Strongly Regular Cayley Graphs, Skew Hadamard Difference Sets, and Rationality of Relative Gauss Sums

Koji Momihara*

Abstract

In this paper, we give constructions of strongly regular Cayley graphs and skew Hadamard difference sets. Both constructions are based on choosing cyclotomic classes in finite fields, and our results generalize ten of the eleven sporadic examples of cyclotomic strongly regular graphs given by Schmidt and White [24] and several of subfield examples into infinite families. These infinite families of strongly regular graphs have new parameters. The main tools that we employed are relative Gauss sums instead of explicit evaluations of Gauss sums.

Keywords: strongly regular graph; skew Hadamard difference set; relative Gauss sum

1 Introduction

In this paper, we will assume that the reader is familiar with the theory of strongly regular graphs and difference sets. For the theory of strongly regular graphs (srgs), our main reference is the lecture note of Brouwer and Haemers [5]. For difference sets, we refer the reader to Chapter 6 of [4]. We remark that strongly regular graphs are closely related to other combinatorial objects, such as two-weight codes, two-intersection sets in finite geometry, and partial difference sets. For these connections, we refer the reader to [5, p. 132], [7, 20].

Let Γ be a simple and undirected graph and A be its adjacency matrix. A useful way to check whether a graph is strongly regular is by using the eigenvalues of its adjacency matrix. For convenience we call an eigenvalue *restricted* if it has an eigenvector perpendicular to the all-ones vector $\mathbf{1}$. (For a k-regular connected graph, the restricted eigenvalues are the eigenvalues different from k.)

Theorem 1.1. *For a simple graph Γ of order v, not complete or edgeless, with adjacency matrix A, the following are equivalent:*

1. *Γ is strongly regular with parameters (v, k, λ, μ) for certain integers k, λ, μ,*
2. *$A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$ for certain real numbers k, λ, μ, where I, J are the identity matrix and the all-ones matrix, respectively,*
3. *A has precisely two distinct restricted eigenvalues.*

One of the most effective methods for constructing srgs is by the Cayley graph construction. For example, the Paley graph $\mathrm{P}(q)$ is one class of well known Cayley graphs, that is, the graph with the finite field $\mathbb{F}_q$ as vertex set, where two vertices are adjacent when their difference is a

[1]Department of Mathematics, Faculty of Education, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan; Email address: momihara@educ.kumamoto-u.ac.jp

nonzero quadratic. It has the parameters $(v, k, \lambda, \mu) = (4t+1, 2t, t-1, t)$. In general, 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 strongly regular, the connection set D is called a (regular) *partial difference set*. The survey of Ma [20] contains much of what is known about partial difference sets and about connections with strongly regular Cayley graphs.

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 $\{0\}$. The primary example (and for many years, the only known example in abelian groups) of skew Hadamard difference sets is the classical Paley difference set in $(\mathbb{F}_q, +)$ consisting of the nonzero squares of $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of order q, a prime power congruent to 3 modulo 4. Skew Hadamard difference sets are currently under intensive study; see the introduction of [10] for a short survey of known constructions of skew Hadamard difference sets and related problems. As we see in the next section, in order to check that a candidate subset D of $\mathbb{F}_q$ is a partial difference set or a skew Hadamard difference set in $(\mathbb{F}_q, +)$, it is sufficient to compute certain character sums of $\mathbb{F}_q$ in common.

A classical method for constructing both connection sets of strongly regular graphs (i.e., partial difference sets) and difference sets in the additive groups of finite fields is to use cyclotomic classes of finite fields. Let p be a prime, f a positive integer, and let $q = p^f$. Let $k > 1$ be an integer such that $k|(q-1)$, and γ be a primitive element of $\mathbb{F}_q$. Then the cosets $C_i^{(k,q)} = \gamma^i \langle \gamma^k \rangle$, $0 \le i \le k-1$, are called the *cyclotomic classes of order k* of $\mathbb{F}_q$. Many authors have studied the problem of determining when a union D of some cyclotomic classes forms a (partial) difference set. Especially, when D consists of only a subgroup of $\mathbb{F}_q$, many authors have studied extensively [1, 2, 6, 9, 10, 11, 13, 14, 17, 19, 22, 24, 25]. (Some of these authors used the language of cyclic codes in their investigations instead of strongly regular Cayley graphs or partial difference sets. We choose to use the language of srg.) We call a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ *cyclotomic* if D is such. The Paley graphs are primary examples of cyclotomic srgs. Also, if D is the multiplicative group of a subfield of $\mathbb{F}_q$, then it is clear that $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular. These cyclotomic srgs are usually called *subfield examples*. Next, if there exists a positive integer t such that $p^t \equiv -1 \pmod{k}$, then $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular. This case had already generalized so that D is a union of some cyclotomic cosets based on the computation of "pure Gauss sums", see [6, 19]. These examples are usually called *semi-primitive*. Schmidt and White presented the following conjecture on cyclotomic srgs.

Conjecture 1.2. *([24]) Let $\mathbb{F}_{p^f}$ be the finite field, $k \mid \frac{p^f-1}{p-1}$ with $k > 1$, and $C_0 := C_0^{(k,p^f)}$ with $-C_0 = C_0$. If $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ is strongly regular, then one of the following holds:*

(1) (subfield case) $C_0 = \mathbb{F}_{p^d}^*$ where $d \mid f$,

(2) (semi-primitive case) $-1 \in \langle p \rangle \le (\mathbb{Z}/k\mathbb{Z})^*$,

(3) (exceptional case) $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ has one of the parameters given in Table 1.

Recently, the authors of [10, 11, 13] succeeded to generalize the examples of Table 1 except for srgs of No. 1, 5, and 8 into infinite families using "index 2 and 4 Gauss sums".

Theorem 1.3. *(i) ([9]) Let $q = p^{p_1^{m-1}(p_1-1)/2}$, $k = p_1^m$, and $D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i^{(k,q)}$. Then, $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular for any m in the following cases:*

$$(p, p_1) = (2, 7), (3, 107), (5, 19), (5, 499), (17, 67), (41, 163).$$

(ii) ([13]) Let $q = p^{p_1^{m-1}(p_1-1)/4}$, $k = p_1^m$, and $D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i^{(k,q)}$. Then, $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular for any m in the following cases:

$$(p, p_1) = (3, 13), (7, 37).$$

Table 1: Eleven sporadic examples

No.	k	p	f	$e := [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$
1	11	3	5	2
2	19	5	9	2
3	35	3	12	2
4	37	7	9	4
5	43	11	7	6
6	67	17	33	2
7	107	3	53	2
8	133	5	18	6
9	163	41	81	2
10	323	3	144	2
11	499	5	249	2

(iii) ([11]) Let $q = p^{p_1^{m-1}(p_1-1)p_2^{n-1}(p_2-1)/2}$, $k = p_1^m p_2^n$, *and* $D = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j=0}^{p_2^{n-1}-1} C^{(k,q)}_{p_2^n i + p_1^m j}$. *Then,* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is strongly regular for any* n *and* m *in the following cases:*

$$(p, p_1, p_2) = (2, 3, 5), (3, 5, 7), (3, 17, 19).$$

The srgs in the cases when $(p, p_1) = (2, 7)$ of (i), $(p, p_1) = (3, 13)$ of (ii), and $(p, p_1, p_2) = (2, 3, 5)$ of (iii) of Theorem 1.3 are generalizations of subfield examples. The others are generalizations of sporadic examples of Table 1. Note that it is impossible to generalize the example of No. 1 of Table 1 by a similar manner since $\langle 3 \rangle \leq (\mathbb{Z}/11^m\mathbb{Z})^*$ is not of index 2 for $m > 1$.

In [10, 11], the following two constructions of skew Hadamard difference sets and Paley type partial difference sets were given. (A partial difference set D in a group G is said to be of *Paley type* if the parameters of the corresponding strongly regular Cayley graph are $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$.)

Theorem 1.4. *(i) ([10]) Let* $p_1 \equiv 7 \pmod 8$ *be a prime,* $k = 2p_1^m$, *and let* p *be a prime such that* $f := \mathrm{ord}_k(p) = \phi(k)/2$, *where* ϕ *is the Euler totient function. Let* s *be an odd integer,* H *denotes any subset of* $\mathbb{Z}_k$ *such that* $\{i \pmod{p_1^m} \mid i \in H\} = \mathbb{Z}_{p_1^m}$, *and let* $D = \bigcup_{i \in H} C_i^{(k, p^{fs})}$. *Then,* D *is a skew Hadamard difference set if* $p \equiv 3 \pmod 4$ *and* D *is a Paley type partial difference set if* $p \equiv 1 \pmod 4$.

(ii) ([11]) Let $q = p^{p_1^{m-1}(p_1-1)/2}$, $k = 2p_1^m$, *and* $H = Q \cup 2Q \cup \{0\}$, *where* Q *is the subgroup of index* 2 *of* $(\mathbb{Z}/2p_1\mathbb{Z})^*$. *Set* $D = \bigcup_{j=0}^{p_1^{m-1}} \bigcup_{i \in H} C^{(k,q)}_{2j+ip_1^{m-1}}$. *Then,* D *is a skew Hadamard difference set in the case when* $(p, p_1) = (3, 107)$ *and* D *is a Paley type partial difference set in the cases when*

$$(p, p_1) = (5, 19), (17, 67), (41, 163), (5, 499).$$

The proofs of the above theorems are based on index 2 and 4 Gauss sums. In order to show that the srgs of No. 5 and 8 in Table 1 lead to infinite families, we need to explicitly evaluate index 6 Gauss sums if we apply a similar technique of [9, 10, 11, 13]. However, it seems to be difficult to compute index more than 4 Gauss sums, and this implies that it is hard to find new strongly regular graphs or skew Hadamard difference sets on $\mathbb{F}_q$ from index more than 4 cases. In this paper, we will show that explicit evaluations of Gauss sums are not needed if some initial examples of strongly regular Cayley graphs or skew Hadamard difference sets satisfying certain conditions are found. Instead, we will investigate the rationality of "relative Gauss sums". As consequences, we generalize the srgs of No. 5 and 8 in Table 1 into infinite families and find further infinite families of cyclotomic srgs with new parameters as generalizations of subfield examples (see Tables 2 and 3 in Section 3.2). Furthermore, we obtain two infinite families of skew Hadamard difference sets in $(\mathbb{F}_q, +)$, where $q = 3^{3 \cdot 13^{m-1}}$ and $7^{7 \cdot 29^{m-1}}$.

2 Rationality of relative Gauss sums

2.1 Preliminary

Let p be a prime, f a positive integer, and $q = p^f$. The canonical additive character ψ of $\mathbb{F}_q$ is defined by

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

where $\zeta_p = \exp(\frac{2\pi i}{p})$ and $\mathrm{Tr}_{q/p}$ is the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. For a multiplicative character χ of $\mathbb{F}_q$, we define the *Gauss sum*

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

which belongs to $\mathbb{Z}[\zeta_{kp}]$ of integers in the cyclotomic field $\mathbb{Q}(\zeta_{kp})$, where m is the order of χ. Let $\sigma_{a,b}$ be the automorphism of $\mathbb{Q}(\zeta_{kp})$ determined by

$$\sigma_{a,b}(\zeta_k) = \zeta_k^a, \qquad \sigma_{a,b}(\zeta_p) = \zeta_p^b$$

for $\gcd(a,k) = \gcd(b,p) = 1$. Below are several basic properties of Gauss sums [18]:

(i) $G_f(\chi)\overline{G_f(\chi)} = q$ if χ is nontrivial;

(ii) $G_f(\chi^p) = G_f(\chi)$, where p is the characteristic of $\mathbb{F}_q$;

(iii) $G_f(\chi^{-1}) = \chi(-1)\overline{G_f(\chi)}$;

(iv) $G_f(\chi) = -1$ if χ is trivial;

(v) $\sigma_{a,b}(G_f(\chi)) = \chi^{-a}(b)G_f(\chi^a)$;

In general, the explicit evaluation of Gauss sums is a very difficult problem. There are only a few cases where the Gauss sums have been evaluated. The most well known case is *quadratic* case, in other words, the order of χ is two.

Lemma 2.1. *([18]) Let η be the quadratic character of $\mathbb{F}_q = \mathbb{F}_{p^f}$. Then, it holds that*

$$G_f(\eta) = (-1)^{f-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)^f.$$

The next simple case is the so-called *semi-primitive case* (also referred to as *uniform cyclotomy* or *pure Gauss sum*), where there exists an integer j such that $p^j \equiv -1 \pmod{k}$, where k is the order of the multiplicative character χ involved.

Theorem 2.2. *([3]) Suppose that $k > 2$ and p is semi-primitive modulo k, i.e., there exists an s s.t. $p^s \equiv -1 \pmod{k}$. Choose s minimal and write $f = 2st$. Let χ be a multiplicative character of order k. Then,*

$$p^{-f/2}G_f(\chi) = \begin{cases} (-1)^{t-1} & \text{if } p = 2; \\ (-1)^{t-1+(p^s+1)t/k} & \text{if } p > 2. \end{cases}$$

This theorem was used to find strongly regular graphs and difference sets on $\mathbb{F}_q$, e.g., see [2, 6].

The next interesting case is the index 2 case where the subgroup $\langle p\rangle$ generated by $p \in (\mathbb{Z}/k\mathbb{Z})^*$ has index 2 in $(\mathbb{Z}/k\mathbb{Z})^*$ and $-1 \notin \langle p\rangle$. In this case, it is known that k can have at most two odd prime divisors. Many authors have investigated this case, see e.g., [1, 16, 21, 23, 30, 31]. In particular, complete solution to the problem of evaluating Gauss sums in this case was recently given in [30]. Also, the index 4 case was treated in [8, 29]. Recently, these index 2 and 4 Gauss sums

were applied to show the existence of infinite families of new strongly regular graphs and skew Hadamard difference sets on $\mathbb{F}_q$ in [9, 10, 11, 13]. However, it is quite difficult to explicitly evaluate Gauss sums of general index. This implies that it is difficult to find new strongly regular graphs on $\mathbb{F}_q$ from index more than 4 cases if we apply a similar technique of [9, 10, 11, 13]. However, we will show in Section 3 of this paper that explicit evaluations of Gauss sums are not needed if some initial examples of strongly regular graphs or skew Hadamard difference sets satisfying certain conditions are found. Instead, we will use rationality of relative Gauss sums. For two nontrivial multiplicative characters χ of $\mathbb{F}_{p^f}$ and χ' of $\mathbb{F}_{p^{f'}}$ with $f \mid f'$, the *relative Gauss sum associated with* χ *and* χ' is defined as

$$\vartheta_p(\chi', \chi) := \frac{G_{f'}(\chi')}{p^{\frac{f'-f}{2}} G_f(\chi)}.$$

In particular, we investigate when $\vartheta_p(\chi', \chi) = 1$ or -1 holds in the case where both of $G_{f'}(\chi')$ and $G_f(\chi)$ are of index e case. Note that the concept of relative Gauss sums was introduced in [28] as the fractional $G_{f'}(\chi')/G_f(\chi)$, where χ is the restriction of χ' to $\mathbb{F}_{p^f}$. Hence, our definition generalize his definition and normalize so that the absolute value is equal to 1 when χ and χ' are nontrivial.

Below, we give important formulae on Gauss sums. The following is known as *the Davenport-Hasse lifting formula*.

Theorem 2.3. *([3, 18]) Let χ be a nontrivial character on $\mathbb{F}_q = \mathbb{F}_{p^f}$ and let χ' be the lifted character of χ to $\mathbb{F}_{q'} = \mathbb{F}_{p^{fs}}$, i.e., $\chi'(\alpha) := \chi(\mathrm{Norm}_{\mathbb{F}_{q'}/\mathbb{F}_q}(\alpha))$ for $\alpha \in \mathbb{F}_{q'}$. Then, it holds that*

$$G_{fs}(\chi') = (-1)^{s-1}(G_f(\chi))^s.$$

The following is called *the Davenport-Hasse product formula*.

Theorem 2.4. *([3]) Let η be a character on $\mathbb{F}_q = \mathbb{F}_{p^r}$ of order $\ell > 1$. For every nontrivial character χ on $\mathbb{F}_q$,*

$$G_r(\chi) = \frac{G_r(\chi^\ell)}{\chi^\ell(\ell)} \prod_{i=1}^{\ell-1} \frac{G_r(\chi\eta^i)}{G_r(\eta^i)}.$$

We close this subsection providing the following lemma [28].

Lemma 2.5. *([28]) Let χ' be a character of order k' of $\mathbb{F}_{p^{f'}}$ and χ be the restriction of χ' to $\mathbb{F}_{p^f}$, where $f \mid f'$. If χ is nontrivial on $\mathbb{F}_{p^f}$, it holds that*

$$p^{\frac{f-f'}{2}} \vartheta_p(\chi', \chi) = \sum_{x \in L; \mathrm{Tr}_{p^{f'}/p^f}(x)=1} \chi'(x),$$

where L is a set of representatives for $\mathbb{F}^*_{p^{f'}}/\mathbb{F}^*_{p^f}$.

2.2 Relative Gauss sums

In this section, fix an integer $k > 1$, and let p be a prime such that $\gcd(p, k) = 1$. Let f be the order of p in $(\mathbb{Z}/k\mathbb{Z})^*$ and set $q = p^f$. Write $\zeta_k = e^{2\pi i/k}$ and $\zeta_p = e^{2\pi i/p}$. Define

$$K = \mathbb{Q}(\zeta_k),\ M = K(\zeta_p) = \mathbb{Q}(\zeta_k, \zeta_p),$$

and let O_k and O_M denote their respective rings of integers. For $j \in (\mathbb{Z}/k\mathbb{Z})^*$, define $\sigma_j \in \mathrm{Gal}(M/\mathbb{Q}(\zeta_p))$ by $\sigma_j(\zeta_k) = \zeta_k^j$. Let P be a prime ideal of O_K lying over p. Then, for some prime ideal $\mathfrak{p}$ of O_M such that $PO_M = \mathfrak{p}^{p-1}$ and $\mathfrak{p} \cap O_K = P$. Write $P_j = \sigma_j(P)$ and $\mathfrak{p}_j = \sigma_j(\mathfrak{p})$, and

then $P_jO_M = \mathfrak{p}_j^{p-1}$. Let T be a set of representatives of $(\mathbb{Z}/k\mathbb{Z})^*/\langle p\rangle$. Then, $pO_K = \prod_{j\in T} P_j$ follows, where P_j are all distinct, and hence $pO_M = \prod_{j\in T} \mathfrak{p}_j^{p-1}$ holds.

Define the character χ_P of order k on the finite field O_K/P by letting $\chi_P(\alpha+P)$ denote the unique power of ζ_k such that

$$\chi_P(\alpha + P) \equiv \alpha^{(q-1)/k} \pmod{P},$$

when $\alpha \in O_K \setminus P$. When $\alpha \in P$, set $\chi_P(\alpha + P) = 0$. We call χ_P *the Teichmüller character associated to* P. Now we identify χ_P with a character of $\mathbb{F}_q$.

Define

$$\theta(k,p) = \sum_{t\in(\mathbb{Z}/k\mathbb{Z})^*} \left\langle \frac{t}{k} \right\rangle \sigma_t^{-1},$$

called *the Stickelberger element*, where $\langle x\rangle$ is the fractional part of the rational x. Every integer a can be written uniquely in the form $\sum_{i=0}^{n} a_i p^i$, where $0 \le a_i < p$. We denote by $s_p(a)$ the sum of all a_i. The following are given in [3, 15].

Lemma 2.6. *For any integer a, $0 \le a < q-1$, we have*

$$s_p(a) = (p-1)\sum_{i=0}^{f-1} \left\langle \frac{p^i a}{q-1} \right\rangle.$$

Theorem 2.7. *Let k be a positive integer. Let p be a prime such that $\gcd(p,k) = 1$ and f be the order of p in $(\mathbb{Z}/k\mathbb{Z})^*$. For a prime ideal $\mathfrak{p}$ of O_M lying over P, it holds*

$$G_f(\chi_P^{-1})O_M = \mathfrak{p}^{\sum_{t\in T} s_p(t(q-1)/k)\sigma_t^{-1}} = \mathfrak{p}^{(p-1)\sum_{t\in T}\sum_{i=0}^{f-1}\langle tp^i/k\rangle\sigma_t^{-1}} \subseteq O_M.$$

This theorem is known as *the Stickelberger relation*. By the relation $G_f(\chi^a)G_f(\chi^{-a}) = \pm p^f$, we also have

$$G_f(\chi_P)O_M = \mathfrak{p}^{(p-1)(f\sum_{t\in T}\sigma_t - \sum_{t\in T}\sum_{i=0}^{f-1}\langle tp^i/k\rangle\sigma_t^{-1})}.$$

In the rest of this paper, we will assume the following. Let $h = 2^t p_1 p_2 \cdots p_\ell$ be a positive integer with distinct odd primes p_i and p be a prime satisfying the following: For any divisor $d = 2^s p_{i_1}\cdots p_{i_m}$ of h, if $\langle p\rangle$ is of index u modulo d, then so does $\langle p\rangle$ modulo $d' = 2^s p_{i_1}^{x_1}\cdots p_{i_m}^{x_m}$ for any $x_i \ge 1$. Let e denotes the index of $\langle p\rangle$ modulo h. Let p_1 be an odd prime factor of $k = 2^t p_1^{e_1} p_2^{e_2}\cdots p_\ell^{e_\ell}$ and set $k' = kp_1$. Then, by the assumption, $\langle p\rangle$ is again of index e in both of $(\mathbb{Z}/k\mathbb{Z})^*$ and $(\mathbb{Z}/k'\mathbb{Z})^*$. Set $q = p^f$ and $q' = p^{f'}$, where $f = \phi(k)/e$ and $f' = \phi(k')/e$.

Let $O_K, O_{K'}, O_M, O_{M'}, O_L, O_{L'}$ denote the respective rings of integers of $\mathbb{Q}(\zeta_k)$, $\mathbb{Q}(\zeta_{k'})$, $\mathbb{Q}(\zeta_k,\zeta_p)$, $\mathbb{Q}(\zeta_{k'},\zeta_p)$, $\mathbb{Q}(\zeta_{p^f-1})$, $\mathbb{Q}(\zeta_{p^{f'}-1})$. Let $P \subseteq O_K$ be a prime ideal lying over p and $\mathfrak{p} \subseteq O_M$ be a prime ideal lying over P. Also, let $\mathfrak{p}' \subseteq O_{M'}$ be a prime ideal lying over $\mathfrak{p}$ and let $P' = \mathfrak{p}' \cap O_{K'}$, so that $\mathfrak{p}' \cap O_M = \mathfrak{p}$ and $P' \cap O_K = P$. Let T' be a set of representatives for $(\mathbb{Z}/k'\mathbb{Z})^*/\langle p\rangle$. Then, there is a one to one correspondence between $\{\sigma_j(P)(=: P_j) \mid j \in T\}$ and $\{\sigma'_j(P)(=: P'_j) \mid j \in T'\}$ such that $P_j = P'_j \cap O_K$, where $\sigma'_j \in \mathrm{Gal}(\mathbb{Q}(\zeta_{k'p})/\mathbb{Q}(\zeta_p))$ satisfying $\sigma'_j(\zeta_{k'}) = \zeta_{k'}^j$. By multiplying $O_{K'}$ to both side of $pO_K = \prod_{j\in T} P_j$, together with $pO_{K'} = \prod_{j\in T'} P'_j$, we have $P_jO_{K'} = P'_j$. Furthermore, by multiplying $O_{M'}$ to both side of $P_jO_{K'} = P'_j$, we have $P_jO_{M'} = P'_jO_{M'} = \mathfrak{p'}_j^{p-1}$, where $\mathfrak{p'}_j \subseteq O_{M'}$ is a prime ideal lying over P'_j. On the other hand, since $P_jO_{M'} = \mathfrak{p}_j^{p-1}O_{M'}$, we obtain $\mathfrak{p}_jO_{M'} = \mathfrak{p'}_j$.

Let $\mathfrak{P} \subseteq O_L$ and $\mathfrak{P}' \subseteq O_{L'}$ be prime ideals lying over P and P', respectively. It is known that $O_L/\mathfrak{P} = \{\alpha + \mathfrak{P} \mid \alpha \in O_K/P\}$ and that

$$\chi_{\mathfrak{P}}^{\frac{p^f-1}{k}}(\alpha + \mathfrak{P}) = \chi_P(\alpha + P)$$

for $\alpha \in O_K$, so that

$$G_f(\chi_{\mathfrak{P}}^{a\frac{p^f-1}{k}}) = G_f(\chi_P^a).$$

See Exercise 11-1 of [3]. Now, we can take the set $\{0\} \cup \{\zeta_{p^f-1}^i \,|\, 0 \le i \le p^f - 1\}$ as representatives for $O_L/\mathfrak{P}$ and then

$$\chi_{\mathfrak{P}}(\zeta_{p^f-1}^i + \mathfrak{P}) = \zeta_{p^f-1}^i.$$

By the definition of Teichmüller characters, for $\alpha \in (\zeta_{p^f-1} + \mathfrak{P}) \cap O_K$ and $\beta \in (\zeta_{p^{f'}-1} + \mathfrak{P}') \cap O_{K'}$ it holds

$$\begin{aligned} \chi_P(\alpha^i + P) &= \chi_{\mathfrak{P}}(\zeta_{p^f-1}^{\frac{p^f-1}{k}i} + \mathfrak{P}) = \chi_{\mathfrak{P}'}^{\frac{p^f-1}{k}}(\zeta_{p^{f'}-1}^{\frac{p^{f'}-1}{p^f-1}i} + \mathfrak{P}') \\ &= \chi_{\mathfrak{P}'}^{p_1}(\zeta_{p^{f'}-1}^{\frac{p^{f'}-1}{kp_1}i} + \mathfrak{P}') = \chi_{P'}^{p_1}(\beta^i + P'), \end{aligned} \tag{2.1}$$

where $\alpha + P$ and $\beta + P'$ are primitive root of the finite fields O_K/P and $O_{K'}/P'$.

First, we show the following lemma.

Lemma 2.8. *Let $\chi_{P'}$ and χ_P be the Teichmüller characters associated to P' and P, respectively. Then,*

$$(\vartheta_p(\chi_{P'}, \chi_P) :=) \frac{G_{f'}(\chi_{P'})}{p^{\frac{\phi(k)(p_1-1)}{2e}} G_f(\chi_P)}$$

is a $2k'$th or k'th root of unity according as k' is odd or not.

Proof: First of all, we see $\vartheta_p(\chi_{P'}, \chi_P) \in \mathbb{Q}(\zeta_{k'})$. Note that χ_P is the restriction of $\chi_{P'}$ to $\mathbb{F}_{p^f}$ since

$$\chi_{\mathfrak{P}'}^{\frac{p^{f'}-1}{k'}}(\zeta_{p^f-1} + \mathfrak{P}') = \chi_{\mathfrak{P}}^{\frac{p^f-1}{k}}(\zeta_{p^f-1} + \mathfrak{P})$$

by $(p^{f'} - 1)/k' \equiv (p^f - 1)/k \,(\mathrm{mod}\, p^f - 1)$. (Thus, in this case, our definition of relative Gauss sums is just the normalization of Yamamoto's relative Gauss sums.) By Lemma 2.5, $\vartheta_p(\chi_{P'}, \chi_P) \in \mathbb{Q}(\zeta_{k'})$ follows.

Put $f = \frac{\phi(k)}{e}$ and $f' = \frac{\phi(k)p_1}{e}$, and set $h = 2^t \prod_{i=1}^{\ell} p_i$, where $p_1, p_2, \ldots, p_\ell$ be all distinct prime factors of k and t is the highest power of 2 dividing k. It is clear that

$$k \sum_{i=0}^{f-1} \left\langle \frac{tp^i}{k} \right\rangle = \sum_{i=0}^{f-1} [tp^i]_k,$$

where $[a]_k$ means the reduction of a modulo k. In other words, it is equal to

$$\begin{aligned} \sum_{x \in \langle p \rangle \le (\mathbb{Z}/k\mathbb{Z})^*} [tx]_k &= \sum_{y=0}^{\frac{k}{h}-1} \sum_{z \in \langle p \rangle \le (\mathbb{Z}/h\mathbb{Z})^*} hy + [tz]_h \\ &= k(\frac{k}{h} - 1)\phi(h)/2e + \frac{k}{h} \sum_{z \in \langle p \rangle \le (\mathbb{Z}/h\mathbb{Z})^*} [tz]_h \end{aligned}$$

where note that t's modulo h again forms a set of representatives of $(\mathbb{Z}/h\mathbb{Z})^*/\langle p \rangle$. Thus, we have

$$\sum_{i=0}^{f-1} \left\langle \frac{tp^i}{k} \right\rangle = \frac{\phi(k) - \phi(h)}{2e} + \frac{1}{h} \sum_{z \in \langle p \rangle \le (\mathbb{Z}/h\mathbb{Z})^*} [tz]_h.$$

Similarly, we obtain

$$\sum_{i=0}^{f'-1}\left\langle \frac{tp^i}{k'}\right\rangle = \frac{\phi(k')-\phi(h)}{2e} + \frac{1}{h}\sum_{z\in\langle p\rangle\le(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h.$$

Hence, by the Stickelberger relation, we obtain

$$G_{f'}(\chi_{P'})O_{M'} = \mathfrak{p}'^{(p-1)((f'-\frac{\phi(k')-\phi(h)}{2e})\sum_{t\in T'}\sigma_t-\sum_{t\in T'}(\frac{1}{h}\sum_{z\in\langle p\rangle\le(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h)\sigma_t^{-1})}.$$

Furthermore, by noting that $\mathfrak{p}O_{M'} = \mathfrak{p}'$, we have

$$G_f(\chi_P)O_{M'} = \mathfrak{p}'^{(p-1)((f-\frac{\phi(k)-\phi(h)}{2e})\sum_{t\in T'}\sigma_t-\sum_{t\in T'}(\frac{1}{h}\sum_{z\in\langle p\rangle\le(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h)\sigma_t^{-1})}.$$

Since $pO_{M'} = \mathfrak{p}'^{(p-1)\sum_{i\in T'}\sigma_t}$, it follows that $p^{\frac{\phi(k')-\phi(k)}{2e}}G_f(\chi_P)O_{M'} = G_{f'}(\chi_{P'})O_{M'}$, i.e., $\vartheta_p(\chi_{P'},\chi_P)$ is a unit of $O_{M'}$. But, $\vartheta_p(\chi_{P'},\chi_P)\in\mathbb{Q}(\zeta_{k'})$, and hence it is a unit of $O_{K'}$. Furthermore, all the conjugates of $\vartheta_p(\chi_{P'},\chi_P)$ in $O_{K'}$ have absolute value 1. Therefore, $\vartheta_p(\chi_{P'},\chi_P)$ is a root of unity in $O_{K'}$, which completes the proof. □

Lemma 2.9. *Let $d = 2\gcd(k',p-1)$ or $\gcd(k',p-1)$ according as k' is odd or even. Then, it holds that*

$$\vartheta_p(\chi_{P'},\chi_P)^d = 1.$$

Proof: Define $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_p,\zeta_{k'})/\mathbb{Q}(\zeta_p))$ by $\sigma(\zeta_{pk'}) = \zeta_{pk'}^{k'\ell+p}$, where ℓ is the inverse of k' modulo p. Let ψ' and ψ be the respective canonical additive characters of $\mathbb{F}_{q'}$ and $\mathbb{F}_q$. Then,

$$\begin{aligned}
\sigma\left(\frac{G_{f'}(\chi_{P'})}{G_f(\chi_P)}\right) &= \sigma\left(\frac{\sum_{\alpha\in\mathbb{F}_{q'}}\psi'(\alpha)\chi_{P'}(\alpha)}{\sum_{\beta\in\mathbb{F}_q}\psi(\beta)\chi_P(\beta)}\right)\\
&= \frac{\sum_{\alpha\in\mathbb{F}_{q'}}\psi'((k'\ell+p)\alpha)\chi_{P'}^{k'\ell+p}(\alpha)}{\sum_{\beta\in\mathbb{F}_q}\psi((k'\ell+p)\beta)\chi_P^{k'\ell+p}(\beta)}\\
&= \frac{\sum_{\alpha\in\mathbb{F}_{q'}}\psi'(\alpha)\chi_{P'}^{p}(\alpha)}{\sum_{\beta\in\mathbb{F}_q}\psi(\beta)\chi_P^{p}(\beta)}\\
&= \frac{G_{f'}(\chi_{P'}^p)}{G_f(\chi_P^p)} = \frac{G_{f'}(\chi_{P'})}{G_f(\chi_P)}.
\end{aligned}$$

Hence, $\sigma(\vartheta_p(\chi_{P'},\chi_P)) = \vartheta_p(\chi_{P'},\chi_P)$. On the other hand, in the case when k' is odd, since $\vartheta_p(\chi_{P'},\chi_P)^2 = \zeta_{k'}^s$ for some s by Lemma 2.8, it follows that $\sigma(\vartheta_p(\chi_{P'},\chi_P)^2) = \vartheta_p(\chi_{P'},\chi_P)^{2(k'\ell+p)} = \vartheta_p(\chi_{P'},\chi_P)^{2p}$, so $\vartheta_p(\chi_{P'},\chi_P)^{2(p-1)} = 1$. Together with $\vartheta_p(\chi_{P'},\chi_P)^{2k'} = 1$, we obtain $\vartheta_p(\chi_{P'},\chi_P)^{2\gcd(k',p-1)} = 1$. In the case when k' is even, since $\vartheta_p(\chi_{P'},\chi_P) = \zeta_{k'}^s$ for some s by Lemma 2.8, it follows that $\sigma(\vartheta_p(\chi_{P'},\chi_P)) = \vartheta_p(\chi_{P'},\chi_P)^{k'\ell+p} = \vartheta_p(\chi_{P'},\chi_P)^p$, so $\vartheta_p(\chi_{P'},\chi_P)^{p-1} = 1$. Together with $\vartheta_p(\chi_{P'},\chi_P)^{k'} = 1$, we obtain $\vartheta_p(\chi_{P'},\chi_P)^{\gcd(k',p-1)} = 1$. □

The following is our main theorem of this section.

Theorem 2.10. *If k' is odd and $\gcd(k',p-1) = 1$, it holds that $\vartheta_p(\chi_{P'},\chi_P) = 1$.*

Proof: By Lemma 2.9, we have $\vartheta_p(\chi_{P'},\chi_P) = -1$ or 1. We consider the reduction of $p^{\frac{\phi(k')-\phi(k)}{2e}}G_f(\chi_P)\vartheta_p(\chi_{P'},\chi_P)$ modulo $\lambda := 1-\zeta_{p_1^{t+1}}$, where t is the highest power of p_1 dividing k. It is clear that $p^{\frac{\phi(k)(p_1-1)}{2e}}\equiv 1\pmod{\lambda}$. Let $h := k'/p_1^{t+1}$. Since χ_P and $\chi_{P'}$ can be written as $\chi_P^{xh}\chi_P^{yp_1^{t+1}}$ and $\chi_{P'}^{xh}\chi_{P'}^{yp_1^{t+1}}$ for some x and y such that $xh+yp_1^{t+1}\equiv 1\pmod{k'}$. Then, we have $G_{f'}(\chi_{P'})\equiv G_{f'}(\chi_{P'}^{yp_1^{t+1}})\pmod{\lambda}$ and $G_f(\chi_P)\equiv G_f(\chi_P^{yp_1^{t+1}})\pmod{\lambda}$, where both of $\chi_{P'}^{yp_1^{t+1}}$ and $\chi_P^{yp_1^{t+1}}$ are of order h. Now, note that

$$\chi_{\mathfrak{P}}^{yp_1^t\frac{p^f-1}{k}}(\zeta_{p^{fp_1}-1}^{i\frac{p^{fp_1}-1}{p^f-1}}+\mathfrak{P}) = \chi_{\mathfrak{P}'}^{yp_1^t\frac{p^f-1}{k}}(\zeta_{p^{fp_1}-1}^{i\frac{p^{fp_1}-1}{p^f-1}}+\mathfrak{P}') = \chi_{\mathfrak{P}'}^{yp_1^{t+1}\frac{p^{fp_1}-1}{kp_1}}(\zeta_{p^{fp_1}-1}^{i}+\mathfrak{P}').$$

By the Davenport-Hasse lifting formula, we have

$$\begin{aligned} G_{f'}(\chi_{P'}^{yp_1^{t+1}}) &= G_{f'}(\chi_{\mathfrak{P}'}^{yp_1^{t+1}\frac{p^{fp_1-1}}{kp_1}}) \equiv (-1)^{p_1-1}(G_f(\chi_{\mathfrak{P}}^{yp_1^t\frac{p^f-1}{k}}))^{p_1} \pmod{\lambda} \\ &= (G_f(\chi_P^{yp_1^t}))^{p_1} \equiv \chi_P^{-yp_1^t}(p_1)G_f(\chi_P^{yp_1^{t+1}}) \pmod{\lambda}. \end{aligned}$$

Therefore, by noting that $\chi_P^{-yp_1^t}(p_1) = 1$, we obtain

$$G_f(\chi_P^{yp_1^{t+1}})(\vartheta_p(\chi_{P'}, \chi_P) - 1) \equiv 0 \pmod{\lambda}.$$

If $\vartheta_p(\chi_{P'}, \chi_P) = -1$, then $\lambda \,|\, 2G_f(\chi_P^{yp_1^{t+1}})$. Here, by Lemma 2.5, note that

$$G_f(\chi_P^{yp_1^{t+1}}) = \sum_{x \in L; \mathrm{Tr}_{p^f/p}(x)=1} \chi_P^{yp_1^{t+1}}(x) \in \mathbb{Q}(\zeta_k),$$

where L is a set of representatives for $\mathbb{F}_{p^f}^*/\mathbb{F}_p^*$. By taking norms of λ and $2G_f(\chi_P^{yp_1^{t+1}})$ in $\mathbb{Q}(\zeta_{k'})$, we obtain the contradiction that p_1 divides $2p$. □

Next, we treat the case when $2 \,||\, k'$ and $\gcd(k'/2, p-1) = 1$.

Corollary 2.11. *Assume that* $2 \,||\, k', k$ *and* $\gcd(k'/2, p-1) = \gcd(k/2, p-1) = 1$. *Then,*

$$\vartheta_p(\chi_{P'}, \chi_P) = (-1)^{\frac{(p-1)(p_1-1)\phi(h)}{4e}},$$

where h *is the product of all distinct odd prime factors of* k'.

Proof: Let $U = \mathbb{Q}(\zeta_k^2)$, $U' = \mathbb{Q}(\zeta_{k'}^2)$, $\tilde{P} = P \cap O_U$, and $\tilde{P'} = P' \cap O_{U'}$. Then, $\vartheta_p(\chi_{\tilde{P}'}, \chi_{\tilde{P}}) = 1$ by Theorem 2.4. Noting that

$$G_f(\chi_P^2) = G_f(\chi_{\mathfrak{P}}^{2\frac{p^f-1}{k}}) = G_f(\chi_{\tilde{P}})$$

and

$$G_{f'}(\chi_{P'}^2) = G_{f'}(\chi_{\mathfrak{P}'}^{2\frac{p^{f'}-1}{k'}}) = G_{f'}(\chi_{\tilde{P}'}),$$

we have

$$\begin{aligned} \vartheta_p(\chi_{P'}, \chi_P) &= \frac{G_{f'}(\chi_{P'})}{p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P)} \\ &= \frac{\chi_P^2(2)G_{f'}(\chi_{P'}^2)G_{f'}(\chi_{P'}\eta')G_f(\eta)}{p^{\frac{\phi(k')-\phi(k)}{2e}} \chi_{P'}^2(2)G_f(\chi_P^2)G_f(\chi_P\eta)G_{f'}(\eta')} \\ &= \frac{\chi_P^2(2)G_{f'}(\chi_{\tilde{P}'})G_{f'}(\chi_{\tilde{P}'}^{(1+k'/2)/2})G_f(\eta)}{p^{\frac{\phi(k')-\phi(k)}{2e}} \chi_{P'}^2(2)G_f(\chi_{\tilde{P}})G_f(\chi_{\tilde{P}}^{(1+k/2)/2})G_{f'}(\eta')} \end{aligned}$$

where η' and η are the respective quadratic characters of $\mathbb{F}_{q'}$ and $\mathbb{F}_q$. Since the restrictions of χ_P^2 and $\chi_{P'}^2$ to $\mathbb{F}_p^*$ are trivial, we have $\chi_P^2(2) = \chi_{P'}^2(2) = 1$. Furthermore, since $\vartheta_p(\chi_{\tilde{P}'}, \chi_{\tilde{P}}) = 1$, we have $G_{f'}(\chi_{\tilde{P}'})/G_f(\chi_{\tilde{P}}) = p^{(\phi(k')-\phi(k))/2e}$. Now, note that $(1+k/2)/2 = h(s-(p_1-1)k/4h) + [gp^m]_h \in (\mathbb{Z}/\frac{k}{2}\mathbb{Z})^*$ if $(1+k'/2)/2 = hs + [gp^m]_h \in (\mathbb{Z}/\frac{k'}{2}\mathbb{Z})^*$ for some g in a set of representatives of $(\mathbb{Z}/h\mathbb{Z})^*/\langle p \rangle$ and $0 \le s \le k'/2h - 1$. Hence, by Theorem 2.10 and our assumption, we have $G_{f'}(\chi_{\tilde{P}'}^{(1+k'/2)/2})/G_f(\chi_{\tilde{P}}^{(1+k/2)/2}) = p^{(\phi(k')-\phi(k))/2e}$. Finally, by the Davenport-Hasse lifting formula and Lemma 2.1, we have

$$\frac{G_{f'}(\eta')}{G_f(\eta)} = (-1)^{p_1-1}(G_f(\eta))^{p_1-1} = (-1)^{\frac{(p-1)(p_1-1)\phi(h)}{4e}} p^{\frac{\phi(k')-\phi(k)}{2e}},$$

which shows the assertion. □

Remark 2.12. *Let ϵ denote $(-1)^{\frac{(p-1)(p_1-1)\phi(h)}{4e}}$ or 1 according as $2||k$ and $\gcd(k'/2, p-1)=1$ or $2 \not| k$ and $\gcd(k', p-1)=1$. By Theorem 2.4 and Corollary 2.11, for any a s.t. $\gcd(a,k')=1$ it is clear that*

$$\vartheta_p(\chi_{P'}^a, \chi_P^a) = \epsilon$$

since $\sigma(\vartheta_p(\chi_{P'}, \chi_P)) = \vartheta_p(\chi_{P'}^a, \chi_P^a)$ and $\sigma(\epsilon)=\epsilon$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{k'p})/\mathbb{Q}(\zeta_p))$ satisfying $\sigma(\zeta_{k'}) = \zeta_{k'}^a$.

Corollary 2.13. *Assume that k' is odd and $\gcd(k', p-1)=1$. Then, it holds that $\vartheta_p(\chi_{P'}^t, \chi_P^t) = 1$ for any t such that $p^s \not| t$, where s is the highest power of p_1 dividing k.*

Proof: Put $t = a \cdot \gcd(t,k)$ with $\gcd(a,k)=1$. Let r' and r be the order of p modulo $k'/\gcd(t,k')(=: u')$ and modulo $k/\gcd(t,k)(=: u)$. Then, by our assumption, $r' = rp_1$ and $u' = up_1$ follow. Write $J = \mathbb{Q}(\zeta_u), J' = \mathbb{Q}(\zeta_{u'}), H = \mathbb{Q}(\zeta_{p^r-1}), H' = \mathbb{Q}(\zeta_{p^{r'}-1})$ and $R = P \cap O_J, R' = P' \cap O_{J'}, \mathfrak{R} = \mathfrak{P} \cap O_H, \mathfrak{R}' = \mathfrak{P}' \cap O_{H'}$. Then, we have

$$\chi_{\mathfrak{R}}^{a\frac{p^r-1}{u}}(\zeta_{p^f-1}^{i\frac{p^f-1}{p^r-1}} + \mathfrak{R}) = \chi_{\mathfrak{P}}^{a\frac{p^f-1}{u}}(\zeta_{p^f-1}^i + \mathfrak{P}) = \chi_{\mathfrak{P}}^{\frac{p^f-1}{k}t}(\zeta_{p^f-1}^i + \mathfrak{P})$$

and hence $\chi_{\mathfrak{P}}^{\frac{p^f-1}{k}t}$ is the lift of $\chi_{\mathfrak{R}}^{a\frac{p^r-1}{u}}$ to $\mathbb{F}_{p^f}$. Similarly, $\chi_{\mathfrak{P}'}^{\frac{p^{f'}-1}{k'}t}$ is the lift of $\chi_{\mathfrak{R}'}^{a\frac{p^{r'}-1}{u'}}$ to $\mathbb{F}_{p^{f'}}$. Now, by the Davenport-Hasse lifting formula, we have

$$\begin{aligned}
\vartheta_p(\chi_{P'}^t, \chi_P^t) &= \frac{G_{f'}(\chi_{P'}^t)}{p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P^t)} = \frac{G_{f'}(\chi_{\mathfrak{P}'}^{\frac{p^{f'}-1}{k'}t})}{p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_{\mathfrak{P}}^{\frac{p^f-1}{k}t})} \\
&= \frac{(-1)^{f'/r'-1}(G_{r'}(\chi_{\mathfrak{R}'}^{a\frac{p^{r'}-1}{u'}}))^{f'/r'}}{(-1)^{f/r-1} p^{\frac{\phi(k')-\phi(k)}{2e}} (G_r(\chi_{\mathfrak{R}}^{a\frac{p^r-1}{u}}))^{f/r}} \\
&= \frac{1}{p^{\frac{\phi(k')-\phi(k)}{2e}}} \cdot \left(\frac{G_{r'}(\chi_{R'}^a)}{G_r(\chi_R^a)}\right)^{f/r}.
\end{aligned}$$

Applying Theorem 2.10, the above is equal to

$$\frac{1}{p^{\frac{\phi(k')-\phi(k)}{2e}}} \cdot \left(p^{\frac{r'-r}{2}} \vartheta_p(\chi_{R'}, \chi_R)\right)^{f/r} = 1,$$

which completes the proof. □

3 Constructions of strongly regular graphs and skew Hadamard difference sets

3.1 General construction

We first recall the following well-known lemma in the theory of difference sets (see e.g., [20, 26]).

Lemma 3.1. *Let $(G,+)$ be an abelian group of odd order v, D a subset of G of size $\frac{v-1}{2}$. Assume that $D \cap -D = \emptyset$ and $0 \notin D$. Then, D is a skew Hadamard difference set in G if and only if*

$$\chi(D) = \frac{-1 \pm \sqrt{-v}}{2}$$

for all nontrivial characters χ of G. On the other hand, assume that $0 \notin D$ and $-D = D$. Then D is a Paley type partial difference set in G if and only if

$$\chi(D) = \frac{-1 \pm \sqrt{v}}{2}$$

for all nontrivial characters χ of G.

Let q be a prime power and let $C_i^{(k,q)} = \gamma^i\langle\gamma^k\rangle$, $0 \le i \le k-1$, be the cyclotomic classes of order k of $\mathbb{F}_q$, where γ is a fixed primitive element of $\mathbb{F}_q$. From now on, we will assume that D is a union of cyclotomic classes of order k of $\mathbb{F}_q$. In order to check whether a candidate subset, $D = \bigcup_{i\in I} C_i^{(k,q)}$, is a connection set of a strongly regular Cayley graph (i.e., a regular partial difference set), we will compute the sums $\psi(aD) := \sum_{x\in D}\psi(ax)$ for all $a \in \mathbb{F}_q^*$, where ψ is the canonical additive character of $\mathbb{F}_q$, since the restricted eigenvalues of Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, as explained in [5, p. 134], are $\psi(\gamma^a D)$, where $a = 0, 1, \ldots, q-2$. Similarly, to check whether D is a skew Hadamard difference set in $(\mathbb{F}_q, +)$, we will compute the sums $\psi(aD)$ for all $a \in \mathbb{F}_q^*$ because of Lemma 3.1. Thus, by Theorem 1.1 and Lemma 3.1, in both cases we need to show that the set $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\}$ has precisely two elements. Note that the sum $\psi(aD)$ can be expressed as a linear combination of Gauss sums using the orthogonality of characters:

$$\begin{aligned}
\psi(aD) &= \frac{1}{k}\sum_{i\in I}\sum_{x\in\mathbb{F}_q^*}\psi(a\gamma^i x^k)\\
&= \frac{1}{k}\sum_{i\in I}\sum_{x\in\mathbb{F}_q^*}\frac{1}{q-1}\sum_{y\in\mathbb{F}_q^*}\psi(y)\sum_{\chi\in\widehat{\mathbb{F}_q^*}}\chi(a\gamma^i x^k)\overline{\chi(y)}\\
&= \frac{1}{(q-1)k}\sum_{i\in I}\sum_{x\in\mathbb{F}_q^*}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}G(\chi^{-1})\chi(a\gamma^i x^k)\\
&= \frac{1}{(q-1)k}\sum_{i\in I}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}G(\chi^{-1})\chi(a\gamma^i)\sum_{x\in\mathbb{F}_q^*}\chi(x^k)\\
&= \frac{1}{k}\sum_{\chi\in C_0^\perp}G(\chi^{-1})\sum_{i\in I}\chi(a\gamma^i),
\end{aligned}$$

where $\widehat{\mathbb{F}_q^*}$ is the group of multiplicative characters of $\mathbb{F}_q^*$ and $C_0^\perp$ is the subgroup of $\widehat{\mathbb{F}_q^*}$ consisting of all χ which are trivial on $C_0^{(k,q)}$.

In this section, similar to Section 2, we will assume the following. Let $h = 2^t p_1 p_2 \cdots p_\ell$ be a positive integer with distinct odd primes p_i and let p be a prime satisfying the following: For any divisor $d = 2^s p_{i_1}\cdots p_{i_m}$ of h, if $\langle p\rangle$ is of index u modulo d, then so does $\langle p\rangle$ modulo $d' = 2^s p_{i_1}^{x_1}\cdots p_{i_m}^{x_m}$ for any $x_i \ge 1$. Let e denotes the index of $\langle p\rangle$ modulo h. We write $k = \prod_{i=1}^{\ell} 2^t p_i^{e_i}$ and $k' = kp_1$.

Theorem 3.2. *Let $q = p^f$ and $q' = p^{f'}$, where $f = \phi(k)/e$ and $f' = \phi(k')/e$, and let*

$$J = \{x \,|\, x \text{ divides } k \text{ and } x \text{ is not divisible by } p_1^{e_1}\} \subseteq \mathbb{N}.$$

Let J_1 and J_2 be a partition of J into two parts and let I be a subset of $\{0, 1, \ldots, k-1\}$ satisfying the following conditions:

(i) $\sum_{i\in I}\zeta_k^{ij} = 0$ *for all* $j \in J_1$.

(ii) $\theta_p(\chi_{P'}^j, \chi_P^j) = \epsilon$ *for all* $j \in J_2$, *where* $\epsilon = 1$ *or* -1 *not depending on* j.

(iii) If $\ell \ge 2$ *or* $t \ge 1$,

$$G_{f'}(\chi_{P'}^{-p_1^{e_1+1}v}) = \epsilon p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P^{-p_1^{e_1}v})$$

for all $1 \le v \le k/p_1^{e_1} - 1$.

Let

$$D = \bigcup_{i\in I} C_i^{(k,q)} \quad \text{and} \quad D' = \bigcup_{i\in I}\bigcup_{j=0}^{p_1-1} C_{ip_1+jk/p_1^{e_1}}^{(kp_1,q')}.$$

Assume that the size of the set $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\}$ is exactly two, where γ is a primitive root of $\mathbb{F}_q$ and ψ is the canonical additive character of $\mathbb{F}_q$. Then, the size of the set $\{\psi'(\omega^a D') \,|\, a = 0, 1, \ldots, q'-2\}$ is exactly two, where ω is a primitive root of $\mathbb{F}_{q'}$ and ψ' is the canonical additive character of $\mathbb{F}_{q'}$.

Proof: In this proof, without loss of generality, we assume that the primitive roots γ and ω have the forms $\gamma = \alpha + P \in O_K/P$ and $\omega = \beta + P' \in O_{K'}/P'$ for α and β of (2.1). Then, $\chi^u_{P'}(\omega^{p_1}) = \chi^u_P(\gamma)$ follows.

To prove the theorem, it is sufficient to evaluate the sum

$$kp_1 \cdot \psi'(\omega^a D') = \sum_{u=0}^{kp_1-1} G_{f'}(\chi_{P'}^{-u}) \sum_{i\in I} \sum_{j=0}^{p_1-1} \chi^u_{P'}(\omega^{a+ip_1+jk/p_1^{e_1}}),$$

where $a = 0, 1, \ldots, k'-1$ and ψ' is the canonical additive character of $\mathbb{F}_{q'}$.

For $u = 0$, we have

$$G_{f'}(\chi^0_{P'}) \sum_{i\in I} \sum_{j=0}^{p_1-1} \chi^0_{P'}(\omega^{a+ip_1+jk/p_1^{e_1}}) = -p_1|I|.$$

For $u = p_1^{e_1} v$ with $v \not\equiv 0 \,(\mathrm{mod}\, p_1)$, we have

$$G_{f'}(\chi_{P'}^{-p_1^{e_1}v}) \sum_{i\in I} \sum_{j=0}^{p_1-1} \chi_{P'}^{p_1^{e_1}v}(\omega^{a+ip_1+jk/p_1^{e_1}}) = 0. \tag{3.1}$$

If $\ell \geq 2$ or $t \geq 1$, for $u = p_1^{e_1+1}v$ with $v \neq 0$, we have

$$G_{f'}(\chi_{P'}^{-p_1^{e_1+1}v}) \sum_{i\in I} \sum_{j=0}^{p_1-1} \chi_{P'}^{p_1^{e_1+1}v}(\omega^{a+ip_1+jk/p_1^{e_1}}) = p_1 G_{f'}(\chi_{P'}^{-p_1^{e_1+1}v}) \sum_{i\in I} \chi_{P'}^{p_1^{e_1+1}v}(\omega^{a+ip_1+jk/p_1^{e_1}})$$

for any j. Note that for each $a \in \{0, 1, \ldots, k'-1\}$, there is a unique $j \in \{0, 1, \ldots, p_1-1\}$ such that $p_1 \,|\, a + jk/p_1^{e_1}$; we write $a + jk/p_1^{e_1} = p_1 j_a$. Then, the above is equal to

$$p_1 G_{f'}(\chi_{P'}^{-p_1^{e_1+1}v}) \sum_{i\in I} \chi_{P'}^{p_1^{e_1+1}v}(\omega^{p_1(j_a+i)}). \tag{3.2}$$

Furthermore, since $\chi^u_{P'}(\omega^{p_1(j_a+i)}) = \chi^u_P(\gamma^{j_a+i})$, by the assumption (iii), eq. (3.2) is rewritten as

$$\epsilon p_1 p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P^{-p_1^{e_1}v}) \sum_{i\in I} \chi_P^{p_1^{e_1}v}(\gamma^{j_a+i}). \tag{3.3}$$

For the remaining cases, we can assume that $p_1^{e_1} \not| u$, and write $u = kv_1 + v_2$ for some $0 \leq v_1 \leq p_1 - 1$ and $0 \leq v_2 \leq k-1$. Then, since $G_{f'}(\chi_{P'}^{kv_1+v_2}) = G_{f'}(\chi_{P'}^{kv_1'+v_2})$ for $0 \leq v_1, v_1' \leq p_1 - 1$, we have

$$\begin{aligned}
&\sum_{v_1=0}^{p_1-1} \sum_{v_2=1}^{k-1} G_{f'}(\chi_{P'}^{-kv_1-v_2}) \sum_{i\in I} \sum_{j=0}^{p_1-1} \chi_{P'}^{kv_1+v_2}(\omega^{a+ip_1+jk/p_1^{e_1}}) \\
= \;& p_1 \sum_{v_2=1}^{k-1} G_{f'}(\chi_{P'}^{-v_2}) \sum_{i\in I} \chi_{P'}^{v_2}(\omega^{p_1(j_a+i)}) \\
= \;& p_1 \sum_{v_2=1;\gcd(v_2,k)\in J_2}^{k-1} G_{f'}(\chi_{P'}^{-v_2}) \sum_{i\in I} \chi_{P'}^{v_2}(\omega^{p_1(j_a+i)}).
\end{aligned}$$

By our assumption that $G_{f'}(\chi_{P'}^{-v_2}) = \epsilon p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P^{-v_2})$ and by $\chi_{P'}^{v_2}(\omega^{p_1(j_a+i)}) = \chi_P^{v_2}(\gamma^{j_a+i})$, the above is equal to

$$\epsilon p_1 p^{\frac{\phi(k')-\phi(k)}{2e}} \sum_{v_2=1;\gcd(v_2,k)\in J_2}^{k-1} G_f(\chi_P^{-v_2}) \sum_{i\in I} \chi_P^{v_2}(\gamma^{j_a+i}).$$

Finally, together with eq. (3.1) and (3.3), we obtain

$$kp_1 \cdot \psi'(\omega^a D') + p_1|I| = \epsilon p_1 p^{\frac{\phi(k')-\phi(k)}{2e}} \sum_{v_2=1}^{k-1} G_f(\chi_P^{-\ell_2}) \sum_{i\in I} \chi_P^{\ell_2}(\gamma^{j_a+i}).$$

Now, by the assumption that the size of the set

$$\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, k-1\}$$

is exactly two, we obtain the assertion. In particular, the two values in $\{\psi'(\omega^a D') \,|\, a = 0, 1, \ldots, q'-2\}$ are given as

$$\frac{1}{kp_1}(\epsilon p_1 p^{\frac{\phi(k)(p_1-1)}{2e}}(ks + |I|) - p_1|I|) = \epsilon p^{\frac{\phi(k)(p_1-1)}{2e}} s + \frac{|I|(\epsilon p^{\frac{\phi(k)(p_1-1)}{2e}} - 1)}{k}, \tag{3.4}$$

where $s = \psi(\gamma^a D)$ for some a. □

3.2 Strongly regular graphs

In this subsection, we write $k = \prod_{i=1}^{\ell} p_i^{e_i}$, where p_i are distinct odd primes and assume that p is a prime such that $\mathrm{ord}_k(p) = \phi(k)/e$. Furthermore, assume that $\langle p\rangle$ is again of index e modulo $k'(:= kp_1)$ and $\gcd(k', p-1) = 1$.

Theorem 3.3. *Let $h = p_1 \cdots p_m p_{m+1} \cdots p_\ell$ with all distinct odd primes p_i and $[(\mathbb{Z}/h\mathbb{Z})^* : \langle p\rangle] = e$. Furthermore, Let $k = p_1^{e_1} \cdots p_m^{e_m} p_{m+1}^{e_{m+1}} \cdots p_\ell^{e_\ell}$, where $e_i \geq 1$ for $1 \leq i \leq m$ and $e_i = 1$ for $m+1 \leq i \leq \ell$, and assume that $\langle p\rangle$ is again of index e modulo k. Let $q_1 = p^d$ and $q = p^f$, where $d = \phi(h)/e$ and $f = \phi(k)/e$. Put $h_j = \prod_{i\neq j} p_i$ for $1 \leq j \leq m$. Assume that there exists an integer s_j s.t. $p^{s_j} \equiv -1 \pmod{h_j}$ for $1 \leq j \leq m$. Let*

$$D := \bigcup_{i_1=0}^{p_1^{e_1-1}-1} \cdots \bigcup_{i_m=0}^{p_m^{e_m-1}-1} C_{i_1 n_1 + \cdots + i_m n_m}^{(k,q)},$$

where $n_j = \prod_{i\neq j} p_i^{e_i}$. If $\mathrm{Cay}(\mathbb{F}_{q_1}, C_0^{(h,q_1)})$ is an srg, then so does $\mathrm{Cay}(\mathbb{F}_q, D)$.

Proof: We will show by induction. Write

$$D = \bigcup_{i_1=0}^{p_1^{e_1-1}-1} \cdots \bigcup_{i_m=0}^{p_m^{e_m-1}-1} C_{i_1 n_1 + \cdots + i_m n_m}^{(k,q)}$$

and assume the size of the set $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\}$ is exactly two. We put

$$I = \bigcup_{i_1=0}^{p_1^{e_1-1}-1} \cdots \bigcup_{i_m=0}^{p_m^{e_m-1}-1} \{i_1 n_1 + \cdots + i_m n_m\}$$

in Theorem 3.2. Let J be the set of positive divisors of k not divisible by $p_1^{e_1}$,

$$J_1 = \{x \,|\, \exists i,\ 1 \leq i \leq m, \text{ s.t. } p_i^r \,||\, x, \text{ where } 1 \leq r \leq e_i - 1\} \subseteq J,$$

and $J_2 = J \setminus J_1$. Then, by the definition of I, it is clear that $\sum_{i\in I} \zeta_k^{ij} = 0$ for all $j \in J_1$.

Furthermore, since the assumption $p^{s_1} \equiv -1 \pmod{h_1}$ implies that p is semi-primitive modulo n_1, by Theorems 2.2, for $u = p_1^{e_1+1}v$ we have

$$G_{f'}(\chi_{P'}^{p_1^{e_1+1}v}) = p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P^{p_1^{e_1}v}).$$

Moreover, by Corollary 2.13, we have for any $a \in J_2$

$$G_{f'}(\chi_{P'}^{a}) = p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P^{a}).$$

Thus, the assumptions (i), (ii), and (iii) of Theorem 3.2 are satisfied. Now, by applying Theorem 3.2, the size of the set $\{\psi'(\gamma^a D') \,|\, a = 0, 1, \ldots, q'-2\}$ is exactly two, where

$$\begin{aligned} D' &= \bigcup_{j=0}^{p_1-1} \bigcup_{i_1=0}^{p_1^{e_1-1}-1} \cdots \bigcup_{i_m=0}^{p_m^{e_m-1}-1} C^{(kp_1,q')}_{p_1(i_1n_1+\cdots+i_mn_m)+jn_1} \\ &= \bigcup_{i=0}^{p_1^{e_1}-1} \bigcup_{i_2=0}^{p_2^{e_2-1}-1} \cdots \bigcup_{i_m=0}^{p_m^{e_m-1}-1} C^{(kp_1,q')}_{in_1+i_2n'_2+\cdots+i_mn'_m} \end{aligned}$$

with $n'_i = n_ip_1$. □

Example 3.4. *(i) If $\ell = 1$ in Theorem 3.3, we do not need the condition that there exists an integer s_j s.t. $p^{s_j} \equiv -1 \pmod{h_j}$. Hence, assuming that*

$$[(\mathbb{Z}/p_1\mathbb{Z})^* : \langle p\rangle] = [(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* : \langle p\rangle] = e,$$

if $\mathrm{Cay}(\mathbb{F}_{p^{\phi(p_1)/e}}, C_0^{(p_1,p^{\phi(p_1)/e})})$ *forms an srg, then so does* $\mathrm{Cay}(\mathbb{F}_{p^{\phi(p_1^{e_1})/e}}, D)$*, where*

$$D = \bigcup_{i=0}^{p_1^{e_1-1}-1} C_i^{(p_1^{e_1},p^{\phi(p_1^{e_1})/e})}.$$

It is easy to see by induction that $\mathrm{ord}_{p_1^{e_1}}(p) = \phi(p_1^{e_1})/e$ *for general e and for all pairs $(k = p_1, p)$ of No. 1, 2, 4, 5, 6, 7, 9, and 11 in Table 1. Thus, all these srgs can be generalized into infinite families. Note that there are a lot of examples in subfield case satisfying* $[(\mathbb{Z}/p_1\mathbb{Z})^* : \langle p\rangle] = e$ *and* $p_1 = \frac{p^{\phi(p_1)/e}-1}{p^t-1}$ *for some $t \,|\, \phi(p_1)/e$. For example, we list ten examples satisfying these conditions in Table 2. These examples can be similarly generalized into nontrivial infinite families.*

(ii) If $\ell = 2$, in Theorem 3.3, we need the condition that there exists an integer s_i s.t. $p^{s_i} \equiv -1 \pmod{p_i}$ for either of $i = 1, 2$. Hence, assuming that p is semi-primitive modulo both of p_1 and p_2, and

$$[(\mathbb{Z}/p_1p_2\mathbb{Z})^* : \langle p\rangle] = [(\mathbb{Z}/p_1^{e_1}p_2^{e_2}\mathbb{Z})^* : \langle p\rangle] = e,$$

if $\mathrm{Cay}(\mathbb{F}_{p^{\phi(p_1p_2)/e}}, C_0^{(p_1p_2,p^{\phi(p_1p_2)/e})})$ *forms an srg, then so does* $\mathrm{Cay}(\mathbb{F}_{p^{\phi(p_1^{e_1}p_2^{e_2})/e}}, D)$*, where*

$$D = \bigcup_{i=0}^{p_1^{e_1-1}-1} \bigcup_{j=0}^{p_2^{e_2-1}-1} C^{(p_1^{e_1}p_2^{e_2},p^{\phi(p_1^{e_1}p_2^{e_2})/e})}_{i_1p_2^{e_2}+i_2p_1^{e_1}}.$$

It is easy to see by induction that $\mathrm{ord}_{p_1^{e_1}p_2^{e_2}}(p) = \phi(p_1^{e_1}p_2^{e_2})/e$ *for any e_1, e_2 and for pairs $(k = p_1p_2, p)$ of No. 3 and 10 in Table 1. Thus, these srgs can be generalized into infinite families. On the other hand, if p is semi-primitive modulo either one of p_1 or p_2, say p_2,*

Table 2: Subfield examples of $\ell = 1$ led to infinite families

p_1	p	f	$e := [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$
7	2	2	2
13	3	3	4
31	2	5	6
31	5	3	10
73	2	9	8
127	2	7	18
307	17	3	102
757	3	9	84
1093	3	7	156
1723	41	3	574

then $\mathrm{Cay}(\mathbb{F}_{p^{\phi(p_1^{e_1}p_2)/e}}, D)$ *forms an srg under the assumption that* $[(\mathbb{Z}/p_1^{e_1}p_2\mathbb{Z})^* : \langle p \rangle] = e$, *where*

$$D = \bigcup_{i=0}^{p_1^{e_1-1}-1} C_{i_1 p_2}^{(p_1^{e_1}p_2, p^{\phi(p_1^{e_1}p_2)/e})}.$$

It is easy to see by induction that $\mathrm{ord}_{p_1^{e_1}p_2}(p) = \phi(p_1^{e_1}p_2)/e$ *for any* e_1 *and* p *is semi-primitive modulo* p_2 *for the triple* $(p_1, p_2, p) = (19, 7, 5)$ *of No. 8 in Table 1. Thus, this srg can be generalized into infinite families. Moreover, we can find some examples in subfield case satisfying* $[(\mathbb{Z}/p_1p_2\mathbb{Z})^* : \langle p \rangle] = e$ *and* $p_1p_2 = \frac{p^{\phi(p_1p_2)/e}-1}{p^t-1}$ *for some* $t \mid \phi(p_1p_2)/e$. *For example, we list four examples satisfying these conditions in Table 3. In the sixth column "sp" of the*

Table 3: Subfield examples of $\ell = 2$ led to infinite families

p_1	p_2	p	f	$e := [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$	sp
3	5	2	4	2	b
5	17	2	8	8	b
31	11	2	10	30	o
127	43	2	14	378	o

table, "b" indicates that p *is semi-primitive modulo both of* p_1 *and* p_2, *and "o" indicates that* p *is semi-primitive modulo* p_2 *only. These examples can be generalized into nontrivial infinite families.*

3.3 Skew Hadamard difference sets

In this subsection, we write $k = 2p_1^{e_1}$, where p_1 is an odd prime and assume that p is a prime such that $\mathrm{ord}_k(p) = \phi(k)/e$. Furthermore, assume that p is again of index e modulo $k'(:= kp_1)$ and $\gcd(k'/2, p-1) = 1$.

Theorem 3.5. *Let* $h = 2p_1$ *with an odd prime* p_1 *and let* p *be a prime such that* $\langle p \rangle$ *is of index* e *modulo* h. *Furthermore, let* $k = 2p_1^{e_1}$ *and assume that* $\langle p \rangle$ *is again of index* e *modulo* k. *Put* $q_1 = p^d$ *and* $q = p^f$, *where* $d = \phi(h)/e$ *and* $f = \phi(k)/e$. *Define* H *as any subset of* $\{0, 1, \ldots, h-1\}$ *such that* $\sum_{i \in H} \zeta_{p_1}^i = 0$. *Let*

$$D = \bigcup_{i \in H} C_i^{(h,q_1)} \quad \text{and} \quad D' = \bigcup_{i_1=0}^{p_1^{e_1-1}} \bigcup_{i \in H} C_{2i_1+ik/h}^{(k,q)}.$$

If D is a skew Hadamard difference set or a Paley type regular partial difference set on $\mathbb{F}_{q_1}$, then so does D' on $\mathbb{F}_q$.

Proof: We will show by induction. Write

$$D = \bigcup_{i_1=0}^{p_1^{e_1-1}} \bigcup_{i\in H} C^{(k,q)}_{2i_1+ik/h}$$

and assume that the size of the set $\{\psi(\gamma^a D) \,|\, a = 0, 1, \ldots, q-2\}$ is exactly two, which are $\frac{-1\pm\sqrt{\tau q}}{2}$, where $\tau = 1$ or -1 according as D is a Paley type regular partial difference set or a skew Hadamard difference set. Now, we put

$$I = \bigcup_{i_1=0}^{p_1^{e_1-1}-1} \bigcup_{i\in H} \{2i_1 + ik/h\}$$

in Theorem 3.2. Let

$$J_2 = \{1\} \subseteq J = \{1, p_1, \ldots, p_1^{e-1}\} \cup 2\{1, p_1, \ldots, p_1^{e-1}\}$$

and $J_1 = J \setminus J_2$. Then, by the definition of I, it is clear that $\sum_{i\in I} \zeta_k^{ij} = 0$ for all $j \in J_1$. By Lemma 2.1, we have

$$G_{f'}(\chi_{P'}^{k'/2}) = (-1)^{\frac{(p-1)(p_1-1)\phi(h)}{4e}} p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P^{k/2}).$$

Furthermore, by Corollary 2.11, we have

$$G_{f'}(\chi_{P'}) = (-1)^{\frac{(p-1)(p_1-1)\phi(h)}{4e}} p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P).$$

Thus, the assumptions (i), (ii), and (iii) of Theorem 3.2 are satisfied. Now, by applying Theorem 3.2, the size of the set $\{\psi'(\gamma^a D') \,|\, a = 0, 1, \ldots, q'-2\}$ is exactly two, where

$$\begin{aligned} D' &= \bigcup_{j=0}^{p_1-1} \bigcup_{i_1=0}^{p_1^{e_1-1}} \bigcup_{i\in H} C^{(k,q)}_{(2i_1+ik/h)p_1+jk/p_1^{e_1}} \\ &= \bigcup_{i_1=0}^{p_1^{e_1}-1} \bigcup_{i\in H} C^{(k,q)}_{2i_1+ik'/h}. \end{aligned}$$

In particular, by eq. (3.4), the two values in $\{\psi'(\gamma^a D') \,|\, a = 0, 1, \ldots, q'-2\}$ are

$$\epsilon p^{\frac{\phi(k)(p_1-1)}{2e}} \left(\frac{-1 \pm \sqrt{\tau p^f}}{2}\right) + \frac{k}{2} \cdot \left(\frac{\epsilon p^{\frac{\phi(k)(p_1-1)}{2e}} - 1}{k}\right) = \frac{-1 \pm \epsilon\sqrt{\tau p^{f'}}}{2},$$

which completes the proof. □

Example 3.6. *In [11], several examples satisfying the condition of Theorem 3.5 were found from index 2 case, which were generalized into infinite families using Gauss sums of index 2. We can find by computer further two examples having the following parameters from index 4 case:*

$$(p_1, p, f, e) = (13, 3, 3, 4) \text{ and } (29, 7, 7, 4).$$

In particular, the latter example was found by Tao Feng [12]. We choose H in Theorem 3.5 as $H = Q \cup 2Q \cup \{p_1\}$ for the former parameter and choose $H = Q \cup 2Q \cup \{0\}$ for the latter parameter, where Q is the subgroup of index 2 of $(\mathbb{Z}/2p_1\mathbb{Z})^*$. It is easy to check that these H satisfies the condition of Theorem 3.5 and $\langle p\rangle$ is of index 4 in $(\mathbb{Z}/2p_1^{e_1}\mathbb{Z})^*$ for general e_1. Hence, these examples can be generalized into infinite families.

4 Final remarks

We close this paper by referring the reader to the interesting paper [27] by Wu. Immediately after writing up this manuscript, the author became aware that Wu [27] obtained a nice result on the existence problem of cyclotomic srgs.

In our paper, cyclotomic constructions of strongly regular Cayley graphs and skew Hadamard difference sets on $\mathbb{F}_q$ were given. For example, we proved the following result (which follows from the more general theorem 3.3): For an odd prime p_1, assume that (i) $\gcd(p(p-1), p_1) = 1$ (ii) $\langle p \rangle$ is of index e modulo p_1 (iii) $\mathrm{Cay}(\mathbb{F}_{p^{(p_1-1)/e}}, C_0^{(p^{(p_1-1)/e}, p_1)})$ is strongly regular. Then, if $\langle p \rangle$ is of index e modulo p_1^m, $\Gamma = \mathrm{Cay}(\mathbb{F}_{p^{p_1^{m-1}(p_1-1)/e}}, \bigcup_{i=0}^{p_1^{m-1}-1} C_i^{(p^{p_1^{m-1}(p_1-1)/e}, p_1^m)})$ is also strongly regular. Since there are a lot of subfield or sporadic examples satisfying the assumption of this result, we consequently obtain many new infinite families of strongly regular Cayley graphs. This result can be viewed as a "recursive" construction of srgs not saying anything about the existence of "starting" srgs.

On the other hand, Wu [27] gave necessary and sufficient conditions for Γ to be an srg by generalizing the method used in the paper of Ge, Xiang, and Yuan [13]. Although it seems that the assumptions of our main result are simpler and the situation is definitely much more general than that of [27], the approach in [27] is obviously different from ours and his results are not completely included in ours. In fact, Wu [27] obtained two conditions (one is an equation and the other is a congruence) which are necessary and sufficient for the construction to give rise to an srg, and his approach has the advantage of revealing an interesting connection between strongly regular Cayley graphs $\mathrm{Cay}(\mathbb{F}_{p^{(p_1-1)/e}}, C_0^{(p^{(p_1-1)/e}, p_1)})$ and cyclic difference sets in $(\mathbb{Z}/p_1\mathbb{Z}, +)$, which will be very effective to get some new cyclic difference sets and also a strong necessary condition for the existence of cyclotomic srgs.

Acknowledgements

The work of K. Momihara was supported by JSPS under Grant-in-Aid for Research Activity start-up 23840032.

References

[1] L. D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, *DSN Progr. Rep.,* **16** (1973), 128–131.

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

[3] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.

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

[5] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, course notes, available at `http://homepages.cwi.nl/~aeb/math/ipm.pdf`

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

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

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

[9] T. Feng, Q. Xiang, Strongly regular graphs from union of cyclotomic classes, to appear in *J. Combin. Theory* (B).

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

[11] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, ArXiv: 1201.0701.

[12] T. Feng, Private communication.

[13] G. Ge, Q. Xiang, T. Yuan, Construction of strongly regular Cayley graphs using index four Gauss sums, ArXiv: 1201.0702.

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

[15] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory,* 2*nd ed.,* Graduate Texts in Mathematics 84,

[16] P. Langevin, Calcus de certaines sommes de Gauss, 1990. *J. Number Theory*, **63** (1997), 59–64.

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

[18] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.

[19] 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.

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

[21] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields Appl.,* **4** (1998), 347–361.

[22] 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).

[23] P. Meijer, M. van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, *J. Number Theory*, **100** (2003), 381–395.

[24] B. Schmidt, C. White, All two-weight irreducible cyclic codes, *Finite Fields Appl.,* **8** (2002), 321–367.

[25] T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, Markham Publishing Company, 1967.

[26] R. J. Turyn, Character sums and difference sets, *Pacific J. Math.,* **15** (1965), 319–346.

[27] F. Wu, Constructions of strongly regular graphs using even index Gauss sums, preprint.

[28] K. Yamamoto, On congruences arising from relative Gauss sums, in: *Number Theory and Combinatorics, Japan, 1984*, World Scientific Pub., 1985, pp. 423–446.

[29] J. Yang, S. X. Luo, K. Q. Feng, Gauss sums of index 4: (1) non-cyclic case, *Acta Math. Sin. (Engl. Ser.),* **22** (2006), 833–844.

[30] 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.

[31] J. Yang, L. Xia, A note on the sign (unit root) ambiguities of Gauss sums in the index 2 and 4 case, ArXiv: 0912.1414v1.