Journal of Algebraic Combinatorics **10** (1999), 25–28

Cyclotomy and Strongly Regular Graphs

A.E. BROUWER aeb@cwi.nl
Department of Math. & Computer Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

R.M. WILSON rmw@cco.caltech.edu
Department of Mathematics, California Institute of Technology, Pasadena, California 91125

QING XIANG* xiang@math.udel.edu
Department of Mathematical Sciences, University of Delaware, Newark, DE 19716

Received July 10, 1997

Abstract. We consider strongly regular graphs defined on a finite field by taking the union of some cyclotomic classes as difference set. Several new examples are found.

Keywords: cyclotomy, Gauss sum, strongly regular graph

In this note we consider graphs Γ that have, as vertices, the elements of a finite field $\mathbb{F}_q$, where two vertices are adjacent when their difference belongs to D, a fixed subset of $\mathbb{F}_q$. Note that such a graph will be undirected when $D = -D$, and without loops if $0 \notin D$.

The case where D is a union of cosets of a subgroup of the multiplicative group of a field $\mathbb{F}_q$ was considered in [3]; see also [1]. De Lange [2] gave a few more examples of strongly regular graphs obtained by cyclotomy. Here, we give an 'explanation' of one of his examples, by showing how it fits into the general theory. (There are still two more examples to be explained.) As a result, we obtain infinitely many other examples. The idea is to use a union of cosets of several subgroups of the multiplicative group of $\mathbb{F}_q$.

We start by reviewing the classical stuff. Let $q = p^\kappa$, p prime and $e \mid (q-1)$, say $q = em + 1$. Let $K \subseteq \mathbb{F}_q^*$ be the subgroup of the eth powers (so that $|K| = m$). Let α be a primitive element of $\mathbb{F}_q$. For $J \subseteq \{0, 1, \ldots, e-1\}$ put $u := |J|$ and $D := D_J := \bigcup\{\alpha^j K \mid j \in J\} = \{\alpha^{ie+j} \mid j \in J, 0 \leq i < m\}$. Define a (directed) graph $\Gamma = \Gamma_J$ with vertex set $\mathbb{F}_q$ and edges (x, y) whenever $y - x \in D$. Note that Γ will be undirected iff either -1 is an eth power (i.e., q is even or $e \mid (q-1)/2$) or $J + (q-1)/2 = J$ (arithmetic in $\mathbb{Z}_e$).

Let $A = A_J$ be the adjacency matrix of Γ defined by $A(x, y) = 1$ if (x, y) is an edge of Γ and $= 0$ otherwise. Let us compute the eigenvalues of A. For each (additive) character

*Partially supported by NSA grant MDA 904-97-0104.

χ of $\mathbb{F}_q$ we have

$$(A\chi)(x) = \sum_{y\sim x} \chi(y) = \left(\sum_{d\in D} \chi(d)\right)\chi(x).$$

Thus, each character gives us an eigenvector, and since these are all independent we know all eigenvalues. Their explicit determination requires some theory of Gauss sums. Let us write $A\chi = \theta(\chi)\chi$. Clearly, $\theta(1) = mu$, the valency of Γ. Now assume $\chi \neq 1$. Then $\chi = \chi_g$ for some integer g, where

$$\chi_g(\alpha^j) = \exp\left(\frac{2\pi i}{p}\mathrm{tr}(\alpha^{j+g})\right)$$

and $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace function.

If μ is any multiplicative character of order e (say, $\mu(\alpha^j) = \zeta^j$, where $\zeta = \exp((2\pi i)/e)$) then

$$\sum_{i=0}^{e-1} \mu^i(x) = \begin{cases} e & \text{if } \mu(x) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$\begin{aligned} \theta(\chi_g) &= \sum_{d\in D} \chi_g(d) = \sum_{j\in J}\sum_{u\in K} \chi_{j+g}(u) = \frac{1}{e}\sum_{j\in J}\sum_{x\in\mathbb{F}_q^*} \chi_{j+g}(x)\sum_{i=0}^{e-1}\mu^i(x) \\ &= \frac{1}{e}\sum_{j\in J}\left(-1 + \sum_{i=1}^{e-1}\sum_{x\neq 0}\chi_{j+g}(x)\mu^i(x)\right) = \frac{1}{e}\sum_{j\in J}\left(-1+\sum_{i=1}^{e-1}\mu^{-i}(\alpha^{j+g})G_i\right) \end{aligned}$$

where G_i is the Gauss sum $\sum_{x\neq 0}\chi_0(x)\mu^i(x)$.

In general, determination of Gauss sums seems to be complicated, but there are a few explicit results. For our purposes the most interesting is the following:

Proposition 1 (Stickelberger et al. see [4, 5]) *Suppose $e > 2$ and p is semiprimitive* mod e, *i.e., there exists an l such that $p^l \equiv -1 \pmod{e}$. Choose l minimal and write $\kappa = 2lt$. Then*

$$G_i = (-1)^{t+1}\varepsilon^{it}\sqrt{q},$$

where

$$\varepsilon = \begin{cases} -1 & \textit{if } e \textit{ is even and } (p^l+1)/e \textit{ is odd} \\ +1 & \textit{otherwise}. \end{cases}$$

Under the hypotheses of this proposition, we have

$$\sum_{i=1}^{e-1} \mu^{-i}(\alpha^{j+g})G_i = \sum_{i=1}^{e-1} \zeta^{-i(j+g)}(-1)^{t+1}\varepsilon^{it}\sqrt{q} = \begin{cases} (-1)^t\sqrt{q} & \text{if } r \neq 1, \\ (-1)^{t+1}\sqrt{q}(e-1) & \text{if } r = 1, \end{cases}$$

where $\zeta = \exp((2\pi i)/e)$ and $r = r_{g,j} = \zeta^{-j-g}\varepsilon^t$ (so that $r^e = \varepsilon^{et} = 1$), and hence

$$\theta(\chi_g) = \frac{u}{e}(-1 + (-1)^t\sqrt{q}) + (-1)^{t+1}\sqrt{q} \cdot \#\{j \in J \mid r_{g,j} = 1\}.$$

If we abbreviate the cardinality in this formula with #, then: If $\varepsilon^t = 1$ then $\# = 1$ if $g \in -J \pmod{e}$, and $= 0$ otherwise. If $\varepsilon^t = -1$ (then e is even and p is odd) then $\# = 1$ if $g \in \frac{1}{2}e - J \pmod{e}$, and $= 0$ otherwise. We proved:

Theorem 2 *Let $q = p^\kappa$, p prime and $e \mid (q-1)$, where p is semiprimitive* mod e, *i.e., there is an $l > 0$ such that $p^l \equiv -1 \bmod e$. Choose l minimal with this property and write $\kappa = 2lt$. Choose u, $1 \le u \le e-1$ and assume that q is even or u is even or $e \mid (q-1)/2$. Then the graphs Γ_J (where J is arbitrary for q even or $e \mid (q-1)/2$ and satisfies $J + (q-1)/2 = J$* mod e *otherwise) are strongly regular with eigenvalues*

$$\begin{aligned} k &= \frac{q-1}{e}u && \textit{with multiplicity } 1, \\ \theta_1 &= \frac{u}{e}(-1 + (-1)^t\sqrt{q}) && \textit{with multiplicity } q-1-k, \\ \theta_2 &= \frac{u}{e}(-1 + (-1)^t\sqrt{q}) + (-1)^{t+1}\sqrt{q} && \textit{with multiplicity } k. \end{aligned}$$

(*Obviously, when t is even we have $r = \theta_1$, $s = \theta_2$, and otherwise $r = \theta_2$, $s = \theta_1$, where, as usual, r denotes the nontrivial positive eigenvalue, and s the negative one.*)

Clearly, when $e|e'|(q-1)$ then the set of eth powers is a union of cosets of the set of e'th powers, so when applying the above theorem we may assume that e has been chosen as large as possible, i.e., $e = p^l + 1$. Then the restriction 'q is even or u is even or $e \mid (q-1)/2$' is empty, and J can always be chosen arbitrarily.

The above construction can be generalized. Pick several values e_i $(i \in I)$ with $e_i|(q-1)$. Let K_i be the subgroup of $\mathbb{F}_q^*$ of the e_ith powers. Let J_i be a subset of $\{0, 1, \ldots, e_i - 1\}$. Let $D_i := D_{J_i} := \bigcup\{\alpha^j K_i \mid j \in J_i\}$. Put $D := \bigcup D_i$. If the D_i are mutually disjoint, then D defines a graph of which we can compute the spectrum. Using the above notation, we give the following examples.

Example 3 Let p be odd, and take $e_i = p^{l_i} + 1$ $(i = 1, 2)$ and $q = p^\kappa$ where $\kappa = 4l_is_i$ $(i = 1, 2)$. Pick J_1 to consist of even numbers only, and J_2 to consist of odd numbers only. Then $D_1 \cap D_2 = \emptyset$ and $g \in -J_i \pmod{e_i}$ cannot happen for $i = 1, 2$ simultaneously. This means that the resulting graph will be strongly regular with eigenvalues

$$k = (|J_1|/e_1 + |J_2|/e_2)(q-1)$$

and

$$\theta(\chi_g) = \left(\frac{|J_1|}{e_1} + \frac{|J_2|}{e_2}\right)(-1 + \sqrt{q}) - \sqrt{q} \cdot \delta(g \in -J_i (\mathrm{mod}\ e_i),\ \text{for } i = 1 \text{ or } i = 2)$$

(where $\delta(P) = 1$ if P holds, and $\delta(P) = 0$ otherwise).

This generalizes the first construction of Wilson and Xiang [6] (which is the special case $l_1 = 1$ and $J_1 = \{0\}$). In the special case $p = 3$, $l_1 = 1$, $l_2 = 2$, $e_1 = 4$, $e_2 = 10$, $J_1 = \{0\}$, $J_2 = \{1\}$, the difference set consists of the powers α^i with $i \equiv 0 \pmod 4$ or $i \equiv 1 \pmod{10}$, i.e., is the set $\{1, \alpha, \alpha^4, \alpha^8, \alpha^{11}, \alpha^{12}, \alpha^{16}\}\langle\alpha^{20}\rangle$, and we find the first graph from [2] again. (It has parameters $(v, k, \lambda, \mu) = (6561, 2296, 787, 812)$ and spectrum 2296^1 28^{4264} $(-53)^{2296}$.)

Example 4 Let p be odd, and take $e_i = p^{l_i} + 1$ $(i = 1, 2)$ and $q = p^\kappa$ where $\kappa = 2l_i s_i$ $(i = 1, 2)$, s_1 and s_2 are odd. Pick J_1 and J_2 such that J_1 consists of even numbers only, J_2 consists of odd numbers only, and $-J_1 + \frac{e_1}{2} \cap -J_2 + \frac{e_2}{2} = \emptyset$. Then $D_1 \cap D_2 = \emptyset$ and $g \in -J_i + \frac{e_i}{2} \pmod{e_i}$ cannot happen for $i = 1, 2$ simultaneously. This means that the resulting graph will be strongly regular with eigenvalues

$$k = (|J_1|/e_1 + |J_2|/e_2)(q - 1)$$

and

$$\theta(\chi_g) = \sqrt{q} \cdot \delta\left(g \in -J_i + \frac{e_i}{2} (\mathrm{mod}\ e_i),\ \text{for } i = 1 \text{ or } i = 2\right) - \left(\frac{|J_1|}{e_1} + \frac{|J_2|}{e_2}\right)(1 + \sqrt{q})$$

We remark that in Example 4 it is possible to choose p, l_i, $i = 1, 2$, and J_1, J_2 such that $-J_1 + \frac{e_1}{2} \cap -J_2 + \frac{e_2}{2} = \emptyset$. For example, let p be a prime congruent to 3 modulo 4, l_1, l_2 both odd. Then we have $-J_1 + \frac{e_1}{2} \cap -J_2 + \frac{e_2}{2} = \emptyset$. The resulting graphs have Latin square parameters.

References

1. R. Calderbank and W.M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.* **18** (1986), 97–122.
2. C.L.M. de Lange, "Some new cyclotomic strongly regular graphs," *J. Alg. Combin.* **4** (1995), 329–330.
3. J.H. van Lint and A. Schrijver, "Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields," *Combinatorica* **1** (1981), 63–73.
4. R.J. McEliece and H. Rumsey, Jr., "Euler products, cyclotomy and coding," *J. Number Th.* **4** (1972), 302–311.
5. R.J. McEliece, "Irreducible cyclic codes and Gauss sums," in *Combinatorics*, pp. 183–200 (*Proc. NATO Advanced Study Inst., Breukelen, 1974*; *M. Hall, Jr. and J. H. van Lint* (Eds.)), Part 1, Math. Centre Tracts, Vol. 55, Math. Centrum, Amsterdam, 1974. Republished by Reidel, Dordrecht, 1975 (pp. 185–202).
6. R.M. Wilson and Qing Xiang, "Cyclotomy, half ovoids and two-weight codes," Unpublished preprint, 1997.