J Algebr Comb (2013) 37:313–329
DOI 10.1007/s10801-012-0368-y

Constructions of strongly regular Cayley graphs using index four Gauss sums

Gennian Ge · Qing Xiang · Tao Yuan

Received: 3 August 2011 / Accepted: 22 March 2012 / Published online: 12 April 2012

Abstract We give a construction of strongly regular Cayley graphs on finite fields $\mathbb{F}_q$ by using union of cyclotomic classes and index 4 Gauss sums. In particular, we obtain two infinite families of strongly regular graphs with new parameters.

Keywords Cyclotomy · Gauss sum · Index 4 Gauss sum · Strongly regular graph

1 Introduction

A *strongly regular graph* $\mathrm{srg}(v, k, \lambda, \mu)$ is a simple and undirected graph, neither complete nor edgeless, that has the following properties:

(1) It is a regular graph of order v and valency k.
(2) For each pair of adjacent vertices x, y, there are λ vertices adjacent to both x and y.
(3) For each pair of nonadjacent vertices x, y, there are μ vertices adjacent to both x and y.

For example, a pentagon is an $\mathrm{srg}(5, 2, 0, 1)$, the 3×3 grid (the Cartesian product of two triangles) is an $\mathrm{srg}(9, 4, 1, 2)$, and the Petersen graph is an $\mathrm{srg}(10, 3, 0, 1)$.

G. Ge · T. Yuan
Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, P.R. China

G. Ge
e-mail: gnge@zju.edu.cn

T. Yuan
e-mail: matheufreedom@gmail.com

Q. Xiang (✉)
Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA
e-mail: xiang@math.udel.edu

The first two examples can be generalized. Let $q = 4t + 1$ be a prime power. The Paley graph $P(q)$ is the graph with the elements of the finite field $\mathbb{F}_q$ as vertices; two vertices are adjacent if and only if their difference is a nonzero square in $\mathbb{F}_q$. One can readily check that $P(q)$ is an $\operatorname{srg}(4t + 1, 2t, t - 1, t)$. For a survey on strongly regular graphs, we refer the reader to [4] and [10]. Strongly regular graphs are closely related to two-weight linear codes, projective two-intersection sets in finite geometry, quasi-symmetric designs, and partial difference sets. We refer the reader to [4, 6, 10, 16] for these connections.

The adjacency matrix of a (simple) graph Γ is a $(0, 1)$-matrix A with rows and columns both indexed by the vertices of Γ, where $A_{xy} = 1$ if and only if x, y have an edge in Γ. Clearly A is symmetric with zeros on the diagonal. The eigenvalues of Γ are by definition the eigenvalues of its adjacency matrix A. For convenience, we call an eigenvalue of Γ *restricted* if it has an eigenvector orthogonal to the all-one vector. Below is a well-known characterization of srg by using their eigenvalues; we refer the reader to [4] for its proof.

Theorem 1.1 *For a graph Γ of order v, neither complete nor edgeless, with adjacency matrix A, the following are equivalent*:

(1) *Γ is an $\operatorname{srg}(v, k, \lambda, \mu)$ for certain integers k, λ, μ.*
(2) *$A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$, where I, J are the identity matrix and the all-one matrix, respectively.*
(3) *A has precisely two distinct restricted eigenvalues.*

The two distinct restricted eigenvalues of an srg are usually denoted by r and s, where r is the positive eigenvalue and s the negative one. The Paley graphs are probably the simplest examples of the so-called cyclotomic strongly regular graphs, which we define below. Let $\mathbb{F}_{p^f}$ be the finite field of order p^f, where p is a prime and f is a positive integer. Let D be a subset of $\mathbb{F}_{p^f}$ such that $-D = D$ and $0 \notin D$. We define the *Cayley graph* $\operatorname{Cay}(\mathbb{F}_{p^f}, D)$ to be the graph with the elements of $\mathbb{F}_{p^f}$ as vertices; two vertices are adjacent if and only if their difference belongs to D. When D is a subgroup of the multiplicative group $\mathbb{F}_{p^f}^*$ of $\mathbb{F}_{p^f}$ and $\operatorname{Cay}(\mathbb{F}_{p^f}, D)$ is strongly regular, then we say that $\operatorname{Cay}(\mathbb{F}_{p^f}, D)$ is a *cyclotomic strongly regular graph*. Specializing to the case where D is the subgroup of $\mathbb{F}_q^*$ consisting of the nonzero squares, where q is a prime power congruent to 1 modulo 4, we see that $\operatorname{Cay}(\mathbb{F}_q, D)$ is nothing but the Paley graph $P(q)$.

Cyclotomic srg have been extensively studied by many authors; see [1, 5, 11, 13, 15, 17, 18]. Some of these authors used the language of cyclic codes in their investigations. We choose to use the language of srg. Let D be a subgroup of $\mathbb{F}_{p^f}^*$ of index $N > 1$. If D is the multiplicative group of a subfield of $\mathbb{F}_{p^f}$, then it is easy to show that $\operatorname{Cay}(\mathbb{F}_{p^f}, D)$ is an srg. These cyclotomic srg are usually called *subfield examples*. Next if there exists a positive integer t such that $p^t \equiv -1 \pmod{N}$, then $\operatorname{Cay}(\mathbb{F}_{p^f}, D)$ is an srg by an old result of Stickelberger [19]. These examples are usually called *semi-primitive* cyclotomic srg. The following conjecture of Schmidt and White [18] says that besides the two classes of cyclotomic srg mentioned above, there are only 11 sporadic examples of cyclotomic srg.

Table 1

N	p	f	$[(\mathbb{Z}_N)^* : \langle p\rangle]$
11	3	5	2
19	5	9	2
35	3	12	2
37	7	9	4
43	11	7	6
67	17	33	2
107	3	53	2
133	5	18	6
163	41	81	2
323	3	144	2
499	5	249	2

Conjecture 1.2 (Conjecture 4.4, [18]) *Let $\mathbb{F}_{p^f}$ be the finite field of order p^f, $N|(\frac{p^f-1}{p-1})$, $N>1$, and let C_0 be the subgroup of $\mathbb{F}_{p^f}^*$ of index N. Assume that $-C_0=C_0$. If* Cay$(\mathbb{F}_{p^f}, C_0)$ *is an srg, then one of the following holds*:

(1) (*subfield case*) *$C_0=\mathbb{F}_{p^e}^*$, where $e|f$*,
(2) (*semi-primitive case*) *There exists a positive integer t such that $p^t\equiv -1$* (mod N),
(3) (*exceptional case*) Cay$(\mathbb{F}_{p^f}, C_0)$ *is one of the eleven "sporadic" examples appearing in Table 1.*

The above conjecture remains open. On the construction side, semi-primitive Gauss sums have been quite useful for constructing strongly regular Cayley graphs. Here by *semi-primitive Gauss sums* $g(\chi)$ over $\mathbb{F}_{p^f}$, where the order of χ is N, we mean that there exists some positive integer t such that $p^t\equiv -1 \pmod N$. In such a situation, it is known that an arbitrary union of cyclotomic classes of order N of $\mathbb{F}_{p^f}$ will give rise to an srg. We refer the reader to [2, 5, 15] and [7] for work in this direction. Quite recently, motivated by the examples of De Lange [14] and Ikuta and Munemasa [11], Feng and Xiang [8] considered the problem of constructing strongly regular graphs Cay$(\mathbb{F}_{p^f}, D)$, where D is a union of at least two cyclotomic classes of order N and it is assumed that a single cyclotomic class of order N does not give rise to an srg. They succeeded in generalizing seven of the index 2 examples of cyclotomic srg in Table 1 into infinite families. The main tools used in [8] are index 2 Gauss sums. We remark that even though the first example in Table 1 is an index 2 example ($\mathrm{ord}_{11}(3)=5$), the construction in [8] could not generalize it into an infinite family since $\mathrm{ord}_{11^m}(3)\neq \phi(11^m)/2$ when $m>1$.

In this paper, we use similar idea to construct strongly regular Cayley graphs. Our goal is to generalize the index 4 example in Table 1. Naturally the main tools that we use are index 4 Gauss sums, which will be introduced Sect. 2. We obtain two infinite families of srg with new parameters. The first family generalizes the index 4 example listed in Table 1, and it has parameters

$$v = 7^{9\cdot 37^{m-1}}, \qquad k = \frac{v-1}{37}, \qquad r = \frac{9\cdot 7^{\frac{9\cdot 37^{m-1}-1}{2}}-1}{37}, \quad \text{and}$$
$$s = \frac{-4\cdot 7^{\frac{9\cdot 37^{m-1}+1}{2}}-1}{37},$$

where $m \geq 1$ is an integer. (Note that the λ and μ values of the srg can be computed from v, k, r and s.) The second family generalizes a (trivial) subfield example of cyclotomic srg, and it has parameters

$$v = 3^{3\cdot 13^{m-1}}, \qquad k = \frac{v-1}{13}, \qquad r = \frac{3^{\frac{3\cdot 13^{m-1}+3}{2}}-1}{13}, \quad \text{and}$$
$$s = \frac{-4\cdot 3^{\frac{3\cdot 13^{m-1}-1}{2}}-1}{13},$$

where $m \geq 1$ is an integer.

2 Index 4 Gauss sums

Let p be a prime, f be a positive integer, and $q = p^f$. Let $\mathbb{F}_q$ be the finite field of order q, ζ_p be a complex primitive pth root of unity, and $\mathrm{Tr}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. The multiplicative characters of $\mathbb{F}_q$ are the homomorphisms from the multiplicative group $\mathbb{F}_q^*$ to the multiplicative group $\mathbb{C}^*$ of the complex field $\mathbb{C}$. On the other hand, the additive characters of $\mathbb{F}_q$ are the homomorphisms from the additive group $(\mathbb{F}_q, +)$ to $\mathbb{C}^*$, and they are given by

$$\psi_a : \mathbb{F}_q \to \mathbb{C}^*, \qquad \psi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)},$$

where $a \in \mathbb{F}_q$. We usually write ψ_1 simply as ψ, which is called the *canonical* additive character of $\mathbb{F}_q$.

Now let χ be a multiplicative character of $\mathbb{F}_q$. Define the Gauss sum by

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

We first list some basic properties of Gauss sums.

Proposition 2.1 (Lemma 1.1 [9])

(1) *Let χ_0 be the trivial multiplicative character of $\mathbb{F}_q$. Then $g(\chi_0) = -1$. Also $g(\chi)\overline{g(\chi)} = q$ for any $\chi \neq \chi_0$.*
(2) *Let $N|(q-1)$, χ be a multiplicative character of $\mathbb{F}_q$ of order N, and $\sigma_{a,b} \in \mathrm{Gal}(\mathbb{Q}(\zeta_N, \zeta_p)/\mathbb{Q})$ be such that $\sigma_{a,b}(\zeta_N) = \zeta_N^a$ and $\sigma_{a,b}(\zeta_p) = \zeta_p^b$. Then $\sigma_{a,b}(g(\chi)) = \overline{\chi}^a(b)g(\chi^a)$. Also $\sigma_{p,1}(g(\chi)) = g(\chi^p) = g(\chi)$.*

For more properties of Gauss sums, we refer the reader to [3] and [12]. Gauss sums can be viewed as the Fourier coefficients of the Fourier expansion of the additive characters in terms of the multiplicative characters of $\mathbb{F}_q$. That is,

$$\psi(a) = \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\bar{\chi})\chi(a), \quad \text{for all } a \in \mathbb{F}_q^*, \tag{2.1}$$

where $\bar{\chi} = \chi^{-1}$ and $\widehat{\mathbb{F}_q^*}$ denotes the character group of $\mathbb{F}_q^*$.

In this paper, we will need certain index 4 Gauss sums, which we define below.

Let p be a prime, $N \geq 2$ such that $\gcd(p(p-1), N) = 1$. Thus $p \in \mathbb{Z}_N^*$, the unit group of $\mathbb{Z}_N$. Furthermore, we assume that $-1 \notin \langle p \rangle$ and the order of p modulo N is $f = \frac{\phi(N)}{4}$. It follows that $[\mathbb{Z}_N^* : \langle p \rangle] = 4$ and the decomposition field K of p in the cyclotomic field $\mathbb{Q}(\zeta_N)$ is a quartic abelian imaginary field. Let χ be a multiplicative character of $\mathbb{F}_q$ of order N. Then the Gauss sum $g(\chi)$ is called an *index 4 Gauss sum*. Note that since we assumed that $\gcd(N, p-1) = 1$, we have $\chi(b) = 1$ for any $b \in \mathbb{F}_p^*$, where $\chi \in \widehat{\mathbb{F}_q^*}$ has order N. It follows that $g(\chi) \in \mathbb{Z}[\zeta_N]$ by part (2) of Proposition 2.1.

Since $\gcd(p(p-1), N) = 1$, N must be odd. The assumption $[\mathbb{Z}_N^* : \langle p \rangle] = 4$ implies that N has at most three distinct prime factors (cf. [9]). In fact, the authors of [9] listed all possibilities of N satisfying the above assumptions. In this paper, we are only concerned with one of these possibilities, namely, $N = p_1^m$, where m is a positive integer, p_1 is an odd prime and $p_1 \equiv 5 \pmod 8$. In this case, the decomposition field K is the unique imaginary cyclic quartic subfield of $\mathbb{Q}(\zeta_N)$. In fact, K is a subfield of $\mathbb{Q}(\zeta_{p_1})$. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is canonically isomorphic to the group $\mathbb{Z}_N^*/\langle p \rangle$. Henceforth, we often identify these two groups. We can choose a primitive element g modulo p_1 such that g is also a primitive element modulo $N = p_1^m$ (cf. [12, p. 43]). Let $\sigma : \zeta_N \mapsto \zeta_N^g$. Then σ is a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ and its restriction to K is a generator of $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_N^*/\langle p \rangle \cong \mathbb{Z}_{p_1}^*/\langle p \rangle$. By the choice of g and the index 4 assumption we have $\mathbb{Z}_{p_1}^* = \langle p \rangle \cup g\langle p \rangle \cup g^2\langle p \rangle \cup g^3\langle p \rangle$. We will use the following notation:

$\tilde{C}_j = g^j \langle p \rangle \subseteq \mathbb{Z}_{p_1}^*$ $(0 \leq j \leq 3)$;
$\tilde{f} = \frac{\phi(p_1)}{4} = \frac{p_1 - 1}{4}$;
$b_j = \frac{1}{p_1} \sum_{z \in ([1, p_1 - 1] \cap \tilde{C}_j)} z$ $(0 \leq j \leq 3)$, where $[1, p_1 - 1]$ denotes the set of integers x, $1 \leq x \leq p_1 - 1$;
$b = \min\{b_0, b_1, b_2, b_3\} = b_\lambda$ for some $\lambda \in \{0, 1, 2, 3\}$;
$c = \min\{b_{\lambda+1} - b, b_{\lambda+3} - b\}$, where the subscripts are read modulo 4;
$\eta_j = \sum_{a \in \tilde{C}_j} \zeta_{p_1}^a$ $(0 \leq j \leq 3)$, where ζ_{p_1} is a complex primitive p_1th root of unity.

Lemma 2.2 [9] *With the above assumptions and notation* $\{\eta_j \mid 0 \leq j \leq 3\}$ *is an integral basis of K, and* $\eta_j = \sigma^j(\eta_0)$, *where* $\sigma(\zeta_{p_1}) = \zeta_{p_1}^g$. *The equation* $p_1 = X^2 + Y^2$ *has a unique integer solution* (A, B) *such that* $A \equiv 3 \pmod 4$. *Furthermore*,

$$4\eta_0, 4\eta_2 = (-1+\sqrt{p_1}) \pm i\sqrt{2}[p_1 - A\sqrt{p_1}]^{\frac{1}{2}},$$
$$4\eta_1, 4\eta_3 = (-1-\sqrt{p_1}) \pm i\sqrt{2}[p_1 + A\sqrt{p_1}]^{\frac{1}{2}}.$$

Below let χ be a multiplicative character of $\mathbb{F}_q$ of order N.

Theorem 2.3 [9] *Under the above assumptions, we have* $p^{-\frac{f-\tilde{f}}{2}-b}g(\chi) \in O_K$ *(the integer ring of* K*).*

By Lemma 2.2, we now write $p^{-\frac{f-\tilde{f}}{2}-b}g(\chi)$ as

$$p^{-\frac{f-\tilde{f}}{2}-b}g(\chi) = N_0\eta_0 + N_1\eta_1 + N_2\eta_2 + N_3\eta_3, \quad N_i \in \mathbb{Z}, \ \forall i.$$

Without loss of generality we assume that

$$4\eta_0 = (-1+\sqrt{p_1}) + i\sqrt{2}[p_1 - A\sqrt{p_1}]^{\frac{1}{2}} = 4\overline{\eta}_2,$$
$$4\eta_1 = (-1-\sqrt{p_1}) + i\sqrt{2}[p_1 + A\sqrt{p_1}]^{\frac{1}{2}} = 4\overline{\eta}_3.$$

Then

$$\begin{aligned} &4p^{-\frac{f-\tilde{f}}{2}-b}g(\chi) \\ &\quad= -(N_0+N_1+N_2+N_3) + (N_0-N_1+N_2-N_3)\sqrt{p_1} \\ &\qquad + i\sqrt{2}\big[(N_0-N_2)(p_1-A\sqrt{p_1})^{\frac{1}{2}} + (N_1-N_3)(p_1+A\sqrt{p_1})^{\frac{1}{2}}\big]. \end{aligned} \tag{2.2}$$

We make the following transformation:

$$\begin{cases} M_0 = N_0+N_1+N_2+N_3, \\ M_1 = N_0+N_1-N_2-N_3, \\ M_2 = N_0-N_1+N_2-N_3, \\ M_3 = N_0-N_1-N_2+N_3, \end{cases} \qquad \begin{cases} 4N_0 = M_0+M_1+M_2+M_3, \\ 4N_1 = M_0+M_1-M_2-M_3, \\ 4N_2 = M_0-M_1+M_2-M_3, \\ 4N_3 = M_0-M_1-M_2+M_3. \end{cases}$$

Then

$$\begin{aligned} &4p^{-\frac{f-\tilde{f}}{2}-b}g(\chi) \\ &\quad= -M_0 + M_2\sqrt{p_1} \\ &\qquad + i\sqrt{2}\left[\frac{M_1+M_3}{2}(p_1-A\sqrt{p_1})^{\frac{1}{2}} + \frac{M_1-M_3}{2}(p_1+A\sqrt{p_1})^{\frac{1}{2}}\right]. \end{aligned} \tag{2.3}$$

Theorem 2.4 [9] *The integers* M_0, M_1, M_2, M_3 *defined above satisfy the following conditions*:

$$\begin{cases} 16p^{\tilde{f}-2b} = M_0^2 + p_1\big(M_1^2+M_2^2+M_3^2\big), \\ 2M_0M_2 + 2AM_1M_3 = B\big(M_1^2 - M_3^2\big), \\ M_0+M_1+M_2+M_3 \equiv 0 \pmod 4, \\ M_1 \equiv M_2 \equiv M_3 \pmod 2, \\ M_0 \equiv 4p^{-b} \pmod{p_1}. \end{cases}$$

3 Cyclotomic classes and strongly regular Cayley graphs

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

$$C_i = \left\{\gamma^{i+jN} \,\middle|\, 0 \le j \le \frac{q-1}{N} - 1\right\},$$

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

Note that C_0 consists of all the Nth powers in $\mathbb{F}_q^*$. Therefore C_0 does not depend on the choice of γ. The other classes C_i, $1 \le i \le N-1$, do depend on the choice of γ. As usual, let ψ be the canonical additive character of $\mathbb{F}_q$. The Nth *cyclotomic periods* (also called *Gauss periods*) are defined by

$$\tau_a = \sum_{x \in C_a} \psi(x),$$

where $0 \le a \le N-1$.

Now using (2.1), we have

$$\begin{aligned}\tau_a &= \sum_{x \in C_0} \psi\left(\gamma^a x\right) \\ &= \sum_{x \in C_0} \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\bar{\chi})\chi\left(\gamma^a x\right) \\ &= \frac{1}{(q-1)} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\bar{\chi})\chi\left(\gamma^a\right) \sum_{x \in C_0} \chi(x) \\ &= \frac{1}{N} \sum_{\chi \in C_0^{\perp}} g(\bar{\chi})\chi\left(\gamma^a\right),\end{aligned}$$

where $C_0^{\perp}$ is the subgroup of $\widehat{\mathbb{F}_q^*}$ consisting of all characters χ which are trivial on C_0, i.e. $C_0^{\perp}$ is the unique subgroup of $\widehat{\mathbb{F}_q^*}$ of order N. The above computations give the relationship between Gauss periods and Gauss sums.

Assume that $N = p_1^m$, where p_1 is an odd prime and $p_1 \equiv 5 \pmod 8$, and $p_1 > 5$. Let $p \ne p_1$ be a prime such that $[\mathbb{Z}_N^* : \langle p \rangle] = 4$. It follows that $\gcd(p-1, p_1) = 1$. (This can be seen as follows. If $p \equiv 1 \pmod{p_1}$, then by using Lemma 3 of [12, p. 42] repeatedly, we obtain $p^{p_1^{m-1}} \equiv 1 \pmod{p_1^m}$, contradicting the assumptions that $\mathrm{ord}_{p_1^m}(p) = \frac{p_1^{m-1}(p_1-1)}{4}$ and $p_1 > 5$.) Therefore we have $\gcd(p(p-1), N) = 1$. Define $f = \mathrm{ord}_N(p) = \frac{1}{4}\phi(N)$ and $q = p^f$. Let $C_0, C_1, \dots, C_{N-1}$ be the Nth cyclotomic classes of $\mathbb{F}_q$. Define

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i. \tag{3.1}$$

Using D as connection set, we construct the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$.

Theorem 3.1 *The Cayley graph* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is an undirected, simple, regular graph of valency* $|D|$, *and it has at most five distinct restricted eigenvalues.*

Proof Note that $-1 \in C_0$ since either $2N|(q-1)$ or q is even. Hence $-C_i = C_i$ for all $0 \le i \le N-1$, so $D = -D$. Also $0 \notin D$. We conclude that the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is undirected and without loops. The Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is clearly regular of valency $|D|$. The restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, D)$, as explained in [4, p. 122], are given by

$$\psi\left(\gamma^a D\right) = \sum_{x \in D} \psi\left(\gamma^a x\right), \quad 0 \le a \le N-1.$$

Now we turn to the computations of $\psi(\gamma^a D)$. We have

$$\begin{aligned}
\psi\left(\gamma^a D\right) &= \sum_{i=0}^{p_1^{m-1}-1} \psi\left(\gamma^a C_i\right) \\
&= \sum_{i=0}^{p_1^{m-1}-1} \tau_{i+a} \\
&= \frac{1}{N} \sum_{i=0}^{p_1^{m-1}-1} \sum_{\chi \in C_0^{\perp}} g(\bar{\chi}) \chi\left(\gamma^{a+i}\right) \\
&= \frac{1}{N} \sum_{\chi \in C_0^{\perp}} g(\bar{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi\left(\gamma^{a+i}\right).
\end{aligned}$$

Consider the inner sum $\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i})$, where $\chi \in C_0^{\perp}$. Note that $C_0^{\perp}$ is the unique subgroup of $\widehat{\mathbb{F}_q^*}$ of order $N = p_1^m$. If $\chi \in C_0^{\perp}$ and $\mathrm{ord}(\chi) = 1$ (that is, $\chi = \chi_0$), then $g(\bar{\chi}) = -1$ and $\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = p_1^{m-1}$. If $\chi \in C_0^{\perp}$ and $\mathrm{ord}(\chi) = p_1^j$ $(1 \le j \le m-1)$, then $\chi(\gamma) \ne 1$, $\chi(\gamma)^{p_1^{m-1}} = 1$, and $\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = \chi(\gamma^a) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^i) = \chi(\gamma^a) \frac{\chi(\gamma)^{p_1^{m-1}}-1}{\chi(\gamma)-1} = 0$. Hence,

$$\psi\left(\gamma^a D\right) = \frac{1}{N}\left(-p_1^{m-1} + \sum_{\substack{\chi \in C_0^{\perp} \\ \mathrm{ord}(\chi) = p_1^m}} g(\bar{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi\left(\gamma^{a+i}\right)\right).$$

Next, we consider the characters $\chi \in C_0^{\perp}$ such that $\mathrm{ord}(\chi) = N = p_1^m$, i.e., the generators of $C_0^{\perp}$. We define a multiplicative character θ of $\mathbb{F}_q$ by setting $\theta(\gamma) = \zeta_N$. It is clear that θ is a generator of $C_0^{\perp}$. Thus all generators of $C_0^{\perp}$ are given by θ^t, where $t \in \mathbb{Z}_N^*$. It follows that

$$\psi\big(\gamma^a D\big) = \frac{1}{N}\left(-p_1^{m-1} + \sum_{\substack{\chi\in C_0^{\perp}\\ \mathrm{ord}(\chi)=p_1^m}} g(\bar{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi\big(\gamma^{a+i}\big)\right)$$

$$= \frac{1}{N}\left(-p_1^{m-1} + \sum_{t\in\mathbb{Z}_{p_1^m}^*} g\big(\bar{\theta}^t\big) \sum_{i=0}^{p_1^{m-1}-1} \theta^t\big(\gamma^{a+i}\big)\right).$$

For convenience, we set

$$S_a := \sum_{t\in\mathbb{Z}_{p_1^m}^*} g\big(\bar{\theta}^t\big) \sum_{i=0}^{p_1^{m-1}-1} \theta^t\big(\gamma^{a+i}\big),$$

where $0 \le a \le N-1$.

For each $t \in \mathbb{Z}_{p_1^m}^*$, we write $t = t_1 + p_1 t_2$, where $t_1 \in \mathbb{Z}_{p_1}^*$, $t_2 \in \mathbb{Z}_{p_1^{m-1}}$. For each $a, 0 \le a \le N-1$, there is a unique $i_a \in \{0, 1, 2, \dots, p_1^{m-1}-1\}$, such that $p_1^{m-1} \mid (a+i_a)$. Write $a + i_a = p_1^{m-1} j_a$ for some integer j_a. (When $N = p_1$, we have $i_a = 0$ and $j_a = a$ for all $0 \le a \le N-1$.)

By Theorem 2.3, we have $p^{-\frac{f-\tilde{f}}{2}-b} g(\bar{\theta}) \in O_K$. We can write $p^{-\frac{f-\tilde{f}}{2}-b} g(\bar{\theta}) = N_0\eta_0 + N_1\eta_1 + N_2\eta_2 + N_3\eta_3$, $N_i \in \mathbb{Z}$, $\forall i$. Making the following transformation:

$$\begin{cases} M_0 = N_0 + N_1 + N_2 + N_3, \\ M_1 = N_0 + N_1 - N_2 - N_3, \\ M_2 = N_0 - N_1 + N_2 - N_3, \\ M_3 = N_0 - N_1 - N_2 + N_3. \end{cases}$$

By Theorem 2.4, the integers M_0, M_1, M_2, M_3 satisfy the following conditions:

$$\begin{cases} 16p^{\tilde{f}-2b} = M_0^2 + p_1\big(M_1^2 + M_2^2 + M_3^2\big), \\ 2M_0M_2 + 2AM_1M_3 = B\big(M_1^2 - M_3^2\big), \\ M_0 + M_1 + M_2 + M_3 \equiv 0 \pmod 4, \\ M_1 \equiv M_2 \equiv M_3 \pmod 2, \\ M_0 \equiv 4p^{-b} \pmod{p_1}. \end{cases} \tag{3.2}$$

Here the notation is the same as in Sect. 2.

Next we want to determine how many distinct values $\psi(\gamma^a D)$, $0 \le a \le N-1$, will take. Since $\psi(\gamma^a D) = \frac{1}{N}(-p_1^{m-1} + S_a)$, it suffices to determine the value distribution of $\{S_a \mid 0 \le a \le N-1\}$.

Since η_j, $0 \le j \le 3$, are in $\mathbb{Q}(\zeta_{p_1})$, we have $\sigma_t(\eta_j) = \sigma_{t_1+p_1t_2}(\eta_j) = \sigma_{t_1}(\eta_j)$. Hence $\sigma_t(g(\bar{\theta})) = \sigma_{t_1}(g(\bar{\theta}))$. Therefore $g(\bar{\theta}^t) = g(\bar{\theta}^{t_1}) = p^{\frac{f-\tilde{f}}{2}+b}(N_0\eta_0^{\sigma_{t_1}} + N_1\eta_1^{\sigma_{t_1}} + N_2\eta_2^{\sigma_{t_1}} + N_3\eta_3^{\sigma_{t_1}})$. We now continue the computations of S_a. We have

$$\begin{aligned}
S_a &= \sum_{t \in \mathbb{Z}^*_{p_1^m}} g(\bar{\theta}^t) \sum_{i=0}^{p_1^{m-1}-1} \theta^t(\gamma^{a+i}) \\
&= \sum_{t_1 \in \mathbb{Z}^*_{p_1}} \sum_{t_2 \in \mathbb{Z}_{p_1^{m-1}}} g(\bar{\theta}^{t_1+p_1t_2}) \sum_{i=0}^{p_1^{m-1}-1} \theta^{t_1+p_1t_2}(\gamma^{a+i}) \\
&= \sum_{t_1 \in \mathbb{Z}^*_{p_1}} \sum_{t_2 \in \mathbb{Z}_{p_1^{m-1}}} g(\bar{\theta}^{t_1}) \sum_{i=0}^{p_1^{m-1}-1} \theta^{t_1+p_1t_2}(\gamma^{a+i}) \\
&= \sum_{t_1 \in \mathbb{Z}^*_{p_1}} \sum_{i=0}^{p_1^{m-1}-1} g(\bar{\theta}^{t_1})\theta^{t_1}(\gamma^{a+i}) \sum_{t_2 \in \mathbb{Z}_{p_1^{m-1}}} (\theta^{p_1}(\gamma^{a+i}))^{t_2}.
\end{aligned}$$

If $\theta^{p_1(a+i)}(\gamma) \neq 1$, that is, $p_1^{m-1} \nmid (a+i)$, then

$$\sum_{t_2 \in \mathbb{Z}_{p_1^{m-1}}} (\theta^{p_1}(\gamma^{a+i}))^{t_2} = \frac{1-\theta^{p_1(a+i)\cdot p_1^{m-1}}(\gamma)}{1-\theta^{p_1(a+i)}(\gamma)} = 0.$$

Recall that for each a, $0 \le a \le N-1$, there is a unique $i_a \in \{0, 1, 2, \dots, p_1^{m-1}-1\}$, such that $p_1^{m-1} \mid (a+i_a)$, and we write $a + i_a = p_1^{m-1} j_a$. Thus we have

$$S_a = p_1^{m-1} \sum_{t_1 \in \mathbb{Z}^*_{p_1}} g(\bar{\theta}^{t_1})\theta^{t_1}(\gamma^{p_1^{m-1} j_a}).$$

Note that by the definition of θ, we have $\theta^{t_1}(\gamma^{p_1^{m-1} j_a}) = \zeta_N^{p_1^{m-1} j_a \cdot t_1} = \zeta_{p_1}^{j_a \cdot t_1}$. It will be convenient to introduce ψ_{j_a}, which is an additive character of the prime field $\mathbb{Z}_{p_1}$ such that $\psi_{j_a}(t_1) = \zeta_{p_1}^{j_a \cdot t_1}$. In this way, we have $\theta^{t_1}(\gamma^{p_1^{m-1} j_a}) = \psi_{j_a}(t_1)$. We now have

$$\begin{aligned}
S_a &= p_1^{m-1} \sum_{t_1 \in \mathbb{Z}^*_{p_1}} g(\bar{\theta}^{t_1})\psi_{j_a}(t_1) \\
&= p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b} \sum_{t_1 \in \mathbb{Z}^*_{p_1}} (N_0\eta_0^{\sigma_{t_1}} + N_1\eta_1^{\sigma_{t_1}} + N_2\eta_2^{\sigma_{t_1}} + N_3\eta_3^{\sigma_{t_1}})\psi_{j_a}(t_1) \\
&= p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b} \sum_{i=0}^{3} \sum_{t_1 \in g^i\langle p\rangle} (N_0\eta_0^{\sigma_{t_1}} + N_1\eta_1^{\sigma_{t_1}} + N_2\eta_2^{\sigma_{t_1}} + N_3\eta_3^{\sigma_{t_1}})\psi_{j_a}(t_1) \\
&= p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b} \Bigg[(N_0\eta_0 + N_1\eta_1 + N_2\eta_2 + N_3\eta_3) \sum_{t_1 \in \langle p\rangle} \psi_{j_a}(t_1) \\
&\quad + (N_0\eta_1 + N_1\eta_2 + N_2\eta_3 + N_3\eta_0) \sum_{t_1 \in g\langle p\rangle} \psi_{j_a}(t_1)
\end{aligned}$$

$$+ (N_0\eta_2 + N_1\eta_3 + N_2\eta_0 + N_3\eta_1) \sum_{t_1 \in g^2\langle p\rangle} \psi_{j_a}(t_1)$$
$$+ (N_0\eta_3 + N_1\eta_0 + N_2\eta_1 + N_3\eta_2) \sum_{t_1 \in g^3\langle p\rangle} \psi_{j_a}(t_1)\Bigg].$$

When a runs through $\mathbb{Z}_N$, j_a runs through $\mathbb{Z}_{p_1}$ correspondingly. Note that $\mathbb{Z}_{p_1}^* = \langle p\rangle \cup g\langle p\rangle \cup g^2\langle p\rangle \cup g^3\langle p\rangle$. We therefore have five cases to consider according to $j_a = 0$, and $j_a \in g^i\langle p\rangle$, $i = 0, 1, 2, 3$.

Case I. $j_a = 0$. In this case, we have $\sum_{t_1 \in g^i\langle p\rangle} \psi_{j_a}(t_1) = \frac{p_1-1}{4}$, for $0 \le i \le 3$.

$$\begin{aligned} S_a = p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b}\Bigg[&(N_0\eta_0 + N_1\eta_1 + N_2\eta_2 + N_3\eta_3)\frac{p_1-1}{4} \\ &+ (N_0\eta_1 + N_1\eta_2 + N_2\eta_3 + N_3\eta_0)\frac{p_1-1}{4} \\ &+ (N_0\eta_2 + N_1\eta_3 + N_2\eta_0 + N_3\eta_1)\frac{p_1-1}{4} \\ &+ (N_0\eta_3 + N_1\eta_0 + N_2\eta_1 + N_3\eta_2)\frac{p_1-1}{4}\Bigg] \\ = -p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b}&(N_0 + N_1 + N_2 + N_3)\frac{p_1-1}{4}. \end{aligned}$$

This value of S_a will be denoted by $p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b} T_1$, where $T_1 = (N_0 + N_1 + N_2 + N_3)\frac{1-p_1}{4}$.

Case II. $j_a \in \langle p\rangle$. In this case $\sum_{t_1 \in g^i\langle p\rangle} \psi_{j_a}(t_1) = \eta_i$, $0 \le i \le 3$. We have

$$\begin{aligned} S_a &= p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b}\big[(N_0\eta_0 + N_1\eta_1 + N_2\eta_2 + N_3\eta_3)\eta_0 \\ &\quad + (N_0\eta_1 + N_1\eta_2 + N_2\eta_3 + N_3\eta_0)\eta_1 \\ &\quad + (N_0\eta_2 + N_1\eta_3 + N_2\eta_0 + N_3\eta_1)\eta_2 \\ &\quad + (N_0\eta_3 + N_1\eta_0 + N_2\eta_1 + N_3\eta_2)\eta_3\big] \\ &= p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b}\big[N_0\big(\eta_0^2 + \eta_1^2 + \eta_2^2 + \eta_3^2\big) \\ &\quad + N_1(\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_0) \\ &\quad + N_2(\eta_0\eta_2 + \eta_1\eta_3 + \eta_2\eta_0 + \eta_3\eta_1) \\ &\quad + N_3(\eta_0\eta_3 + \eta_1\eta_0 + \eta_2\eta_1 + \eta_3\eta_2)\big]. \end{aligned}$$

This value of S_a will be denoted by $p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b} T_2$.

Case III. $j_a \in g\langle p\rangle$. In this case $\sum_{t_1 \in g^i\langle p\rangle} \psi_{j_a}(t_1) = \eta_{i+1}$, $0 \le i \le 3$. Similarly we have

$$\begin{aligned} S_a = p_1^{m-1} p^{\frac{f-\tilde{f}}{2}+b}\big[&N_0(\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_0) \\ &+ N_1\big(\eta_0^2 + \eta_1^2 + \eta_2^2 + \eta_3^2\big) \\ &+ N_2(\eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_0) \\ &+ N_3(\eta_0\eta_2 + \eta_1\eta_3 + \eta_2\eta_0 + \eta_3\eta_1)\big]. \end{aligned}$$

This value of S_a will be denoted by $p_1^{m-1}p^{\frac{f-\tilde{f}}{2}+b}T_3$.

Case IV. $j_a \in g^2\langle p\rangle$. In this case $\sum_{t_1\in g^i\langle p\rangle}\psi_{j_a}(t_1)=\eta_{i+2}$, $0\le i\le 3$. Similarly we have

$$\begin{aligned}S_a = p_1^{m-1}p^{\frac{f-\tilde{f}}{2}+b}\big[&N_0(\eta_0\eta_2+\eta_1\eta_3+\eta_2\eta_0+\eta_3\eta_1)\\ &+N_1(\eta_0\eta_1+\eta_1\eta_2+\eta_2\eta_3+\eta_3\eta_0)\\ &+N_2\big(\eta_0^2+\eta_1^2+\eta_2^2+\eta_3^2\big)\\ &+N_3(\eta_0\eta_3+\eta_1\eta_0+\eta_2\eta_1+\eta_3\eta_2)\big].\end{aligned}$$

This value of S_a will be denoted by $p_1^{m-1}p^{\frac{f-\tilde{f}}{2}+b}T_4$.

Case V. $j_a \in g^3\langle p\rangle$. In this case $\sum_{t_1\in g^i\langle p\rangle}\psi_{j_a}(t_1)=\eta_{i+3}$, $0\le i\le 3$. Similarly we have

$$\begin{aligned}S_a = p_1^{m-1}p^{\frac{f-\tilde{f}}{2}+b}\big[&N_0(\eta_0\eta_3+\eta_1\eta_0+\eta_2\eta_1+\eta_3\eta_2)\\ &+N_1(\eta_0\eta_2+\eta_1\eta_3+\eta_2\eta_0+\eta_3\eta_1)\\ &+N_2(\eta_0\eta_1+\eta_1\eta_2+\eta_2\eta_3+\eta_3\eta_0)\\ &+N_3\big(\eta_0^2+\eta_1^2+\eta_2^2+\eta_3^2\big)\big].\end{aligned}$$

This value of S_a will be denoted by $p_1^{m-1}p^{\frac{f-\tilde{f}}{2}+b}T_5$.

Therefore we have shown that S_a, $0\le a\le N-1$, take at most five distinct values. It follows that the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ has at most five distinct restricted eigenvalues. The proof of the theorem is complete. □

We are now ready to consider the question that under what conditions, the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with D defined in (3.1), is strongly regular. By Theorem 1.1, the question is the same as asking under what conditions, the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ will have exactly two distinct restricted eigenvalues. Using the transformation between $\{N_0, N_1, N_2, N_3\}$ and $\{M_0, M_1, M_2, M_3\}$, and the following equations satisfied by η_i:

$$\begin{cases}\eta_0^2+\eta_1^2+\eta_2^2+\eta_3^2=\dfrac{1-p_1}{4},\\[2mm] \eta_0\eta_1+\eta_1\eta_2+\eta_2\eta_3+\eta_3\eta_0=\dfrac{1-p_1}{4},\\[2mm] \eta_0\eta_2+\eta_1\eta_3+\eta_2\eta_0+\eta_3\eta_1=\dfrac{1+3p_1}{4},\end{cases}$$

we have $\{T_1, T_2, T_3, T_4, T_5\} = \{\frac{1-p_1}{4}M_0, \frac{1-p_1}{4}M_0 + p_1N_0, \frac{1-p_1}{4}M_0 + p_1N_1, \frac{1-p_1}{4}M_0 + p_1N_2, \frac{1-p_1}{4}M_0 + p_1N_3\}$. From the proof of Theorem 3.1, we see that the value distribution of the restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, D)$ is completely determined by the value distribution of $\{T_1, T_2, T_3, T_4, T_5\}$.

Theorem 3.2 *If* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is strongly regular, then either* p_1-1 *or* p_1-9 *is a perfect square. In the case where* p_1-1 *is a square*, $\mathrm{Cay}(\mathbb{F}_q, D)$ *is strongly regular if and only if the integer solutions* (M_0, M_1, M_2, M_3) *of* (3.2) *satisfy* $(M_0 : M_1 : M_2 :$

$M_3) \in \{(1:1:1:1), (1:1:-1:-1), (1:-1:1:-1), (1:-1:-1:1)\}$. *In the case where* $p_1 - 9$ *is a square*, $\mathrm{Cay}(\mathbb{F}_q, D)$ *is strongly regular if and only if the integer solutions* (M_0, M_1, M_2, M_3) *of* (3.2) *satisfy* $(M_0 : M_1 : M_2 : M_3) \in \{(3:-1:-1:-1), (3:-1:1:1), (3:1:-1:1), (3:1:1:-1)\}$.

Proof Up to a permutation of indices, we may assume that

$$\begin{cases} T_1 = \dfrac{1-p_1}{4} M_0, \\ T_2 = \dfrac{1-p_1}{4} M_0 + p_1 N_0, \\ T_3 = \dfrac{1-p_1}{4} M_0 + p_1 N_1, \\ T_4 = \dfrac{1-p_1}{4} M_0 + p_1 N_2, \\ T_5 = \dfrac{1-p_1}{4} M_0 + p_1 N_3. \end{cases}$$

We first note that the set $\{T_1, T_2, T_3, T_4, T_5\}$ has at least two distinct elements. Otherwise, we will have $N_0 = N_1 = N_2 = N_3 = 0$; it follows that the Gauss sum $g(\bar{\theta}) = 0$, which is impossible.

If the set $\{T_1, T_2, T_3, T_4, T_5\}$ has exactly two distinct elements, there are fifteen possible cases in total. We discuss these cases one by one.

Case 1. $T_2 = T_3 = T_4 = T_5 \neq T_1 \Leftrightarrow N_0 = N_1 = N_2 = N_3 \neq 0 \Leftrightarrow M_1 = M_2 = M_3 = 0, M_0 \neq 0$. Under the assumptions of this case, we have $M_0^2 = 16 p^{\tilde{f}-2b}$. But $\tilde{f} = \frac{p_1-1}{4}$ is odd since $p_1 \equiv 5 \pmod 8$. It follows that $M_0 \notin \mathbb{Z}$, a contradiction. We conclude that Case 1 cannot occur.

Case 2. $T_1 = T_3 = T_4 = T_5 \neq T_2 \Leftrightarrow N_1 = N_2 = N_3 = 0, N_0 \neq 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (1:1:1:1)$. In this case we have $A = -1$ and $p_1 - 1 = B^2$.

Case 3. $T_1 = T_2 = T_4 = T_5 \neq T_3 \Leftrightarrow N_0 = N_2 = N_3 = 0, N_1 \neq 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (1:1:-1:-1)$. In this case we have $A = -1$ and $p_1 - 1 = B^2$.

Case 4. $T_1 = T_2 = T_3 = T_5 \neq T_4 \Leftrightarrow N_0 = N_1 = N_3 = 0, N_2 \neq 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (1:-1:1:-1)$. In this case we have $A = -1$ and $p_1 - 1 = B^2$.

Case 5. $T_1 = T_2 = T_3 = T_4 \neq T_5 \Leftrightarrow N_0 = N_1 = N_2 = 0, N_3 \neq 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (1:-1:-1:1)$. In this case we have $A = -1$ and $p_1 - 1 = B^2$.

Case 6. $T_1 = T_4 = T_5 \neq T_2 = T_3 \Leftrightarrow N_2 = N_3 = 0, N_0 = N_1 \neq 0 \Leftrightarrow M_0 = M_1 \neq 0,\ M_2 = M_3 = 0$. In this case we have $B = 0$, which is impossible.

Case 7. $T_1 = T_3 = T_5 \neq T_2 = T_4 \Leftrightarrow N_1 = N_3 = 0, N_0 = N_2 \neq 0 \Leftrightarrow M_0 = M_2, M_1 = M_3 = 0$. In this case, we have $M_0 = M_1 = M_2 = M_3 = 0$, which is impossible.

Case 8. $T_1 = T_3 = T_4 \neq T_2 = T_5 \Leftrightarrow N_1 = N_2 = 0, N_0 = N_3 \neq 0 \Leftrightarrow M_0 = M_3 \neq 0\ , M_1 = M_2 = 0$. In this case we have $B = 0$, which is impossible.

Case 9. $T_1 = T_2 = T_5 \neq T_3 = T_4 \Leftrightarrow N_0 = N_3 = 0, N_1 = N_2 \neq 0 \Leftrightarrow M_0 = -M_3$, $M_1 = M_2 = 0$. In this case we have $B = 0$, which is impossible.

Case 10. $T_1 = T_2 = T_4 \neq T_3 = T_5 \Leftrightarrow N_0 = N_2 = 0, N_1 = N_3 \neq 0 \Leftrightarrow M_0 = -M_2, M_1 = M_3 = 0$. In this case we have $M_0 = M_1 = M_2 = M_3 = 0$, which is impossible.

Case 11. $T_1 = T_2 = T_3 \neq T_4 = T_5 \Leftrightarrow N_0 = N_1 = 0, N_2 = N_3 \neq 0 \Leftrightarrow M_0 = -M_1$, $M_2 = M_3 = 0$. In this case we have $B = 0$, which is impossible.
Case 12. $T_3 = T_4 = T_5 \neq T_1 = T_2 \Leftrightarrow N_1 = N_2 = N_3 \neq 0, N_0 = 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (3 : -1 : -1 : -1)$. In this case we have $A = 3$ and $p_1 - 9 = B^2$.
Case 13. $T_2 = T_4 = T_5 \neq T_1 = T_3 \Leftrightarrow N_0 = N_2 = N_3 \neq 0, N_1 = 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (3 : -1 : 1 : 1)$. In this case we have $A = 3$ and $p_1 - 9 = B^2$.
Case 14. $T_2 = T_3 = T_5 \neq T_1 = T_4 \Leftrightarrow N_0 = N_1 = N_3 \neq 0, N_2 = 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (3 : 1 : -1 : 1)$. In this case we have $A = 3$ and $p_1 - 9 = B^2$.
Case 15. $T_2 = T_3 = T_4 \neq T_1 = T_5 \Leftrightarrow N_0 = N_1 = N_2 \neq 0, N_3 = 0 \Leftrightarrow (M_0 : M_1 : M_2 : M_3) = (3 : 1 : 1 : -1)$. In this case we have $A = 3$ and $p_1 - 9 = B^2$.

If $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular, then it has exactly two distinct restricted eigenvalues, thus $\{T_1, T_2, T_3, T_4, T_5\}$ has exactly two distinct elements. From the analysis above, either $p_1 - 1$ or $p_1 - 9$ is a square; suppose (M_0, M_1, M_2, M_3) is a solution of (3.2), we see that (M_0, M_1, M_2, M_3) must be one of the possibilities listed in the statement of the theorem. That is, when $A = -1$, $p_1 - 1$ is a perfect square, $(M_0 : M_1 : M_2 : M_3) \in \{(1 : 1 : 1 : 1), (1 : 1 : -1 : -1), (1 : -1 : 1 : -1), (1 : -1 : -1 : 1)\}$; when $A = 3$, $p_1 - 9$ is perfect square and $(M_0 : M_1 : M_2 : M_3) \in \{(3 : -1 : -1 : -1), (3 : -1 : 1 : 1), (3 : 1 : -1 : 1), (3 : 1 : 1 : -1)\}$.

Conversely, if the integer solutions (M_0, M_1, M_2, M_3) of (3.2) satisfy the conditions stated in the theorem, then it is easy to see from the above analysis that $\{T_1, T_2, T_3, T_4, T_5\}$ has exactly two distinct elements. It follows that $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular.

The proof of the theorem is now complete. □

4 New infinite families of strongly regular Cayley graphs

We used a computer to search for prime pairs (p, p_1), $2 \le p < 10{,}000$, $3 \le p_1 < 10{,}000$, satisfying the conditions specified in Sect. 2 and in the statement of Theorem 3.2. We found two such pairs which are given below. Note that in general for a prime pair (p, p_1) satisfying the conditions $p_1 \equiv 5 \pmod 8$, $\gcd(p(p-1), p_1) = 1$ and $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)/4$ for all $m \ge 1$, there are possibly many solutions (M_1, M_2, M_3, M_4) to (3.2); only those solutions (M_1, M_2, M_3, M_4) which can be used to represent the Gauss sums $g(\bar{\theta})$ should be considered. We refer the reader to Lemma 3.2 of [9] for a method to decide when a solution (M_1, M_2, M_3, M_4) to (3.2) can be used to represent the Gauss sum $g(\bar{\theta})$.

Example 4.1 Let $p_1 = 37$, $p = 7$, $N = p_1^m$ where $m \ge 1$ is any integer. Note that in this case we have $p_1 \equiv 5 \pmod 8$ and $p_1 > 5$. It is straightforward to check that $\mathrm{ord}_{37}(7) = 9 = \frac{\phi(37)}{4}$. By induction on m, one can show that $\mathrm{ord}_{37^m}(7) = \frac{\phi(37^m)}{4}$. Let $f = \mathrm{ord}_{37^m}(7) = \frac{\phi(37^m)}{4}$ and $\mathbb{F}_q$ be the finite field of order $q = 7^f$. Let γ be a fixed primitive element of $\mathbb{F}_q$. Let $C_0 = \langle \gamma^N \rangle, C_1 = \gamma C_0, \dots, C_{N-1} = \gamma^{N-1} C_0$ be the Nth cyclotomic classes of $\mathbb{F}_q$ and let

$$D = \bigcup_{i=0}^{37^{m-1}-1} C_i.$$

We claim that the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular. To prove this claim, it suffices to apply Theorem 3.2 to the current situation.

Lemma 4.1 (Example 1, [9]) *When* $p_1 = 13$ *or* 37, *we have*

$$b = \min\{b_0, b_1, b_2, b_3\} = \frac{\tilde{f} - 1}{2},$$

where $\tilde{f} = \frac{\phi(p_1)}{4}$.

Now for $p_1 = 37$, we have $\tilde{f} = \frac{\phi(37)}{4} = 9, b = 4$, and $p_1 - 1 = 36$ is a perfect square. The integer solutions (A, B) to $p_1 = A^2 + B^2$ with $A \equiv 3 \pmod 4$ are $(-1, \pm 6)$. That is, $A = -1$ and $B = \pm 6$. Also $4p^{-b} = 4 \cdot 7^{-4} \equiv 4 \cdot 9 \equiv -1 \pmod{37}$. We need to determine the (M_0, M_1, M_2, M_3) satisfying (3.2). In our case, (3.2) becomes

$$\begin{cases} 112 = M_0^2 + 37\bigl(M_1^2 + M_2^2 + M_3^2\bigr), \\ 2M_0M_2 - 2M_1M_3 = B\bigl(M_1^2 - M_3^2\bigr), \\ M_0 + M_1 + M_2 + M_3 \equiv 0 \pmod 4, \\ M_1 \equiv M_2 \equiv M_3 \pmod 2, \\ M_0 \equiv -1 \pmod{37}. \end{cases}$$

From the first equation we obtain $M_0^2 = 1$ and $M_1^2 + M_2^2 + M_3^2 = 3$. Therefore, $M_0 = -1$, and $M_1, M_2, M_3 \in \{\pm 1\}$. Together with the conditions, we get a total of four integer solutions $(-1, 1, 1, -1)$, $(-1, 1, -1, 1)$, $(-1, -1, 1, 1)$, $(-1, -1, -1, -1)$. Since each of these four solutions satisfies the conditions of Theorem 3.2, we conclude that $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph, with parameters

$$v = 7^{9\cdot 37^{m-1}}, \qquad k = \frac{v-1}{37}, \qquad r = \frac{9 \cdot 7^{\frac{9\cdot 37^{m-1}-1}{2}} - 1}{37}, \quad \text{and}$$

$$s = \frac{-4 \cdot 7^{\frac{9\cdot 37^{m-1}+1}{2}} - 1}{37}.$$

Example 4.2 Let $p_1 = 13$, $p = 3$, $N = p_1^m$, where $m \geq 1$ is an integer. By induction on m, we also can show that $\mathrm{ord}_{13^m}(3) = \frac{\phi(13^m)}{4}$. Also, we let $f = \frac{\phi(13^m)}{4}$, $q = 3^f$, and $C_0, C_1, \dots, C_{N-1}$ be the Nth cyclotomic classes of $\mathbb{F}_q$. Using

$$D = \bigcup_{i=0}^{13^{m-1}-1} C_i$$

as connection set, we construct the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$. Now $p_1 - 9 = 4$ is a perfect square, $\tilde{f} = \frac{\phi(13)}{4} = 3$ and $b = \frac{\tilde{f}-1}{2} = 1$ by Lemma 4.1.

The integer solutions (A, B) to $p_1 = A^2 + B^2$ with $A \equiv 3 \pmod 4$ are $(3, \pm 2)$. That is, $A = 3$ and $B = \pm 2$. Also $4p^{-b} = 4 \cdot 3^{-1} \equiv 4 \cdot (-4) \equiv -3 \pmod{13}$. We need to determine the (M_0, M_1, M_2, M_3) satisfying (3.2). In our case, (3.2) becomes

$$\begin{cases} 48 = M_0^2 + 13\bigl(M_1^2 + M_2^2 + M_3^2\bigr), \\ 2M_0M_2 + 6M_1M_3 = B\bigl(M_1^2 - M_3^2\bigr), \\ M_0 + M_1 + M_2 + M_3 \equiv 0 \pmod 4, \\ M_1 \equiv M_2 \equiv M_3 \pmod 2, \\ M_0 \equiv -3 \pmod{13}. \end{cases}$$

From the first equation we obtain $M_0^2 = 9$ and $M_1^2 + M_2^2 + M_3^2 = 3$. Therefore, $M_0 = -3$ and $M_1, M_2, M_3 \in \{\pm 1\}$. Similarly, we also get four solutions $(-3, -1, -1, 1), (-3, 1, -1, -1), (-3, -1, 1, -1), (-3, 1, 1, 1)$. Since each of them satisfies the conditions of Theorem 3.2, we conclude that $\mathrm{Cay}(\mathbb{F}_q, D)$ is also a strongly regular graph.

If $m = 1$, then $N = 13$, $f = 3$, $q = p^f = 27$ and $D = C_0 = \mathbb{F}_3^*$, where $\mathbb{F}_3$ is the prime subfield of $\mathbb{F}_{3^3}$. The strongly regular graph in this case belongs to the so-called *subfield case*, and is rather boring. But for $m \geq 2$, the strongly regular graphs $\mathrm{Cay}(\mathbb{F}_q, D)$ are new and their parameters are

$$v = 3^{3\cdot 13^{m-1}}, \qquad k = \frac{v-1}{13}, \qquad r = \frac{3^{\frac{3\cdot 13^{m-1}+3}{2}} - 1}{13}, \quad \text{and}$$

$$s = \frac{-4 \cdot 3^{\frac{3\cdot 13^{m-1}-1}{2}} - 1}{13}.$$

Acknowledgements Research of G. Ge was supported by the National Outstanding Youth Science Foundation of China under Grant No. 10825103, National Natural Science Foundation of China under Grant No. 61171198, and Specialized Research Fund for the Doctoral Program of Higher Education.

Research of Q. Xiang was supported in part by NSF Grant DMS 1001557, by the Overseas Cooperation Fund (Grant 10928101) of China, and by Y.C. Tang disciplinary development fund, Zhejiang University.

References

1. Batten, L., Dover, J.: Some sets of type (m, n) in cubic order planes. Des. Codes Cryptogr. **16**, 211–213 (1999)
2. Baumert, L.D., Mills, W.H., Ward, R.L.: Uniform cyclotomy. J. Number Theory **14**, 67–82 (1982)
3. Berndt, B.C., Evans, R.J., Williams, K.S.: Gauss and Jacobi Sums. Wiley-Interscience, New York (1998)
4. Brouwer, A.E., Haemers, W.H.: Spectra of Graphs. Universitext. Springer, Berlin (2012)
5. Brouwer, A.E., Wilson, R.M., Xiang, Q.: Cyclotomy and strongly regular graphs. J. Algebr. Comb. **10**, 25–28 (1999)
6. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**(2), 97–122 (1986)
7. van Dam, E., Muzychuk, M.: Some implications on amorphic association schemes. J. Comb. Theory, Ser. A **117**, 111–127 (2010)
8. Feng, T., Xiang, Q.: Strongly regular graphs from unions of cyclotomic classes. J. Comb. Theory (B) (in press). doi:10.1016/j.jctb.2011.10.006
9. Feng, K., Yang, J., Luo, S.: Gauss sum of index 4:(1) cyclic case. Acta Math. Sin. Engl. Ser. **21**(6), 1425–1434 (2005)

10. Godsil, C., Royle, G.: Algebraic Graph Theory. GTM, vol. 207. Springer, Berlin (2001)
11. Ikuta, T., Munemasa, A.: Pseudocyclic association schemes and strongly regular graphs. Eur. J. Comb. **31**, 1513–1519 (2010)
12. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory, 2nd edn. Graduate Text in Math., vol. 84. Springer, Berlin (2003)
13. Langevin, P.: A new class of two-weight codes. In: Cohen, S., Niederreiter, H. (eds.) Finite Fields and Applications, Glasgow, 1995. London Math. Soc. Lecture Note Series, vol. 233, pp. 181–187. Cambridge University Press, Cambridge (1996)
14. de Lange, C.L.M.: Some new cyclotomic strongly regular graphs. J. Algebr. Comb. **4**, 329–330 (1995)
15. van Lint, J.H., Schrijver, A.: Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields. Combinatorica **1**, 63–73 (1981)
16. Ma, S.L.: A survey of partial difference sets. Des. Codes Cryptogr. **4**, 221–261 (1994)
17. McEliece, R.J.: Irreducible cyclic codes and gauss sums. In: Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of Designs, Finite Geometry and Coding Theory. Math. Centre Tracts, vol. 55, pp. 179–196. Math. Centrum, Amsterdam (1974)
18. Schmidt, B., White, C.: All two-weight irreducible cyclic codes. Finite Fields Appl. **8**, 1–17 (2002)
19. Stickelberger, L.: Über eine verallgemeinerung der kreistheilung. Math. Ann. **37**, 321–367 (1890)