Strongly Regular Graphs From Union of Cyclotomic Classes

Qing Xiang

University of Delaware
Newark, DE 19716, USA
xiang@math.udel.edu

Joint work with Tao Feng

Definitions and Examples

Strongly Regular Graphs

A *strongly regular graph srg* (v, k, λ, μ) is a graph with v vertices that is regular of valency k and that has the following properties:

- For any two adjacent vertices x, y, there are exactly λ vertices adjacent to both x and y.
- For any two nonadjacent vertices x, y, there are exactly μ vertices adjacent to both x and y.

Classical examples of strongly regular graphs include the Paley graphs. Let $q = 4t + 1$ be a prime power. The *Paley graph* Paley(q) is the graph with the finite field $\mathbb{F}_q$ as vertex set, where two vertices are adjacent when they differ by a (nonzero) square. It is strongly regular with parameters $(4t + 1, 2t, t - 1, t)$. From the point of view of association schemes, strongly regular graphs are equivalent to 2-class association schemes.

Theorem. For a simple graph Γ of order v, not complete or edgeless, with adjacency matrix A, the following are equivalent:

- Γ is strongly regular with parameters (v, k, λ, μ) for certain integers k, λ, μ,
- $A^2 = kI + \lambda A + \mu(J - I - A)$ for certain real numbers k, λ, μ,
- A has precisely two distinct restricted eigenvalues.

Let $q = p^f$ be a prime power, and let γ be a fixed primitive element of $\mathbb{F}_q$. Let $N > 1$ be a divisor of $q - 1$. We define the Nth *cyclotomic classes* $C_0, C_1, \ldots, C_{N-1}$ by

$$C_i = \{\gamma^{jN+i} \mid 0 \leq j \leq \frac{q-1}{N} - 1\},$$

where $0 \leq i \leq N - 1$.

Problem. Assume that $-C_0 = C_0$. Determine for which p, f, N the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, C_0)$ is strongly regular.

Conjecture (Schmidt and White, 2002.) Let $\mathbb{F}_{p^f}$ be the finite field of size p^f, $N|(p^f-1)$, and let C_0 be the subgroup of $\mathbb{F}_{p^f}$ of index N. Assume that $-C_0 = C_0$. If $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ is an SRG, then one of the following holds:

- (subfield case) $C_0 = \mathbb{F}_{p^e}^*$, where $e|f$,
- (semi-primitive case) There exists a positive integer j such that $p^j \equiv -1 \pmod{N}$,
- (exceptional case) Eleven specific examples.

Examples of De Lange, Ikuta and Munemasa

Example 1 (De Lange, 1995) Let $p = 2$, $f = 12$, $N = 45$. Then

$$C_0 \cup C_5 \cup C_{10}$$

gives rise to an SRG, while C_0 does not.

Example 2 (Ikuta and Munemasa, 2008) Let $p = 2$, $f = 20$, $N = 75$. Then

$$C_0 \cup C_3 \cup C_6 \cup C_9 \cup C_{12}$$

gives rise to an SRG, while C_0 does not.

Example 3 (Ikuta and Munemasa, 2008) Let $p = 2$, $f = 21$, $N = 49$. Then

$$C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$$

gives rise to an SRG, while C_0 does not.

New infinite families of SRG

We will generalize each of the above three examples into an infinite family. Moreover we obtain five more infinite families of new SRG by using union of cyclotomic classes.

- $p = 2$, $N = 3^m \cdot 5$, $f = \phi(N)/2 = 3^{m-1} \cdot 4$.
- $p = 2$, $N = 5^m \cdot 3$, $f = \phi(N)/2 = 5^{m-1} \cdot 4$.
- $p = 2$, $N = 7^m$, $f = \phi(N)/2 = 7^{m-1} \cdot 3$.

New infinite families of SRG, continued

- $p = 3$, $p_1 = 107$, $N = p_1^m$, $f = \phi(N)/2 = 53 \cdot 107^{m-1}$.
- $p = 5$, $p_1 = 19$, $N = p_1^m$, $f = \phi(N)/2 = 9 \cdot 19^{m-1}$.
- $p = 5$, $p_1 = 499$, $N = p_1^m$, $f = \phi(N)/2 = 249 \cdot 499^{m-1}$.
- $p = 17$, $p_1 = 67$, $N = p_1^m$, $f = \phi(N)/2 = 33 \cdot 67^{m-1}$.
- $p = 41$, $p_1 = 163$, $N = p_1^m$, $f = \phi(N)/2 = 81 \cdot 163^{m-1}$.

Gauss sums

Let p be a prime, f a positive integer, and $q = p^f$. Let ξ_p be a fixed complex primitive pth root of unity and let $\mathrm{Trace}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{Z}/p\mathbb{Z}$. Define

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi(x) = \xi_p^{\mathrm{Trace}_{q/p}(x)},$$

which is easily seen to be a nontrivial character of the additive group of $\mathbb{F}_q$. Let

$$\chi : \mathbb{F}_q^* \to \mathbb{C}^*$$

be a character of $\mathbb{F}_q^*$. We define the *Gauss sum* by

$$g(\chi) = \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi(a).$$

Gauss sums, semi-primitive case

Theorem (Stickelberger)
Let p be a prime, and $m > 2$ be an integer. Suppose that there is a positive integer t such that $p^t \equiv -1 \pmod{m}$, with t chosen minimal. Let χ be a character of order m of $\mathbb{F}_{p^f}^*$ for some positive integer f. Then $f = 2ts$ for some positive integer s, and

$$p^{-f/2} g(\chi) = \begin{cases} (-1)^{s-1}, & \text{if } p = 2, \\ (-1)^{s-1+\frac{(p^t+1)s}{m}}, & \text{if } p > 2. \end{cases}$$

Gauss sums, index 2 case

Theorem (Langevin, 1997)
Let $N = p_1^m$, where p_1 is a prime such that $p_1 > 3$ and $p_1 \equiv 3 \pmod 4$. Let p be a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2$ (that is, $f := \mathrm{ord}_N(p) = \phi(N)/2$) and let $q = p^f$. Let χ be a multiplicative character of order N of $\mathbb{F}_q$, and h be the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then the Gauss sum $g(\chi)$ over $\mathbb{F}_q$ is determined up to complex conjugation by

$$g(\chi) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0},$$

where

1. $h_0 = \frac{f-h}{2}$,
2. $b, c \not\equiv 0 \pmod p$,
3. $b^2 + p_1 c^2 = 4p^h$,
4. $bp^{h_0} \equiv -2 \pmod{p_1}$.

There are more theorems in the index 2 case. We will not list all of them here.

Apparently, we have more problems.

1. Are there more examples in higher index case?
2. It seems extremally difficult to completely understand when $\mathrm{Cay}(\mathbb{F}_q, C_{i_1} \cup C_{i_2} \cup \cdots \cup C_{i_\ell})$ is an SRG.