CYCLOTOMY, GAUSS SUMS, DIFFERENCE SETS AND STRONGLY REGULAR CAYLEY GRAPHS

QING XIANG[1]

ABSTRACT. We survey recent results on constructions of difference sets and strongly regular Cayley graphs by using union of cyclotomic classes of finite fields. Several open problems are raised.

1. INTRODUCTION

We start by reviewing the relationship between binary sequences with two-level autocorrelations and cyclic difference sets. Let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ be a binary sequence with $a_j = \pm 1$ for all j. We define the (periodic) *autocorrelation function* of $\mathbf{a}$ by

$$\mathcal{A}_{\mathbf{a}}(\tau) = \sum_{j=0}^{v-1} a_j a_{j+\tau}, \ \forall \tau,$$

where the subscripts $j + \tau$ are taken modulo v. A binary sequence $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ is said to have *two-level autocorrelations* if

$$\mathcal{A}_{\mathbf{a}}(\tau) = \begin{cases} v, & \text{if } \tau \equiv 0 \pmod{v}, \\ \gamma, & \text{otherwise.} \end{cases}$$

Binary sequences with two-level autocorrelations have found many applications in radar, sonar, and synchronization. Golomb may have been the first to point out that such sequences are equivalent to cyclic (v, k, λ) difference sets. We now give the definition of difference sets in a (not necessarily cyclic) group of order v. Let G be a finite multiplicative group of order v. A k-element subset D of G is called a (v, k, λ) *difference set* in G if the list of "differences" $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, represents each nonidentity element in G exactly λ times. A moment's reflection shows that the translates of D by all group elements form the blocks of a (v, k, λ) symmetric design, and G is a regular automorphism group of the design. For this reason difference sets play an important role in combinatorial design theory.

Given a subset D in the cyclic group $(\mathbb{Z}/v\mathbb{Z}, +)$, we define its *characteristic sequence* $\mathbf{a} = (a_i)_{0 \leq i \leq v-1}$ by setting $a_i = 1$ if $i \in D$, and $a_i = -1$ otherwise. From the definition of difference set, we see that D is a (v, k, λ) difference set in $\mathbb{Z}/v\mathbb{Z}$ if and only if

$$\mathcal{A}_{\mathbf{a}}(\tau) = \begin{cases} v, & \text{if } \tau \equiv 0 \pmod{v}, \\ \gamma := v - 4(k - \lambda), & \text{otherwise.} \end{cases}$$

This shows the equivalence of binary sequences with two-level autocorrelations and cyclic (v, k, λ) difference sets. More generally, (v, k, λ) abelian difference sets are equivalent to binary arrays with two-level autocorrelations. For background material on difference sets, we refer the reader to the books [1], [23] and Chapter 6 of [5]. Several survey papers on difference sets have also appeared during the past two decades. See [20], [21, 22], [28], and [42, 43]. In this paper we

Key words and phrases. Cyclotomy, difference set, Gauss sum, strongly regular graph.

[1]Research supported in part by NSF Grant DMS 1001557.

will focus on recent constructions of difference sets and strongly regular Cayley graphs by using cyclotomic classes of finite fields.

2. Cyclotomy and Gauss Sums

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 N^{th} *cyclotomic classes* $C_0, C_1, \ldots, C_{N-1}$ of $\mathbb{F}_q$ by

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

where $0 \le i \le N-1$. That is, C_0 is the subgroup of $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ consisting of all nonzero N^{th} powers in $\mathbb{F}_q$, and $C_i = \gamma^i C_0$, $1 \le i \le N-1$. Important in the study of cyclotomic (or power residue) difference sets are the cyclotomic numbers. For integers a, b with $0 \le a, b < N$, the cyclotomic number (a, b) is defined by

$$(a, b) = |(C_a + 1) \cap C_b|.$$

In terms of these cyclotomic numbers, Lehmer [27] gave necessary and sufficient conditions for C_0 to be a difference set in $(\mathbb{F}_q, +)$.

Theorem 2.1. *Let C_0 be defined as above. Then C_0 is a difference set in $(\mathbb{F}_q, +)$ if and only if N is even, $(q-1)/N$ is odd, and*

$$(a, 0) = \frac{(q-1-N)}{N^2}$$

for $a = 0, 1, 2, \ldots, \frac{N}{2} - 1$.

Theorem 2.1 has been used to construct difference sets for small values of N. When N is large, Lehmer's theorem is not very useful since the cyclotomic numbers involved are difficult to compute. Cyclotomic numbers can be determined from the knowledge of Jacobi sums or Gauss sums (cf. [4, p. 79]). Therefore it is possible to use Gauss sums to construct and study difference sets directly. We give the definition of Gauss sums below.

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

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

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

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

If χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, then it is easy to see that $g(\chi_0) = -1$. We are usually concerned with nontrivial Gauss sums $g(\chi)$, i.e., those with $\chi \ne \chi_0$.

While it is easy to show that the absolute value of a nontrivial Gauss sum $g(\chi)$ is equal to $\sqrt{q}$, the explicit determination of Gauss sums is a difficult problem. However, there are a few cases where the Gauss sums $g(\chi)$ can be explicitly evaluated. The simplest case is the so-called *semi-primitive case*, where there exists an integer j such that $p^j \equiv -1 \pmod{N}$ and N is the order of χ in $\widehat{\mathbb{F}}_q^*$ (the group of multiplicative characters of $\mathbb{F}_q$). Some authors [3, 4] also refer to this case as uniform cyclotomy, or pure Gauss sums. We state the following theorem concerning the semi-primitive case.

Theorem 2.2. ([4, p. 364]) *Let p be a prime, and $N > 2$ be an integer. Suppose that there is a positive integer t such that $p^t \equiv -1 \pmod N$, with t chosen minimal. Let χ be a character of order N of $\mathbb{F}_{p^r}^*$ for some positive integer r. Then $r = 2ts$ for some positive integer s, and*

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

The next interesting case is the index 2 case, where $-1 \notin \langle p \rangle$, the cyclic subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ generated by p (the characteristic of the finite field $\mathbb{F}_q$), and $\langle p \rangle$ has index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$ (again here N is the order of χ in $\widehat{\mathbb{F}}_q^*$). Many authors have studied this case, including McEliece [32], Langevin [25], Mbodj [31], Meijer and Van der Vlugt [33], and Yang and Xia [45]. In particular, combined with previous work, a complete solution to the problem of evaluating Gauss sums in the index 2 case was recently given in [45]. We state here a couple of sample results in the index 2 case. Below we use $\phi(N)$ to denote the number of integers k with $1 \le k \le N$ such that $\gcd(k, N) = 1$, and $\mathrm{ord}_N(p)$ to denote the order of p modulo N, which is the smallest positive integer f such that $p^f \equiv 1 \pmod N$.

Theorem 2.3. ([25]) *Let $N = p_1^m$, where m is a positive integer, 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) $bp^{h_0} \equiv -2 \pmod{p_1}$.

Theorem 2.4. ([45], Case D; Theorem 4.12) *Let $N = 2p_1^m$, where $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$ and m is a positive integer. Assume that p is a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2$. Let $f = \phi(N)/2$, $q = p^f$, and χ be a multiplicative character of order N of $\mathbb{F}_q$. Then, for $0 \le t \le m-1$, we have*

$$\begin{aligned} g(\chi^{p_1^t}) &= \begin{cases} (-1)^{\frac{p-1}{2}(m-1)} p^{\frac{f-1}{2} - hp_1^t} \sqrt{p^*} \left(\frac{b + c\sqrt{-p_1}}{2} \right)^{2p_1^t}, & \text{if } p_1 \equiv 3 \pmod 8, \\ (-1)^{\frac{p-1}{2} m} p^{\frac{f-1}{2}} \sqrt{p^*}, & \text{if } p_1 \equiv 7 \pmod 8; \end{cases} \\ g(\chi^{2p_1^t}) &= p^{\frac{f - p_1^t h}{2}} \left(\frac{b + c\sqrt{-p_1}}{2} \right)^{p_1^t}; \\ g(\chi^{p_1^m}) &= (-1)^{\frac{p-1}{2}\frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{p^*}, \end{aligned}$$

where $p^* = (-1)^{\frac{p-1}{2}} p$, h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and b and c are integers determined by $4p^h = b^2 + p_1 c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

Note that Theorem 2.4 above is Theorem 4.12 in [45], whose statement contains several misprints. We corrected those misprints in the above statement. Recently, in a series of papers [11], [12], [14], [13], we used index 2 Gauss sums to construct difference sets, strongly regular Cayley graphs and pseudocyclic (but non-amorphic) association schemes. These constructions will be discussed in the next two sections.

We also mention that index 4 Gauss sums were studied in [15], [44] though the problem of evaluating Gauss sums in the index 4 case is not completely solved.

3. Difference sets from unions of cyclotomic classes

The idea of constructing difference sets from cyclotomic classes of finite fields goes back to Paley [36]. In the mid-20th century, Baumert, Chowla, Hall, Lehmer, Storer, Whiteman, Yamamoto, etc. pursued this line of research vigorously. The book by Storer [38] contains a summary of results in this direction up to 1967. See also Chapter 5 of the book by Baumert [1] for a summary. This method for constructing difference sets, however, has had only very limited success.

Let $q = p^f$ be a prime power, and let $N > 1$ be a divisor of $q-1$. Let γ be a fixed primitive element of $\mathbb{F}_q$ and $C_i = \{\gamma^{jN+i} \mid 0 \le j \le \frac{q-1}{N} - 1\}$, $0 \le i \le N-1$, be the N^{th} cyclotomic classes of $\mathbb{F}_q$. It is known (cf. [5, p. 123–124]) that a single cyclotomic class, say C_0, can form a difference set in $(\mathbb{F}_q, +)$ if $N = 2, 4$, or 8 and q satisfies certain conditions. It should be noted that in order to obtain difference sets this way, the conditions on q are quite restrictive when $N = 4$ or 8. It is conjectured that the converse is also true.

Conjecture 3.1. *Let q be a prime power, and let $N > 1$ be a divisor of $q-1$. Let C_0 be the subgroup of $\mathbb{F}_q^*$ consisting of all nonzero N^{th} powers of $\mathbb{F}_q$. If C_0 is a difference set in $(\mathbb{F}_q, +)$, then N is necessarily $2, 4$, or 8.*

This conjecture remains open though it has been verified (cf. [10]) up to $N = 20$. If one uses a union of cyclotomic classes, instead of just one single class, for the purpose of constructing difference sets, the only new family of difference sets found in this way is Hall's sextic difference sets [18] in $(\mathbb{F}_q, +)$ formed by taking a union of three cyclotomic classes of order 6, where $q = 4x^2 + 27$ is a prime power congruent to 1 modulo 6. One of the reasons that very few difference sets have been discovered by using union of cyclotomic classes is that the investigations often relied on cyclotomic numbers and these numbers are in general very difficult to compute if N is large.

It is therefore a great surprise that more than fifty years after the construction of Hall's sextic difference sets, Feng and this author [11] constructed a class of Hadamard difference sets in $(\mathbb{F}_q, +)$ by using a union of cyclotomic classes of order $N = 2p_1^m$, where p_1 is a prime. We give the detailed statement below. (A difference set D in an additively written finite group G is called *skew Hadamard* if G is the disjoint union of D, $-D$, and $\{0\}$.)

Theorem 3.2. *Let $p_1 \equiv 7 \pmod 8$ be a prime, $N = 2p_1^m$, and let p be a prime such that $f := \text{ord}_N(p) = \phi(N)/2$. Let s be an odd integer, I any subset of $\mathbb{Z}/N\mathbb{Z}$ such that $\{i \pmod{p_1^m} \mid i \in I\} = \mathbb{Z}/p_1^m\mathbb{Z}$, and let*

$$D = \bigcup_{i \in I} C_i \subseteq \mathbb{F}_{p^{fs}}^*.$$

Then D is a skew Hadamard difference set if $p \equiv 3 \pmod 4$.

Several remarks are in order. First we comment that the difference sets from Theorem 3.2 are not cyclic since the f satisfying the conditions of theorem is greater than 1. Secondly, it should be noted that there is a great deal of flexibility in choosing the index set I in Theorem 3.2. Namely, there are $2^{p_1^m}$ choices of the index set I since each pair $\{i, i + p_1^m\}$, $0 \le i \le p_1^m - 1$, contributes exactly one element to I. This flexibility has interesting implications in terms of association schemes [35]. Thirdly, as we have seen above, Theorem 3.2 produces $2^{p_1^m}$ skew Hadamard difference sets in $(\mathbb{F}_q, +)$, where $q = p^{fs}$. Sorting out inequivalent ones from these difference sets seems to be a very difficult problem.

The case where p_1 is a prime congruent to 3 modulo 8 and $N = 2p_1^m$ is more complicated. Feng and this author [11] first gave a construction of skew Hadamrd difference sets in the case where $N = 2p_1$, $p_1 \equiv 3 \pmod 8$ is a prime. Later on, this construction was generalized by Feng, Momihara and this author [14] to work in the case where $N = 2p_1^m$, $p_1 \equiv 3 \pmod 8$ is a prime. Below we state the construction from [14].

Theorem 3.3. *Let $p_1 \equiv 3 \pmod 8$ be a prime, $p_1 \neq 3$, $N = 2p_1^m$, and let $p \equiv 3 \pmod 4$ be a prime such that $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, $J = \langle p\rangle \cup 2\langle p\rangle \cup \{0\} \pmod{2p_1}$, and define*

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j\in J} C_{2i+p_1^{m-1}j}.$$

Assume that $1+p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then D is a skew Hadamard difference set in the additive group of $\mathbb{F}_q$.

Note that in Theorem 3.3, we need to choose a suitable primitive element γ of $\mathbb{F}_q$ in order for the construction to work. We refer the reader to [14] for details on how to choose such a primitive element of $\mathbb{F}_q$.

The difference sets constructed in both Theorem 3.2 and Theorem 3.3 are skew Hadamard. Such difference sets are currently under intensive study. We refer the reader to [11] for a short summary of recent results on skew Hadamard difference sets.

4. Strongly regular graphs from unions of cyclotomic classes

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.

Let $q = 4t + 1$ be a prime power. The *Paley graph* $\mathrm{P}(q)$ 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 $\mathrm{P}(q)$ is an $\mathrm{srg}(4t+1, 2t, t-1, t)$. For a survey on strongly regular graphs, we refer the reader to [6], [17] and [9]. Strongly regular graphs are closely related to two-weight codes, two-intersection sets in finite geometry, and partial difference sets. For these connections, we refer the reader to [8, 30].

One of the most effective methods for constructing strongly regular graphs is by the Cayley graph construction. For example, the Paley graph $\mathrm{P}(q)$ and the Clebsch graph are both Cayley graphs (moreover they are cyclotomic). Let G be an additively written group of order v, and let D be a subset of G such that $0 \notin D$ and $-D = D$, where $-D = \{-d \mid d \in D\}$. The *Cayley graph on G with connection set D*, denoted $\mathrm{Cay}(G, D)$, is the graph with the elements of G as vertices; two vertices are adjacent if and only if their difference belongs to D. In the case when $\mathrm{Cay}(G, D)$ is a strongly regular graph, the connection set D is called a (regular) *partial difference set*. The survey of Ma [30] contains much of what is known about partial difference sets.

Next we consider the so-called cyclotomic srg. Let $q = p^f$ be a prime power, $N > 1$ be a divisor of $q - 1$, and let D be the subgroup of $\mathbb{F}_q^*$ of index N. If $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular, then we speak of a *cyclotomic strongly regular graph*. Cyclotomic srg have been extensively studied by many authors; see [32, 29, 7, 25, 37, 19]. Some of these authors used the language of cyclic codes in their investigations. Here we use the language of srg. Let D be the 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 $\mathrm{Cay}(\mathbb{F}_{p^f}, D)$ 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 $\mathrm{Cay}(\mathbb{F}_{p^f}, D)$ is an srg by Theorem 2.2. These examples are usually called *semi-primitive* cyclotomic srg. The following conjecture of Schmidt and White [37] says that besides the two classes of cyclotomic srg mentioned above, there are only 11 sporadic examples of cyclotomic srg.

Conjecture 4.1. (Conjecture 4.4, [37]) *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 $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ 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 $p^t \equiv -1 \pmod N$,

(3) (exceptional case) $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ is one of the eleven "sporadic" examples appearing in the following table.

N	p	f	$[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle]$
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

Table I

This conjecture can be thought as the counterpart of Conjecture 3.1 in the context of cyclotomic srg. It remains largely open. Also this conjecture is closely related to cyclic difference sets which are "subdifference sets" of the Singer difference sets. For details, see [37].

In order to construct more srg by using cyclotomic classes of finite fields, one is natually led to consider strongly regular Cayley graphs over finite fields with connection sets being unions of cyclotomic classes (instead of a single cyclotomic class). Some sporadic examples of such srg had been found by computer search. For example, the following are known:

(i) (De Lange [24]) Let $q = 2^{12}$ and $N = 45$. Then, $\mathrm{Cay}(\mathbb{F}_q, C_0 \cup C_5 \cup C_{10})$ is a strongly regular graph.
(ii) (Ikuta and Munemasa [19]) Let $q = 2^{20}$ and $N = 75$. Then, $\mathrm{Cay}(\mathbb{F}_q, C_0 \cup C_3 \cup C_6 \cup C_9 \cup C_{12})$ is a strongly regular graph.
(iii) (Ikuta and Munemasa [19]) Let $q = 2^{21}$ and $N = 49$. Then, $\mathrm{Cay}(\mathbb{F}_q, C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6)$ is a strongly regular graph.

Recently Feng and this author [12] extended the above examples to infinite families by using index 2 Gauss sums over $\mathbb{F}_q$. Below is the main theorem from [12].

Theorem 4.2. (i) *Let $p_1 \equiv 3 \pmod 4$ be a prime, $p_1 \neq 3$, $N = p_1^m$, and let p be a prime such that $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and*

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i \subset \mathbb{F}_q^*.$$

Assume that $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph.

(ii) *Let p_1 and p_2 be primes such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $N = p_1^m p_2$, and let p be a prime such that $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2}(p) = \phi(p_2)$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and*

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} C_{ip_2} \subset \mathbb{F}_q^*.$$

Assume that $p_1 = 2p^{h/2} + (-1)^{\frac{p_1-1}{2}} b$, $p_2 = 2p^{h/2} - (-1)^{\frac{p_1-1}{2}} b$, h is even, and $1 + p_1 p_2 = 4p^h$, where $b \in \{1, -1\}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1 p_2})$. Then $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph.

For explicit families of strongly regular Cayley graphs arising from Theorem 4.2 we refer the reader to [12]. Very recently, Feng, Momihara and this author [14] could generalize the construction of strongly regular Cayley graphs in Theorem 4.2 (ii) to the case where $N = p_1^m p_2^n$.

Theorem 4.3. *Let p_1 and p_2 be primes such that $p_1 \equiv 1 \pmod 4$ and $p_2 \equiv 3 \pmod 4$, $N = p_1^m p_2^n$, where m, n are positive integers. Let p be a prime such that $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and*

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j=0}^{p_2^{n-1}-1} C_{p_2^n i + p_1^m j} \subset \mathbb{F}_q^*.$$

Assume that $p_1 = 2p^{h/2} + b$, $p_2 = 2p^{h/2} - b$, h is even, and $1 + p_1 p_2 = 4p^h$, where $b \in \{1, -1\}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1 p_2})$. Then $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph.

Applying Theore 4.3 we obtain three infinite families of strongly regular graphs, whose parameters are listed in the following table.

TABLE 1. The parameters λ and μ of the srg can be computed by $\lambda = s + r + sr + k$ and $\mu = k + sr$. The parameters r and s are the two nontrivial eigenvalues of the srg.

No.	p	N	h	b	v	k	r, s
1	2	$3^m \cdot 5^n$	2	1	$2^{4 \cdot 3^{m-1} \cdot 5^{n-1}}$	$\frac{2^{4 \cdot 3^{m-1} \cdot 5^{n-1}} - 1}{15}$	$r = \frac{8 \cdot 2^{2 \cdot 3^{m-1} \cdot 5^{n-1}} - 1 - 1}{15}$ $s = \frac{-7 \cdot 2^{2 \cdot 3^{m-1} \cdot 5^{n-1}} - 1 - 1}{15}$
2	3	$5^m \cdot 7^n$	2	-1	$3^{12 \cdot 5^{m-1} \cdot 7^{n-1}}$	$\frac{3^{12 \cdot 5^{m-1} \cdot 7^{n-1}} - 1}{35}$	$r = \frac{17 \cdot 3^{6 \cdot 5^{m-1} \cdot 7^{n-1}} - 1 - 1}{35}$ $s = \frac{-18 \cdot 3^{6 \cdot 5^{m-1} \cdot 7^{n-1}} - 1 - 1}{35}$
3	3	$17^m \cdot 19^n$	4	-1	$3^{144 \cdot 17^{m-1} \cdot 19^{n-1}}$	$\frac{3^{144 \cdot 17^{m-1} \cdot 19^{n-1}} - 1}{323}$	$r = \frac{161 \cdot 3^{72 \cdot 17^{m-1} \cdot 19^{n-1}} - 2 - 1}{323}$ $s = \frac{-162 \cdot 3^{72 \cdot 17^{m-1} \cdot 19^{n-1}} - 2 - 1}{323}$

Both Theorem 4.2 and 4.3 make use of index 2 Gauss sums. Recently we [16] also used index 4 Gauss sums to construct strongly regular Cayley graphs. Two infinite families of srg were found in this way. Below r and s denote the nontrivial eigenvalues of the strongly regular graphs.

Example 4.4. (i) *Let $p_1 = 37,\ p = 7,\ N = p_1^m$ where $m \geq 1$ is any integer. We have $\mathrm{ord}_{37^m}(7) = \frac{\phi(37^m)}{4}$. Let $f = \frac{\phi(37^m)}{4}$ and $q = 7^f$. Let γ be a fixed primitive element of $\mathbb{F}_q$. Let $C_0 = \langle \gamma^N \rangle, C_1 = \gamma C_0, \ldots, C_{N-1} = \gamma^{N-1} C_0$ be the N^{th} cyclotomic classes of $\mathbb{F}_q$ and*

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

Then the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular, with parameters

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

(ii) *Let $p_1 = 13,\ p = 3,\ N = p_1^m$, where $m \geq 1$ is an integer. We have $\mathrm{ord}_{13^m}(3) = \frac{\phi(13^m)}{4}$. Let $f = \frac{\phi(13^m)}{4}$ and $q = 3^f$. Let γ be a fixed primitive element of $\mathbb{F}_q$. Let $C_0 = \langle \gamma^N \rangle, C_1 = \gamma C_0, \ldots, C_{N-1} = \gamma^{N-1} C_0$ be the N^{th} cyclotomic classes of $\mathbb{F}_q$ and*

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

Then the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular, with parameters

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

So far we have succeeded in generalizing 8 of the 11 sporadic examples in Table I (in the statement of Conjecture 4.1) into infinite families. When we first submitted the current paper in Jan. 2012, we remarked that it should be possible to use index 6 Gauss sums to construct strongly regular Cayley graphs also. This and much more have been done in two recent preprints [34] and [41]. The constructions in [34] are recursive, and they are more general than that in [41], while the construction in [41] is direct, and leads to an interesting connection between srg and cyclic difference sets in $(\mathbb{Z}/p_1\mathbb{Z}, +)$.

5. Open problems

In this section, we raise a few open problems on cyclotomic constructions of difference sets and strongly regular Cayley graphs. Of course the most obvious problems are to settle Conjecture 3.1 and 4.1. It is known [39, 40] that the truth of Conjecture 3.1 implies that the only flag-transitive finite projective planes are the Desarguesian ones. Therefore the solution of Conjecture 3.1 will lead to the solution of an old problem in finite geometry. On the constructive side, we raise the following questions.

Problem 5.1. *Is it possible to generalize Hall's construction of sextic difference sets in the case where $N = 2 \cdot 3^m$, for some $m > 1$.*

Problem 5.2. *In the two-page paper* [24]*, De Lange constructed four strongly regular Cayley graphs by using union of cyclotomic classes of finite fields. Now all but one example have been explained and generalized into infinite families. See* [7, 12]*. Find a generalization of De Lange's last example (Example (b) of* [24]*).*

Problem 5.3. *In* [2]*, Baumert and Fredricksen showed how to construct all* 6 *inequivalent* $(127, 63, 31)$ *cyclic difference sets by taking unions of* 18^{th} *cyclotomic classes of the finite field* $\mathbb{Z}/127\mathbb{Z}$*. Can this cyclotomic construction be generalized to obtain more cyclic difference sets with Singer parameters?*

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics 182, Springer-Verlag, 1971.

[2] L. D. Baumert, H. Fredricksen, The cyclotomic numbers of order eighteen with applications to difference sets, *Math. Comp.* **21** (1967), 204–219.

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

[4] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, A Wiley-Interscience Publication, 1998.

[5] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*. Vol. I. Second edition. Encyclopedia of Mathematics and its Applications, 78. Cambridge University Press, Cambridge, 1999.

[6] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, Springer Universitext, 2012.

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

[8] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc* **18** (1986), 97–122.

[9] P. Cameron, Strongly regular graphs, in Topics in Algebraic Graph Theory (eds. L. W. Beineke and R. J. Wilson), Cambridge Univ. Press, Cambridge, 2004, 203-221.

[10] R. J. Evans, Nonexistence of twentieth power residue difference sets, *Acta Arith.* **84** (1999), 397-402.

[11] T. Feng, Q. Xiang, Cyclotomic constructions of skew Hadamard difference sets, *J. Combin. Theory* (A) **119** (2012), 245–256.

[12] T. Feng, Q. Xiang, Strongly regular graphs from unions of cyclotomic classes, *J. Combin. Theory* (B), in press.

[13] T. Feng, F. Wu, Q. Xiang, Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes, *Des. Codes and Cryptogr.*, in press.

[14] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, *submitted*, `arXiv:1201.0701`.

[15] K. Q. Feng, J. Yang, and S. X. Luo, Gauss sum of index 4: (1) cyclic case, *Acta Math. Sin.* (Engl. Ser.) **21** (2005), 1425–1434.

[16] G. Ge, Q. Xiang and T. Yuan, Constructions of strongly regular Cayley graphs using index four Gauss sums, *submitted*, `arXiv:1201.0702`.

[17] C. Godsil, G. Royle, *Algebraic Graph Theory*, GTM 207, Springer-Verlag, 2001.

[18] M. Hall, Jr., A survey of difference sets, *Proc. Amer. Math. Soc.* **7** (1956), 975–986.

[19] T. Ikuta, A. Munemasa, Pseudocyclic association schemes and strongly regular graphs, *European J. Combin.* **31** (2010), 1513–1519.

[20] D. Jungnickel, Difference sets, Contemporary design theory, 241–324, Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1992.

[21] D. Jungnickel, B. Schmidt, Difference sets: an update, Geometry, combinatorial designs and related structures (Spetses, 1996), 89–112, London Math. Soc. Lecture Note Ser., 245, Cambridge Univ. Press, Cambridge, 1997.

[22] D. Jungnickel, B. Schmidt, Difference sets: a second update, Combinatorics '98 (Mondello). Rend. Circ. Mat. Palermo (2) Suppl. No. 53 (1998), 89–118.

[23] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Society Lecture Note Series **74**, Cambridge University Press, 1983.

[24] C. L. M. de Lange, Some new cyclotomic strongly regular graphs, *J. Alg. Combin.* **4** (1995), 329–330.

[25] P. Langevin, Calculs de certaines sommes de Gauss, *J. Number Theory* **63** (1997), 59–64.

[26] P. Langevin, A new class of two-weight codes, in *Finite Fields and Applications* (Glasgow 1995), London Math. Soc. Lecture Note Series, No. 233, S. Cohen and H. Niederreiter, eds. Cambridge University Press, 1996, pp. 181–187.

[27] E. Lehmer, On residue difference sets, *Can. J. Math.* **5** (1953), 425–432.

[28] R. A. Liebler, Constructive representation theoretic methods and non-abelian difference sets, Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), 331–352, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, Kluwer Acad. Publ., Dordrecht, 1999.

[29] J. H. van Lint, A. Schrijver, Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica* **1** (1981), 63–73.

[30] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.

[31] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields and Appl.* **4** (1998), 347–361.
[32] R. J. McEliece, Irreducible cyclic codes and Gauss sums. Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory, in: Math. Centre Tracts, vol. 55, Math. Centrum, Amsterdam, 1974, pp.179–196.
[33] P. Meijer, M. van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, *J Number Theory* **100** (2003), 381–395.
[34] K. Momihara, Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, `arXiv:1202.6414`.
[35] M. Muzychuk, On T-amorphous association schemes, *preprint*.
[36] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.
[37] B. Schmidt, C. White, All two-weight irreducible cyclic codes, *Finite Fields Appl.* **8** (2002), 1–17.
[38] T. Storer, *Cyclotomy and difference sets*, Markham, Chicago, 1967.
[39] K. Thas, Finite flag-transitive projective planes: a survey and some remarks, *Discrete Math.* **266** (2003), 417429.
[40] K. Thas, D. Zagier, Finite projective planes, Fermat curves, and Gaussian periods, *J. Eur. Math. Soc. (JEMS)* **10** (2008), 173190.
[41] F. Wu, Constructions of strongly regular Cayley graphs using even index Gauss sums, preprint.
[42] Q. Xiang, Recent results on difference sets with classical parameters, Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), 419–437, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, Kluwer Acad. Publ., Dordrecht, 1999.
[43] Q. Xiang, Recent progress in algebraic design theory, *Finite Fields Appl.* (Ten Year Anniversary Edition) **11** (2005), 622–653.
[44] J. Yang, S. X. Luo, K. Q. Feng, Gauss sum of index 4: (2) Non-cyclic case. *Acta Math. Sin.* (Engl. Ser.) **22** (2006), 833844.
[45] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A* **53** (2010), 2525–2542.

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA, email: `xiang@math.udel.edu`