数理解析研究所講究録
第 768 巻 1991 年 23-28

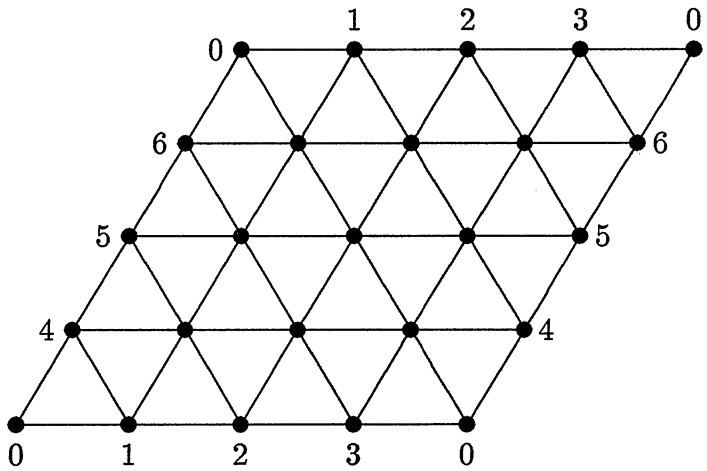
Fusion in Association Schemes

宗政昭弘
Akihiro Munemasa
Department of Mathematics
Osaka Kyoiku University

December 17, 1990

Let us begin with a well-known example of cospectral graphs (Two graphs are said to be cospectral if their adjacency matrices have the same spectrum).

The graph Γ_1 depicted below is called the Shrikhande graph. The vertices with the same label are identified. Γ_1 is a regular graph of valency 6 with 16 vertices. Its spectrum is $6^1 2^6 (-2)^9$.



The graph Γ_2 has $\{0,1,2,3\}^2$ as the set of vertices, and two distinct vertices (a_1, a_2), (b_1, b_2) are adjacent if $a_1 = b_1$ or $a_2 = b_2$. Γ_2 is called the Hamming graph $H(2,4)$ or the Latin square graph $L_2(4)$. Γ_2 has the same spectrum as that of Γ_1, and Shrikhande [9] showed that Γ_1 and Γ_2 are the only graphs with the spectrum $6^1 2^6 (-2)^9$. Γ_1 and Γ_2 are not isomorphic. Indeed, Γ_2 contains K_4 as a subgraph, while Γ_1 does not.

Definition. A strongly regular graph Γ with parameters (k, λ, μ) is an undirected graph such that

$$\#\{z \in \Gamma | x \sim z, z \sim y\} = \begin{cases} k & \text{if } x = y \\ \lambda & \text{if } x \sim y \\ \mu & \text{otherwise} \end{cases}$$

The number of vertices is given by $1+k+k(k-\lambda-1)/\mu$. The complement of a strongly regular graph is a strongly regular graph.

Both Γ_1 and Γ_2 are strongly regular graphs with parameters (6,2,2). Let us investigate Γ_1 and Γ_2 in more detail. The automorphism group of Γ_1 is a vertex-transitive, rank 4 permutation group, while the automorphism group of Γ_2 is a vertex-transitive, rank 3 permutation group. If we regard $\mathrm{Aut}\Gamma_i$ as acting on the direct product $V\Gamma_i \times V\Gamma_i$ of the set of vertices $V\Gamma_i$ $(i = 1, 2)$, then two nontrivial orbitals of $\mathrm{Aut}\Gamma_2$ are precisely edges and non-edges. On the other hand, $\mathrm{Aut}\Gamma_1$ acts transitively on edges, but the set of non-edges is decomposed into two orbitals of $\mathrm{Aut}\Gamma_1$. Therefore two graphs are group theoretically quite different, however they share the same algebraic properties (parameters, spectrum).

Definition. An association scheme of class d is a pair $(X, \{R_i\}_{0 \le i \le d})$ such that

$$X \times X = R_0 \cup \cdots \cup R_d,$$

$$R_0 = \{(x,x) | x \in X\},$$

$$(x,y) \in R_i \Longleftrightarrow (y,x) \in R_i,$$

$$p_{ij}^k = \#\{z \in X | (x,z) \in R_i, (z,y) \in R_j\} \quad \text{for any } (x,y) \in R_k.$$

Indeed this is the definition of symmetric association scheme, however in this talk, all association schemes are assumed to be symmetric. For more general and detailed theory of association schemes, see [1].

Note that strongly regular graphs are equivalent to association schemes of class 2, via the correspondence

$$R_1 = \{\text{edges}\}$$

$$R_2 = \{\text{non-edges}\}$$

The three parameters of the strongly regular graph are $k = p_{11}^0$, $\lambda = p_{11}^1$, $\mu = p_{11}^2$.

An association scheme of class d can be constructed from a generously transitive permutation group of rank $d+1$. A permutation group G on X is said to be generously transitive if

$$\forall x, \forall y \in X \; \exists \sigma \in G \;\text{ such that }\; x^\sigma = y, y^\sigma = x.$$

The set of relations $R_0, R_1, \ldots, R_d$ are defined to be the G-orbits on $X \times X$.

Since $\mathrm{Aut}\Gamma_1$ is a generously transitive permutation group of rank 4, the orbits R_0, R_1, R_2, R_3 defines an association scheme $\mathfrak{X}_1 = (V\Gamma_1, \{R_0, R_1, R_2, R_3\})$ of class 3. We may renumber the relation if necessary and assume R_1 is the set of edges of Γ_1.

Since Γ_1 is a strongly regular graph, $\mathfrak{X}_1' = (V\Gamma_1, \{R_0, R_1, R_2 \cup R_3\})$ is an association scheme of class 2. We say that $\mathfrak{X}_1'$ is obtained from $\mathfrak{X}_1$ by merging of classes, or by fusion. It is now appropriate to give a formal definition.

Definition. Let $\mathfrak{X} = (X, \{R_i\}_{0\leq i\leq d})$ be an association scheme and 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 $\mathfrak{X}$. $\mathfrak{X}$ is called *amorphous* if $(X, \{R_{\Lambda j}\}_{0\leq j\leq d'})$ is a fusion scheme of $\mathfrak{X}$ for any partition $\{\Lambda_j\}_{0\leq j\leq d'}$ with $\Lambda_0 = \{0\}$.

Any association scheme of class 2 is amorphous. The association scheme $\mathfrak{X}_1$ above is indeed amorphous so that $(V\Gamma_1, \{R_0, R_2, R_1 \cup R_3\})$, $(V\Gamma_1, \{R_0, R_3, R_1 \cup R_2\})$ are fusion schemes of $\mathfrak{X}_1$.

An obvious construction of fusion schemes comes from a permutation group and its generously transitive subgroup. Let $\tilde{G} \supset G$ be permutation groups acting on a set X, and assume G is generously transitive (hence $\tilde{G}$ is also generously transitive), rank$\tilde{G} <$ rank$G$. The G-orbits on $X \times X$ are refinement of $\tilde{G}$-orbits on $X \times X$, so one obtains an association scheme and its fusion scheme. From this group theoretic point of view, it is hard to imagine the existence of amorphous association scheme of large number of classes. However, there do exist amorphous association schemes of arbitrary large number of classes.

Example. Affine plane scheme (Gol'fand and Klin [4]). Let $S_1, \ldots, S_{n-1}$ be mutually orthogonal Latin squares of order n. Define an association scheme with vertices $X = \{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$,

$$R_1 = \{((j,k),(j,k'))|(j,k),(j,k') \in X, k \neq k'\},$$

$$R_2 = \{((j,k),(j',k))|(j,k),(j',k) \in X, j \neq j'\},$$

$$R_i = \{((j,k),(j',k'))|S_{i-2}(j,k) = S_{i-2}(j',k'),\ (j,k) \neq (j',k')\},\ \ 3 \leq i \leq n+1.$$

Then $(X, \{R_i\}_{0\leq i\leq n+1})$ is an amorphous association scheme.

Example. (Baumert–Mills–Ward [3]) Let p be a prime. The cyclotomic scheme of class e on $GF(p^{2s})$ is amorphous if and only if there exists a divisor r of s such that e divides $p^r + 1$. The concept of amorphous association scheme was introduced after the work [3] had been published. Apparently, many combinatorists were unaware of the work of Baumert–Mills–Ward, who classified amorphous cyclotomic schemes in combinatorist's terminology. The cyclotomic scheme of class e is closely related to the Gauss sum with a multiplicative character of order e as the argument. Such Gauss sums are easily computable precisely when the corresponding cyclotomic scheme is amorphous. See Bannai–Munemasa [2] for details.

Furthermore, amorphous association schemes of class 4 can be derived from Hadamard matrices (Ivanov-Chuvaeva [6]).

Note that a number of strongly regular graphs are obtained from an amorphous association scheme of large number of classes. In particular, each nontrivial relation of an amorphous association scheme defines a strongly regular graph of Latin square type or negative Latin square type.

Definition. A strongly regular graph with parameters (k, λ, μ) is said to be of Latin square type if there exist integers $g, n > 0$ such that $k = g(n-1)$, $\lambda = (g-1)(g-2) + n - 2$, $\mu = g(g-1)$. A strongly regular graph with parameters (k, λ, μ) is said to be of negative Latin square type if there exist integers $g, n > 0$ such that $k = g(n+1)$, $\lambda = (g+1)(g+2) - n - 2$, $\mu = g(g+1)$.

Theorem 1 ([7] [5]) *Let* $\mathfrak{X} = (X, \{R_i\}_{0 \le i \le d})$ *be an association scheme of classs* d *with* $d \ge 3$. *Then* $\mathfrak{X}$ *is amorphous if and only if either*

(i) (X, R_i) *is a strongly regular graph of Latin square type for each* i, $1 \le i \le d$

or

(ii) (X, R_i) *is a strongly regular graph of negative Latin square type for each* i, $1 \le i \le d$.

The aim of this talk is to present our recent result [5] which gives a construction of a new family of amorphous association schemes.

Definition. Let $f(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ be a primitive polynomial of degree s, that is, $GF(p^s) = \mathbf{Z}/p\mathbf{Z}[x]/(f(x))$ and the image of x is a primitive element of $GF(p^s)$. There exists $g(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ such that $f(x)g(x) = x^{p^s-1} - 1$. By Hensel's Lemma there exist $F(x), G(x) \in \mathbf{Z}/p^m\mathbf{Z}[x]$ such that

$$F(x) \equiv f(x) \bmod p$$

$$G(x) \equiv g(x) \bmod p$$

$$F(x)G(x) = x^{p^s-1} - 1$$

The ring $R = GR(p^m, s) = \mathbf{Z}/p^m\mathbf{Z}[x]/(F(x))$ is called a Galois ring (see [8]). R is a local ring with the maximal ideal pR, and $R/pR \cong GF(p^s)$.

In what follows, we assume $p^m = 2^2 = 4$. Let ξ be the image of x in R, $\bar{\xi}$ the image of ξ in K. We have

$$R^* = \langle \xi \rangle \times \varepsilon,$$

$$|\langle \xi \rangle| = 2^s - 1, \ |\varepsilon| = 2^s$$

$$\varepsilon = 1 + 2R = \{1 + 2\xi^i | i = 0, 1, \ldots, 2^s - 2\} \cup \{1\}$$

and $T = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^s-2}\}$ is a set of representatives of $R/2R$. It should be mentioned that $T - \{0\}$ is a multiplicative subgroup of R^*, but T is not in general an additive subgroup of R. Since $R = \{t + 2r | t \in T, r \in R\}$, and $2R = 2\{t + 2r | t \in T, r \in R\}$

$= \{2t | t \in T\}$, we see $R = \{t_1 + 2t_2 \ | t_1, t_2 \in T\}$, and this representation of elements of R is unique.

$$R^* = R - 2R = \{t_2 + 2t_2 | t_1 \neq 0\} = \langle \xi \rangle \times \{1 + 2t_2 | t_2 \in T\}$$

Define a mapping $\iota : K \longrightarrow R$ by $0 \mapsto 0$, $\bar{\xi}^i \mapsto \xi^i$, $(0 \leq i \leq 2^s - 2)$. Define $\phi : K \longrightarrow \varepsilon$ by $\phi(\alpha) = 1 + 2\iota(\alpha)$. Since

$$\iota(\alpha + \beta) \equiv \iota(\alpha) + \iota(\beta) \bmod 2$$

we have

$$2\iota(\alpha + \beta) = 2\iota(\alpha) + 2\iota(\beta)$$

Therefore ϕ is a group isomorphism. Let H be a subgroup of K, $K = \cup_{i=1}^{r} H + \alpha_i$, $|K : H| = r$. Then

$$\begin{aligned} \varepsilon &= \cup_{i=1}^{r} \phi(H + \alpha_i) \\ &= \cup_{i=1}^{r} \phi(H)\phi(\alpha_i) \end{aligned}$$

Let $\mathfrak{X}(H) = (R, \{S_i\}_{0 \leq i \leq r+1})$ be an association scheme defined by

$$(x, y) \in S_0 \Leftrightarrow x - y = 0$$

$$(x, y) \in S_i \Leftrightarrow x - y \in \langle \xi \rangle \phi(H + \alpha_i), \quad 1 \leq i \leq r$$

$$(x, y) \in S_{r+1} \Leftrightarrow x - y \in 2R - \{0\}$$

Theorem 2 *$\mathfrak{X}(H)$ is amorphous if and only if $H^\perp$ is totally isotropic with respect to the symmetric bilinear form*

$$(\alpha, \beta) = \mathbf{Tr}_{K/GF(2)}(\alpha\beta)$$

If we set $H^\perp$ to be a maximal totally isotropic subspace, then $\mathfrak{X}(H)$ is of class $2^{[s/2]} + 1$.

If we set $s = 2$ in the above theorem, $\mathfrak{X}(H)$ is the association scheme $\mathfrak{X}_1$ which is obtained from the action of AutΓ_1 described earlier.

The proof of Theorem 2 is best given in terms of Gauss sums and Jacobi sums over $GR(4, s)$. Another tool in the proof is Bannai–Muzichuk criterion for the existence of a fusion scheme. See [5] for details.

A possible direction for further reseach is to generalize Theorem 2 for an arbitrary characteristic p^m. We found a few examples of amorphous association schemes over $GR(p^2, s)$ with p odd, but so far we were unable to obtain a nice criterion as in Theorem 2.

References

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

[2] E. Bannai and A. Munemasa, Davenport-Hasse theorem and cyclotomic association schemes, Report of Conference on Algebraic Combinatorics, Hirosaki University, 1990.

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

[4] Ja. Ju. Gol'fand and M. H. Klin, Amorphic cellular rings I, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system studies 1985, 32–38 (in Russian).

[5] T. Ito, A. Munemasa and M. Yamada, Amorphous association schemes over the Galois rings of characteristic 4, submitted.

[6] A. A. Ivanov and I. V. Chuvaeva, Action of the group M_{12} on Hadamard matrices, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system studies, 1985, 159–169 (in Russian).

[7] A. V. Ivanov, Amorphic cellular rings II, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system studies, 1985, 39–49 (in Russian).

[8] B. R. McDonald, Finite Rings with Identity, Dekker, New York, 1974.

[9] S. S. Shrikhande, The uniqueness of the L_2 association scheme, Ann. Math. Statistics 30 (1959), 781–798.