Non-amorphous association schemes in which all nontrivial relations are strongly regular*

Akihiro Munemasa

The 22nd PNU–POSTECH Algebraic Combinatorics Seminar
November 24, 2007
(joint work with Takuya Ikuta)

Definition 1. A *strongly regular graph* is a regular graph of valency k for which there exist constants $\lambda \geq 0$ and $\mu > 0$ such that every pair of adjacent (resp. non-adjacent) vertices has λ (resp. μ) common neighbours.

A connected regular graph has its valency as the Perron–Frobenius eigenvalue. We call all the other eigenvalues *nontrivial* eigenvalues of the graph. Strongly regular graphs are regular graphs with exactly two nontrivial eigenvalues.

Example 2. The 4-cycle is a strongly regular graph with $(k, \lambda, \mu) = (4, 0, 2)$.

Example 3. Let α be a primitive element of the finite field GF(16) of 16 elements. Let Γ be the graph with vertex set GF(16), where two vertices x, y are adjacent whenever $x - y \in \langle \alpha^3 \rangle$. Then Γ is a strongly regular graph with $(k, \lambda, \mu) = (5, 0, 2)$.

The construction method of the above example is known as "Cayley graphs." Let G be a finite group, S a subset of G closed under inversion and $1 \notin S$. Then the graph $\mathrm{Cay}(G, S)$ is the graph with vertex set G, where two vertices x, y are adjacent whenever $x^{-1}y \in S$.

*corrected December 5, 2007

Example 4 (Brouwer–Wilson–Xiang, 1999)**.** Let $q = p^s$ be a prime power, where p is a prime. Let e be a divisor of $q-1$ such that $e \mid p^r + 1$ for some $r < s$ and $f \nmid p^r - 1$ for any $r < s$, where $f = (q-1)/e$. Then $\mathrm{Cay}(\mathrm{GF}(q), \langle \alpha^e \rangle)$ is a strongly regular graph.

The above example is essentially due to Baumert–Mills–Ward [1]. In order to explain its number theoretical background, let $e \mid q-1$ be arbitrary. Then

$$\mathrm{Cay}(\mathrm{GF}(q), \langle \alpha^e \rangle \alpha) \cong \mathrm{Cay}(\mathrm{GF}(q), \langle \alpha^e \rangle \alpha^2) \cong \cdots \cong \mathrm{Cay}(\mathrm{GF}(q), \langle \alpha^e \rangle) \qquad (1)$$

and let $A_1, A_2, \dots, A_e$ be the adjacency matrices of these graphs. Then they are simultaneously diagonalizable, and $A_1 + A_2 + \cdots + A_e = J - I$. Note that $f = (q-1)/e$ is the Perron–Frobenius eigenvalue of A_i for each i, and we may assume that f appears in the $(1,1)$-entry of the diagonalized form of A_i for every i. Then we construct a $(q-1) \times e$ matrix whose column vectors are the diagonal entries other than the $(1,1)$-entry of the diagonalized form of A_i $(i = 1, \dots, e)$. Removing the repeated columns, we obtain an $e \times e$ matrix P_0. The entries of P_0 are called the Gaussian periods, and the matrix P_0 is also known as the principal part of the eigenmatrix of the cyclotomic association scheme of class e on $\mathrm{GF}(q)$. The eigenvalues of P_0 are the well-known Gauss sums. Then the result of Baumert–Mills–Ward can be stated in terms of P_0 as follows.

Theorem 5. *Let e be a divisor of $q-1$, where $q = p^s$ and p is a prime. Then*

$$P_0 = \begin{bmatrix} a & & b \\ & \ddots & \\ b & & a \end{bmatrix}$$

if and only if $e \mid p^r + 1$ for some $r < s$.

In particular, there are exactly two nontrivial eigenvalues for each of the Cayley graphs (1), so these graphs are strongly regular provided they are connected. The convenience of the use of the matrix P_0 is that one can immediately derive the eigenvalues of the edge-union of these graphs. For example, the edge-union of two of the graphs in (1) has nontrivial eigenvalues $a + b$ and $2b$, so this graph is again strongly regular. The same is true for the edge-union of an arbitrary number of these graphs. Thus, Theorem 5 can be restated as follows.

Theorem 6. *Let e be a divisor of $q-1$, where $q = p^s$ and p is a prime. Let α be a primitive element of* $\mathrm{GF}(q)$. *Then* $\mathrm{Cay}(\mathrm{GF}(q), \bigcup_{i\in\Lambda}\langle\alpha^e\rangle\alpha^i)$ *is strongly regular for all $\emptyset \neq \Lambda \subsetneq \{1,\ldots,e\}$ if and only if $e \mid p^r+1$ for some $r < s$ and $f \nmid p^r - 1$ for any $r < s$, where $f = (q-1)/e$.*

Strongly regular graphs can be constructed in many ways, not only as Cayley graphs over finite fields. We now define the concept of an association scheme, which generalizes the edge-subgraph decomposition defined by the decomposition of the multiplicative group of a finite field into cosets.

Definition 7. An association scheme is a collection of regular graphs on the same set of vertices, represented by their adjacency matrices $A_1, \ldots, A_e$, such that

(i) $A_1 + \cdots + A_e = J - I$,

(ii) $A_1, \ldots, A_e$ are pairwise commutative,

(iii) $\langle I, A_1, \ldots, A_e\rangle$ is closed under multiplication.

Let k_i be the valency of the graph represented by A_i. Then the matrices $A_1, \ldots, A_e$ can be simultaneously diagonalized in such a way that the diagonalized form of A_i has k_i in the $(1,1)$-entry. Then we construct a matrix whose column vectors are the diagonal entries except the $(1,1)$-entry of the diagonalized form of A_i ($i = 1, \ldots, e$). Removing the repeated columns, we obtain an $e \times e$ matrix P_0. The matrix P_0 is called the principal part of the eigenmatrix of the association scheme.

If, for an association scheme, the matrix P_0 is of the following form:

$$P_0 = \begin{bmatrix} g_1 + h & g_2 & \cdots & g_e \\ g_1 & g_2 + h & \cdots & \vdots \\ \vdots & g_2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & g_e \\ g_1 & g_2 & \cdots & g_e + h \end{bmatrix} \tag{2}$$

then for any $\Lambda \subset \{1, \ldots, e\}$, $\sum_{i\in\Lambda} A_i$ has two nontrivial eigenvalues, for example, $g_1 + \cdots + g_i + h$ and $g_1 + \cdots + g_i$ for $\Lambda = \{1, \ldots, i\}$.

Definition 8. An amorphous association scheme is an association scheme whose principal part of the eigenmatrix is given by (2) for some $g_1, \ldots, g_e, h$.

Baumert–Mills–Ward determined for which q, e with $e \mid q-1$, the adjacency matrices of the Cayley grpahs (1) give an amorphous association scheme.

Conjecture 9 (A. V. Ivanov, [4])**.** If, in an association scheme, the graph defined by its adjacency matrices are all strongly regular, then it is amorphous.

This conjecture turned out to be false, as van Dam [3] gave a counterexample. In order to put this example in a proper context, we consider an association scheme whose eigenmatrix has principal part given by the following.

$$\begin{bmatrix} s_1 & r_2 & r_2 & r_2 \\ r_1 & r_2 & s_2 & s_2 \\ r_1 & s_2 & r_2 & s_2 \\ r_1 & s_2 & s_2 & r_2 \end{bmatrix} \tag{3}$$

If such an association scheme exists, then each of its four adjacency matrices defines a strongly regular graph (provided it is connected), so it gives a counterexample to Ivanov's conjecture.

Theorem 10. *Let A_1, A_2, A_3, A_4 be the adjacency matrices of an association scheme whose eigenmatrix has principal part given by* (3)*. Assume that the valency of A_1 is the multiplicity of the eigenvalue r_1. Then the size is $(30r+4)^2$ and*

$$\begin{aligned} k_1 &= 12(6r+1)(10r+1) = 12k_2, \\ s_1 &= -4(6r+1), \\ r_1 &= 6r, \\ s_2 &= -7r-1, \\ r_2 &= 8r+1. \end{aligned}$$

If we want to construct an association scheme satisfying the conditions of Theorem 10 over a finite field $\mathrm{GF}(q)$, then $q = (30r+4)^2$, hence $q = 2^{8h+4}$ for some nonnegative integer h, and $r = \frac{2}{15}(2^{4h}-1)$. If $h = 0$, then we obtain

$$P_0 = \begin{bmatrix} -4 & 1 & 1 & 1 \\ 0 & 1 & -1 & -1 \\ 0 & -1 & 1 & -1 \\ 0 & -1 & -1 & 1 \end{bmatrix}$$

In this association scheme, the three graphs defined by A_2, A_3, A_4 are disconnected, so it does not give a counterexample. The case $h = 1$ corresponds to the first (and the only previously known) counterexample given by van Dam [3]. It is constructed as follows: Let α be a primitive element of $\mathrm{GF}(2^{12})$, and let H be the subgroup of the multiplicative group of $\mathrm{GF}(2^{12})$ of index 45. Let $S = H \cup H\alpha^5 \cup H\alpha^{10}$. Then the adjacency matrices

$$\begin{aligned}
A_2 &: \mathrm{Cay}(\mathrm{GF}(2^{12}), S), \\
A_3 &: \mathrm{Cay}(\mathrm{GF}(2^{12}), S\alpha^{15}), \\
A_4 &: \mathrm{Cay}(\mathrm{GF}(2^{12}), S\alpha^{30}), \\
A_1 &: \mathrm{Cay}(\mathrm{GF}(2^{12}), \text{“the rest”}).
\end{aligned}$$

We have found an example for $h = 2$, as follows.

Theorem 11 (Ikuta–M.)**.** *Let α be a primitive element of* $\mathrm{GF}(2^{20})$*, and let H be the subgroup of the multiplicative group of* $\mathrm{GF}(2^{20})$ *of index* 75*. Let $S = H \cup H\alpha^3 \cup H\alpha^6 \cup H\alpha^9 \cup H\alpha^{12}$. Then the adjacency matrices*

$$\begin{aligned}
A_2 &: \mathrm{Cay}(\mathrm{GF}(2^{20}), S), \\
A_3 &: \mathrm{Cay}(\mathrm{GF}(2^{20}), S\alpha^{25}), \\
A_4 &: \mathrm{Cay}(\mathrm{GF}(2^{20}), S\alpha^{50}), \\
A_1 &: \mathrm{Cay}(\mathrm{GF}(2^{20}), \text{“the rest”})
\end{aligned}$$

define an association scheme whose eigenmatrix has principal part (3) *with* $h = 2$*.*

References

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

[2] A.E. Brouwer, R.M. Wilson, and Q. Xiang, *Cyclotomy and strongly regular graphs*, J. Algbraic Combin. **10** (1999), 25–28.

[3] E. R. van Dam, *Strongly regular decompositions of the complete graph*, J. Algraic Combin. **17** (2003), 181–201.

[4] A.A. Ivanov and C.E. Praeger, *Problem session at ALCOM-91*, Europ. J. Combin. **15** (1994), 105–112.