is the $e+1$ by $e+1$ submatrix of T' consisting of $e+1$ distinct rows. The rows of P can be rearranged in such a way that

$$P = \begin{pmatrix} 1 & f & \cdots & f \\ 1 & & & \\ \vdots & & P_0 & \\ 1 & & & \end{pmatrix}$$

with $q = 1 + ef$, $P_0 = \sum_{i=0}^{e-1} \eta_i C^i$, where C is the e by e matrix:

$$C = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{pmatrix}$$

The matrix P_0 is called the principal part of the character table. The number η_i's are called Gaussian periods, given by

$$\eta_i = \sum_{\beta \in \langle \alpha^e \rangle \alpha^{i-1}} \chi(\beta)$$

for a fixed nontrivial additive character χ. Let T be a nonsingular matrix such that

$$T^{-1}CT = \begin{pmatrix} 1 & & & & \\ & \xi & & & \\ & & \xi^2 & & \\ & & & \ddots & \\ & & & & \xi^{e-1} \end{pmatrix}$$

where ξ is a primitive e-th root of unity. Then we have

$$\begin{aligned} T^{-1}P_0T &= \sum_{i=0}^{e-1} \eta_i T^{-1}C^iT \\ &= \mathrm{diag}(\sum_{i=0}^{e-1} \eta_i, \sum_{i=0}^{e-1} \eta_i \xi^i, \ldots, \sum_{i=0}^{e-1} \eta_i \xi^{(e-1)i}) \\ &= \mathrm{diag}(G(\psi^0, \chi), G(\psi, \chi), \ldots, G(\psi^{e-1}, \chi)) \end{aligned}$$

where ψ is the multiplicative character of F defined by $\psi(\alpha^j) = \xi^j, j = 0, 1, \ldots$. Therefore, the eigenvalues of P_0 are Gauss sums.

Theorem 1 (Davenport-Hasse [6]) *Let $K = GF(q^s)$ be an extension of $F = GF(q)$, χ an additive character of F, ψ a multiplicative character of F. Let*

$$\tilde{\psi} = \psi \circ \mathbf{N}_{K/F}$$

$$\tilde{\chi} = \chi \circ \mathbf{Tr}_{K/F}$$

Then we have

$$G(\tilde{\psi}, \tilde{\chi}) = (-1)^{s-1} G(\psi, \chi)^s$$

Suppose that $\tilde{P_0}$ is the principal part of the first eigenmatrix of the cyclotomic scheme of class e on $GF(q^s)$. Then, by a suitable rearrangement of rows and columns, the following matrix equation holds

$$\tilde{P_0} = (-1)^{s-1} P_0^s$$

This is simply a direct consequence of Davenport-Hasse theorem.

Example. Let $q = r^2$ be a square and take $e = r + 1$. Then $\langle \alpha^e \rangle$ is the multiplicative group of $GF(r)$. One can readily see that $P_0 = rI - J$. The spectrum of P_0 is $(-1)^1 (r)^r$. Notice that this fact is essentially equivalent to Theorem 2. One can apply Davenport-Hasse theorem to conclude that the principal part of the first eigenmatrix of the cyclotomic association schemes of class $r + 1$ on $GF(r^{2s})$ is given by

$$-(-r)^s I + \frac{(-r)^s - 1}{r + 1} J$$

Theorem 2 *Let $q = r^2$ be a square, ψ a multiplicative character of order $r + 1$ of $GF(q)$. Then there exists an additive character χ such that $G(\psi^i, \chi) = r$ for $1 \leq i \leq r$.*

This theorem is a direct consequence of Stickelberger's theorem [11].

Definition. Let $(X, \mathcal{R})$ be an e-class commutative association scheme. The association scheme is called pseudocyclic if the multiplicities m_1,m_2, …,m_d coincide each other. Notice that if $(X, \{R_i\}_{0 \leq i \leq d})$ is pseudocyclic, then the valencies $k_i = p_i(0)$ $(1 \leq i \leq d)$ coincide each other. More precisely,

Proposition 3 *Let $(X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme of class d over a finite set X of cardinality $v = 1 + kd$, with $k = k_i$ for $1 \leq i \leq d$. Let*

$$\mathcal{B} = \{R_i(x) \mid x \in X, 1 \leq i \leq d\}$$

The following are equivalent.
(i) $(X, \{R_i\}_{0 \leq i \leq d})$ *is pseudocyclic.*
(ii) $\sum_{i=1}^{d} p_{ii}^j = k - 1$.
(iii) $\mathcal{B}$ *is a* 2-$(v, k, k - 1)$-*design.*

Proof. See [[4], Proposition 2.2.7] □

A pseudocyclic association scheme has the first eigenmatrix of the form

$$\begin{pmatrix} 1 & f & \cdots & f \\ 1 & & & \\ \vdots & & P_0 & \\ 1 & & & \end{pmatrix}$$

with $|X| = 1 + ef$.

2 Amorphic association schemes

In this section, we state a theorem of A. V. Ivanov on amorphic association schemes, and present the classification of amorphic cyclotomic scheme due to Baumert, Mills and Ward [3]. Throughout this section, we let p be a prime, ζ a primitive p-th root of unity. We denote the all one matrix by the same notation J regardless the size, since no confusion is likely.

First let us define amorphic association schemes. Let $\{\Lambda_j\}_{0\leq j\leq d'}$ be a partition of $\{0, 1, \ldots, d\}$ with $\Lambda_0 = \{0\}$. Let $R_{\Lambda_j} = \bigcup_{i\in\Lambda_j} R_i$. If $(X, \{R_{\Lambda_j}\}_{0\leq j\leq d'})$ becomes an association scheme, then it is said to be a *fusion* scheme of the association scheme $(X,\{R_i\}_{0\leq i\leq d})$. The association scheme $(X,\{R_i\}_{0\leq i\leq d})$ is called *amorphic* if $(X, \{R_{\Lambda j}\}_{0\leq j\leq d'})$ is a fusion scheme of the association scheme $(X, \{R_i\}_{0\leq i\leq d})$ for any partition $\{\Lambda_j\}_{0\leq j\leq d'}$ with $\Lambda_0 = \{0\}$.

There is a simple criterion in terms of the first eigenmatrix P for a given partition $\{\Lambda_j\}_{0\leq j\leq d'}$ to give rise to a fusion scheme (due to Bannai [1], Muzichuk [10]): there exists a partition $\{\Delta_i\}_{0\leq j\leq d'}$ of $\{0, 1, \ldots, d\}$ with $\Delta_0 = \{0\}$ such that each (Δ_i, Λ_j) block of P has a constant row sum. The constant row sum turns out to be the (i, j) entry of the first eigenmatrix of the fusion scheme. Examples of amorphic association schemes are derived from affine planes. The isomorphism classes of affine planes of order q is in one-to-one correspondence with the isomorphism classes of association schemes having the same parameters as the cyclotomic scheme of class $q + 1$ on $GF(q^2)$.

Theorem 4 (A. V. Ivanov [9]) *Let $(X, \mathcal{R})$ be an amorphic association scheme of class d, $d \geq 3$, on n vertices. Then n is a square, say $n = m^2$. If we write $k_i = p^0_{ii}$, $\lambda_i = p^i_{ii}$, $\mu_i = p^j_{ii}$, $(j \neq i, 0)$, then either*

(i) *there exist integers g_i, $(1 \leq i \leq d)$ such that*

$$\begin{aligned} k_i &= g_i(m-1) \\ \lambda_i &= (g_i-1)(g_i-2)+m-2 \\ \mu_i &= g_i(g_i-1) \end{aligned}$$

or

(ii) *there exist integers* g_i, $(1 \leq i \leq d)$ *such that*

$$\begin{array}{rcl} k_i & = & g_i(m+1) \\ \lambda_i & = & (g_i+1)(g_i+2)-m-2 \\ \mu_i & = & g_i(g_i+1) \end{array}$$

Definition. An amorphic association scheme satisfying (i) (resp. (ii)) in Theorem 4 is said to be of Latin square type (resp. negative Latin square type).

The following lemma is immediate from Theorem 4.

Lemma 5 *A pseudocyclic association scheme of class* d *is amorphic if and only if the principal part of the first eigenmatrix is a linear combination of* J *and* I, *where* J *is the all one matrix of size* d *and* I *is the identity matrix of size* d.

Therefore the cyclotomic scheme of class $r+1$ on $GF(r^{2s})$ is amorphic, in view of example in the previous section. Since any fusion scheme of amorphic association scheme is also amorphic, the cyclotomic scheme of class e on $GF(r^{2s})$ is amorphic, if e divides $r+1$. These are the only amorphic cyclotomic schemes, as we will see in Theorem 7. It should be noted that the first eigenmatrix of an amorphic pseudocyclic association scheme is uniquely determined by the number of classes and the number of vertices. Let us describe the parameters of pseudocyclic amorphic association schemes of class at least 3. Let the number of vertices be m^2, $m^2-1=ef$, where e is the number of classes. We have $f=g(m-1)$ for some integer g, if the association scheme is of Latin square type, $f=g(n+1)$ for some integer g, if it is of negative Latin square type. In what follows, the upper sign of the double sign corresponds to the case of Latin square type, the lower corresponds to the case of negative Latin square type. We will express the parameters and the eigenvalues in terms of e and g.

$$m^2-1=ef=eg(m\mp 1)$$

$$m=eg\mp 1$$

$$f=g(eg\mp 2)$$

Suppose that the first eigenmatrix is of the form

$$\begin{pmatrix} 1 & f & \cdots & f \\ 1 & a & & b \\ \vdots & & \ddots & \\ 1 & b & & a \end{pmatrix}$$

By the orthogonality relation, we have

$$1+a+(e-1)b=0$$

$$f+a^2+(e-1)b^2=ef+1$$

$$b = \frac{-1 + (eg \mp 1)}{e}, \frac{-1 - (eg \mp 1)}{e}$$

The integrality of b forces that $b = \mp g$. Then $a = -1 \pm (e-1)g$. The intersection numbers are

$$p_{ii}^{i} = g^2 - 1 \pm g(e-3), 1 \leq i \leq e$$

$$p_{ii}^{j} = g(g \mp 1), 1 \leq i \leq e, 1 \leq j \leq e, i \neq j$$

$$p_{ij}^{k} = g^2, 1 \leq i \leq e, 1 \leq j \leq e, 1 \leq k \leq e, i \neq j, j \neq k, k \neq i$$

Now we present a short proof of the classification of amorphic cyclotomic association schemes due to Baumert, Mills and Ward [3]. The following lemma, appeared in [8], plays a key role in our proof.

Lemma 6 (Suzuki) *Let G be a finite abelian group and let ϵ be a complex-valued function on G. Suppose*

(i) $|\epsilon(a)| = 1$ *for any nonidentity element a of G,*

(ii) *there exists some $\alpha \in \mathbf{C}$ such that $(\epsilon, \chi)_G \in \{\alpha, \alpha+1, \alpha-1\}$ for any irreducible character χ of G.*

Then $\epsilon = \psi$ on $G - \{1_G\}$ or $\epsilon = -\psi$ on $G - \{1_G\}$ for some irreducible character ψ of G.

Theorem 7 *Let p be a prime. A cyclotomic scheme of class e on $GF(p^{2s})$ is amorphic if and only if there exists a divisor r of s such that e divides $p^r + 1$.*

Proof. We may assume $e \geq 3$, since the case $e = 2$ is trivial. Let $p^{2s} - 1 = ef$. If the scheme is of Latin square type, then f is divisible by $p^s - 1$. Thus e divides $p^s + 1$.

We prove the assertion for the case of negative Latin square type by induction. Since f is divisible by $p^s + 1$, we see that e divides $p^s - 1$, that is, there exists a cyclotomic scheme of class e on $K = GF(p^s)$. We aim to show that this scheme is amorphic. Let P_0 be the principal part of its first eigenmatrix. Let $L = GF(p^{2s})$,

$$\tilde{\psi} = \psi \circ \mathbf{N}_{L/K}$$

$$\tilde{\chi} = \chi \circ \mathbf{Tr}_{L/K}$$

By Davenport–Hasse Theorem, we have

$$-(T^{-1} P_0 T)^2 = \mathrm{diag}((G(\tilde{\psi}^0, \tilde{\chi}), G(\tilde{\psi}, \tilde{\chi}), \ldots, G(\tilde{\psi}^{e-1}, \tilde{\chi}))$$

For an appropriate choice of χ, we have

$$G(\tilde{\psi}^j, \tilde{\chi}) = -p^s, \ j = 1, \ldots, e-1.$$

This implies

$$G(\psi^j, \chi) = \epsilon(j)\sqrt{p^s}, \ j = 1, \ldots, e-1,$$

$$\sum_{i=0}^{e-1} \eta_i \xi^{ij} = \epsilon(j)\sqrt{p^s},\ j = 1, \ldots, e-1,$$

where $\epsilon(j) = \pm 1$. It follows that

$$\eta_i = \frac{1}{e}\left(-1 + \sqrt{p^s}\sum_{j=1}^{e-1} \epsilon(j)\xi^{-ij}\right)$$

Suppose that s is odd. Then η_i belongs to $\mathbf{Q}(\sqrt{p}, \xi)$, which has an automorphism τ fixing ξ and sending $\sqrt{p}$ to $-\sqrt{p}$. Then $\eta_i + \eta_i^\tau = -2/e$, which is a contradiction since $e \geq 3$. Therefore s is even. Now we see that η_i belongs to $\mathbf{Q}(\xi) \cap \mathbf{Q}(\zeta) = \mathbf{Q}$. Since

$$\sqrt{p^s}(\eta_i - \eta_0) = \frac{p^s}{e}(\sum_{j=1}^{e-1} \epsilon(j)\xi^{-ij} - 1)$$

and $p^s \equiv 1 \bmod e$, we see that $\frac{1}{e}\sum_{j=1}^{e-1} \epsilon(j)\xi^{-ij}$ is an integer, hence it must be 0 or ± 1. This implies

$$\sum_{j=1}^{e-1} \epsilon(j)\xi^{-ij} \in \{\frac{1}{e}\sum_{j=1}^{e-1}, \frac{1}{e}\sum_{j=1}^{e-1} +1, \frac{1}{e}\sum_{j=1}^{e-1} -1\}$$

By Lemma 6 we conclude $\epsilon(j) = \xi^{kj}$ for some k. Since $\epsilon(j) = \pm 1$ we see $k = 0$, or $k = e/2$ and e even. Now one can conclude the cyclotomic schemeof class e on $GF(p^s)$ is amorphic. Repeating this procedure, one eventually reaches amorphic association scheme of Latin square type, which was treated earlier. □

3 Notes

3.1 Davenport-Hasse theorem for association schemes

Davenport-Hasse theorem provides a powerful tool to compute the character table i.e., Gaussian periods of cyclotomic scheme, as shown in section 1. The fact that a power of the principal part of the character table as a matrix is the principal part of the character table of another association scheme is quite remarkable, and we are interested in the situations where this phenomenon occurs.

Here is an example. Consider cyclotomic schemeof class 3 on $GF(4)$ and $GF(16)$. The principal part of their character tables are

$$P_0 = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

$$\tilde{P_0} = \begin{pmatrix} -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

Notice that the relation $-P_0^2 = \tilde{P_0}$ holds. Now consider the principal part of the character table of $\mathbf{Z}_4$, the cyclic group of order 4:

$$Q_0 = \begin{pmatrix} i & -1 & -i \\ -1 & 1 & -1 \\ -i & -1 & i \end{pmatrix}$$

Then

$$-Q_0^2 = \begin{pmatrix} 1 & 1 & -3 \\ 1 & -3 & 1 \\ -3 & 1 & 1 \end{pmatrix}$$

which is the same as $\tilde{P_0}$ up to some permutation of rows. This motivated us to search for an association scheme on $\mathbf{Z}_4 \times \mathbf{Z}_4$ having the same parameters as cyclotomic scheme of class 3 on $GF(16)$. Indeed, the following partition of $\mathbf{Z}_4 \times \mathbf{Z}_4$ defines an S-ring (hence an association scheme) with the desired property.

$$\begin{aligned} S_0 &= \{(0,0)\} \\ S_1 &= \{(2,2),(0,1),(0,3),(1,0),(3,0)\} \\ S_2 &= \{(1,1),(3,3),(0,2),(3,2),(1,2)\} \\ S_3 &= \{(2,0),(2,1),(2,3),(1,3),(3,1)\} \end{aligned}$$

This association scheme was already included in the list of A. V. Ivanov [9], however, no interpretation was previously known. This association scheme has only the trivial automorphisms, namely, the translations by the elements of $\mathbf{Z}_4 \times \mathbf{Z}_4$ and the inversion, therefore the scheme is not Schurian. We now give the relationship between this association scheme and the Shrikhande-Bose difference set.

Let $\mathcal{D} = \{D - \{(0,0)\} | \mathbf{Z}_4 \times \mathbf{Z}_4 \supset D : (v,k,\lambda)\text{-difference set}, (0,0) \in D = -D\}$. Then $GL(2,\mathbf{Z}_4)$ acts transitively on $\mathcal{D}$. For example $S_1 = \{(2,2),(0,1),(0,3),(1,0),(3,0)\} \in \mathcal{D}$. Let

$$D_0 = \{(1,0),(2,0),(3,0),(0,1),(0,2),(0,3)\}$$

D_0 is called the Shrikhande-Bose difference set. $\{(0,0)\} \cup S_0$ is equivalent to D_0, i.e., there exists $g \in G = (\mathbf{Z}_4 \times \mathbf{Z}_4) \cdot GL(2,\mathbf{Z}_4)$ such that $D_0^g = \{(0,0)\} \cup S_0$. This implies the following characterization of the Shrikhande-Bose difference set.

Proposition 8 *If $D \subset \mathbf{Z}_4 \times \mathbf{Z}_4$ is a difference set satisfying $(0,0) \in D, D = -D$, then D is equivalent to the Shrikhande-Bose difference set.*

Let

$$\Sigma = \{(S_1, S_2, S_3) \in \mathcal{D} \times \mathcal{D} \times \mathcal{D} | S_1, S_2, S_3 \text{ are disjoint}\}$$

Then $GL(2, \mathbf{Z}_4)$ acts transitively on Σ. Moreover, $\langle \underline{(0,0)}, \underline{S_1}, \underline{S_2}, \underline{S_3} \rangle$ is an S-ring on $\mathbf{Z}_4 \times \mathbf{Z}_4$ for any $(S_1, S_2, S_3) \in \Sigma$. Conversely, suppose $\langle \underline{(0,0)}, \underline{S_1}, \underline{S_2}, \underline{S_3} \rangle$ is an S-ring on $\mathbf{Z}_4 \times \mathbf{Z}_4$ which defines an amorphic pseudocyclic association scheme, then $(0,0) \cup S_i$ is a difference set for $i = 1, 2, 3$. Therefore $S_i \in \mathcal{D}$, and so $(S_1, S_2, S_3) \in \Sigma$.

Finally let us mention another design associated to our S-ring. In view of Proposition 3, one obtains (16,5,4)-difference families on $GF(16)$ and on $\mathbf{Z}_4 \times \mathbf{Z}_4$. These two designs have the same inner distribution, but not isomorphic.

3.2 Fusion schemes of non-amorphic cyclic association scheme

There are many non-amorphic cyclotomic schemes which have nontrivial fusion schemes. Cyclotomic schemes are pseudocyclic association schemes, with the additional property: the principal part of the character table is a circulant matrix. We call pseudocyclic association scheme with this property cyclic. If e is not prime, then there exist a fusion scheme of cyclic association schemes corresponding to subgroups of the cyclic group of order e. (see [8]). We call such fusion scheme trivial.

Theorem 9 *If $e \leq 5$, then the only cyclic association schemes with a nontrivial fusion scheme are amorphic association schemes.*

Fusion schemes of class 2 of cyclotomic schemes have been extensively studied, since such a fusion scheme gives rise to a two weight code [5]. If $e \geq 6$ then there exist non-amorphic cyclic association schemes which have nontrivial fusion scheme. We give a few examples below.

Example. Let $K = GF(49)$, α a generator of K^*,

$$T : K \to K; \ x \mapsto x^q$$

$$S : K \to K; \ x \mapsto x\alpha$$

Let $H = \langle S^{12}, S^3T \rangle$. Then one obtains a cyclic association scheme of class 6 on K via the action on the group $K \cdot H$. This association scheme has nontrivial fusion schemes, however, it is not amorphic.

Example. The cyclotomic scheme of class 7 on $GF(64)$ has nontrivial fusion schemes of class 2, however, it is not amorphic. The fusion schemes give rise to (64,28,12)-difference sets.

References

[1] E. Bannai, Subschemes of some association schemes, to appear in J. algebra.

[2] E. Bannai and T. Ito, Algebraic Combinatorics I : Association schemes, Benjamin/Cummings 1984.

[3] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy, J. Number Theory 14 (1982), 67 - 82.

[4] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Springer, Berlin-Heidelberg 1989.

[5] A. R. Calderbank and W. M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (1986) 97-122.

[6] H. Davenport and H. Hasse, Die Nullstellen der Kongruenzzetafunctionen in gewissen zyklischen Fällen, J. Reine. Angew. Math. 172 (1935), 151-182.

[7] Ja. Ju. Golfand and M. H. Klin, Amorphic cellular rings I, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system sciences 1985, 32 - 38 (in Russian).

[8] T. Ikuta, T. Ito and A. Munemasa, On certain pseudocyclic association schemes, submitted.

[9] A. V. Ivanov, Amorphic cellular rings II, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system sciences, 1985, 104 - 111 (in Russian).

[10] M. E. Muzichuk, Ph.D.thesis, unpublished.

[11] L. Stickelberger, Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann. 37 (1890), 321-367