

# STRONGLY REGULAR CAYLEY GRAPHS FROM PARTITIONS OF SUBDIFFERENCE SETS OF THE SINGER DIFFERENCE SETS

KOJI MOMIHARA\*, QING XIANG†

ABSTRACT. In this paper, we give a new lifting construction of “hyperbolic” type of strongly regular Cayley graphs. Also we give new constructions of strongly regular Cayley graphs over the additive groups of finite fields based on partitions of subdifference sets of the Singer difference sets. Our results unify some recent constructions of strongly regular Cayley graphs related to  $m$ -ovoids and  $i$ -tight sets in finite geometry. Furthermore, some of the strongly regular Cayley graphs obtained in this paper are new or nonisomorphic to known strongly regular graphs with the same parameters.

## 1. INTRODUCTION

We assume that the reader is familiar with the basic theory of strongly regular graphs and difference sets. For strongly regular graphs (srgs), our main references are [3] and [9]. For difference sets, we refer the reader to [10] and Chapter 6 of [2]. Strongly regular graphs are closely related to many other combinatorial/geometric objects, such as two-weight codes, two-intersection sets,  $m$ -ovoids,  $i$ -tight sets, and partial difference sets. For these connections, we refer the reader to [3, p. 132], [5, 12], and some more recent papers [7, 6, 4] on Cameron-Liebler line classes and hemisystems.

Let  $\Gamma$  be a (simple, undirected) graph. The adjacency matrix of  $\Gamma$  is the  $(0, 1)$ -matrix  $A$  with both rows and columns indexed by the vertex set of  $\Gamma$ , where  $A_{xy} = 1$  when there is an edge between  $x$  and  $y$  in  $\Gamma$  and  $A_{xy} = 0$  otherwise. 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  $\Gamma$  of order  $v$ , not complete or edgeless, with adjacency matrix  $A$ , the following are equivalent:*

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

For a proof of Theorem 1.1, we refer the reader to [3]. An effective method to construct strongly regular graphs is by using Cayley graphs. 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 over  $G$  with connection set  $D$* , denoted  $\text{Cay}(G, D)$ , 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  $\text{Cay}(G, D)$  is a strongly regular graph, the connection set  $D$  is called a (regular) *partial difference set*. Examples of strongly regular Cayley graphs are the Paley graphs  $P(q)$ , where  $q$  is a prime power congruent to 1 modulo 4, the Clebsch graph, and the affine orthogonal graphs ([3]). For  $\Gamma = \text{Cay}(G, D)$  with  $G$  abelian, the eigenvalues of  $\Gamma$  are exactly  $\chi(D) := \sum_{d \in D} \chi(d)$ , where  $\chi$  runs through the character group of  $G$ . This fact reduces the problem of computing eigenvalues of abelian Cayley graphs to that

---

*Key words and phrases.* Affine polar graph,  $i$ -tight set,  $m$ -ovoid, quadratic form, Singer difference set, strongly regular graph, subdifference set.

\*Research supported by JSPS under Grant-in-Aid for Young Scientists (B) 17K14236 and Scientific Research (B) 15H03636.

†Research partially supported by an NSF grant DMS-1600850.

of computing some character sums, and is the underlying reason why the Cayley graph construction has been very effective for the purpose of constructing srgs. The survey of Ma [12] contains much of what is known about partial difference sets and about connections with strongly regular graphs.

A  $(v, k, \lambda, \mu)$  srg is said to be of *Latin square type* (respectively, *negative Latin square type*) if  $(v, k, \lambda, \mu) = (n^2, r(n - \epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$  and  $\epsilon = 1$  (respectively,  $\epsilon = -1$ ). When  $v$  (the number of vertices) is a prime power, many constructions of srgs with Latin square or negative Latin square type parameters are known. For example, the srgs arising from partial spreads of  $\text{PG}(2m-1, q)$  have Latin square parameters, and the affine orthogonal graphs,  $\text{VO}^-(2m, q)$ , have negative Latin square type parameters. Still the range of  $r$  in the parameters  $(n^2, r(n - \epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$  of the known srgs of Latin square or negative Latin square type can sometimes be limited; moreover Latin square and negative Latin square type strongly regular Cayley graphs with certain extra properties<sup>1</sup> have found many connections with finite geometric objects such as  $m$ -ovoids and  $i$ -tight sets (cf. [7, 6, 4]). Therefore it is of interest to construct more strongly regular Cayley graphs of Latin square or negative Latin square type. The purpose of the current paper is two fold. First, we give new constructions of strongly regular Cayley graphs, and obtain some new srgs. Secondly, we unify and give simpler proofs for some recent constructions of strongly regular Cayley graphs.

The paper is organized as follows. In Section 2, we review some basic properties of Gauss sums which will be used in later sections. In Section 3, we give two constructions of strongly regular Cayley graphs on the additive group of  $\mathbb{F}_{q^2}$  by lifting a cyclotomic strongly regular graph on  $\mathbb{F}_q$ . The first lifting construction (Proposition 3.2) is of “elliptic” type, and it was already given in [15]. The second lifting construction (Proposition 3.4) is of “hyperbolic” type, and this construction is new. In Section 4, we generalize and unify the constructions of strongly regular Cayley graphs corresponding to  $m$ -ovoids and  $i$ -tight sets in [7, 4]. We give a general construction of strongly regular Cayley graphs by using a certain partition of a subdifference set (and its complement) of the Singer difference set. When the subdifference sets arise from subfields, we recover the results in [7, 4]. In Sections 5, 6, and 7, we apply the general construction in Section 4 to the three known cases of subdifference sets of the Singer difference sets, namely, the semiprimitive case, the sporadic case, and the subfield case. We either recover strongly regular Cayley graphs constructed in some of our recent papers [14, 7, 4], or we produce new strongly regular Cayley graphs. In particular, Corollaries 7.7 and 7.9 give strongly regular Cayley graphs with the same parameters as the affine polar graphs. By using a computer, it is shown that the newly constructed graphs in Corollaries 7.7 and 7.9 are not isomorphic to the affine polar graphs when the parameters are small.

## 2. PRELIMINARIES

We will use Gauss sums and Gauss periods to compute character values of certain subsets of  $\mathbb{F}_q$ , the finite field of order  $q$ . So it is helpful to introduce characters of both kinds of finite fields, and review basic properties of Gauss sums. Let  $p$  be a prime,  $f$  a positive integer, and  $q = p^f$ . The canonical additive character  $\psi_{\mathbb{F}_q}$  of  $\mathbb{F}_q$  is defined by

$$\psi_{\mathbb{F}_q} : \mathbb{F}_q \rightarrow \mathbb{C}^*, \quad \psi_{\mathbb{F}_q}(x) = \zeta_p^{\text{Tr}_{q/p}(x)},$$

where  $\zeta_p = \exp(\frac{2\pi i}{p})$  is a complex primitive  $p$ -th root of unity and  $\text{Tr}_{q/p}$  is the trace function from  $\mathbb{F}_q$  to  $\mathbb{F}_p$  defined by  $\text{Tr}_{q/p}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{f-1}}$ . All the additive characters of  $\mathbb{F}_q$  can be obtained from the canonical one. For  $a \in \mathbb{F}_q$ , define

$$\psi_a(x) = \psi_{\mathbb{F}_q}(ax), \quad \forall x \in \mathbb{F}_q. \quad (2.1)$$

<sup>1</sup>For example, the elements of the connection set must all lie on a quadratic surface.

Then  $\{\psi_a \mid a \in \mathbb{F}_q\}$  is the group of additive characters of  $\mathbb{F}_q$ . For a multiplicative character  $\chi$  and the canonical additive character  $\psi_{\mathbb{F}_q}$  of  $\mathbb{F}_q$ , define the *Gauss sum* by

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

Some basic properties of Gauss sums are listed below:

**Proposition 2.1.** ([11, Theorem 5.2]) *Let  $\chi$  be a multiplicative character of  $\mathbb{F}_q$ . Then, the following hold:*

- (i)  $G_q(\chi) \overline{G_q(\chi)} = q$  if  $\chi$  is nontrivial;
- (ii)  $G_q(\chi^p) = G_q(\chi)$ , where  $p$  is the characteristic of  $\mathbb{F}_q$ ;
- (iii)  $G_q(\chi^{-1}) = \chi(-1) \overline{G_q(\chi)}$ ;
- (iv)  $G_q(\chi) = -1$  if  $\chi$  is trivial.

Let  $\omega$  be a fixed primitive element of  $\mathbb{F}_q$  and  $N$  a positive integer dividing  $q-1$ . For  $0 \leq i \leq N-1$  we set  $C_i^{(N,q)} = \omega^i C_0$ , where  $C_0$  is the subgroup of index  $N$  of  $\mathbb{F}_q^*$ . The *Gauss periods* associated with these cosets are defined by  $\psi_{\mathbb{F}_q}(C_i^{(N,q)}) := \sum_{x \in C_i^{(N,q)}} \psi_{\mathbb{F}_q}(x)$ ,  $0 \leq i \leq N-1$ , where  $\psi_{\mathbb{F}_q}$  is the canonical additive character of  $\mathbb{F}_q$ . By orthogonality of characters, the Gauss periods can be expressed as a linear combination of Gauss sums:

$$\psi_{\mathbb{F}_q}(C_i^{(N,q)}) = \frac{1}{N} \sum_{j=0}^{N-1} G_q(\chi^j) \chi^{-j}(\omega^i), \quad 0 \leq i \leq N-1, \quad (2.2)$$

where  $\chi$  is any fixed multiplicative character of order  $N$  of  $\mathbb{F}_q$ . For example, if  $N=2$ , we have

$$\psi_{\mathbb{F}_q}(C_i^{(2,q)}) = \frac{-1 + (-1)^i G_q(\eta)}{2}, \quad 0 \leq i \leq 1, \quad (2.3)$$

where  $\eta$  is the quadratic character of  $\mathbb{F}_q$ .

The quadratic Gauss sum,  $G_q(\eta)$ , can be evaluated explicitly.

**Theorem 2.2.** [11, Theorem 5.15] *Let  $q = p^s$  be a prime power with  $p$  a prime and  $\eta$  be the quadratic character of  $\mathbb{F}_q$ . Then,*

$$G_q(\eta) = \begin{cases} (-1)^{s-1} q^{1/2} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{s-1} i^s q^{1/2} & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (2.4)$$

Also, in the semi-primitive case, the Gauss sum can be computed.

**Theorem 2.3.** ([1, Theorem 11.6.3]) *Let  $p$  be a prime. Suppose that  $N > 2$  and  $p$  is semi-primitive modulo  $N$ , i.e., there exists a positive integer  $j$  such that  $p^j \equiv -1 \pmod{N}$ . Choose  $j$  minimal and write  $f = 2js$  for any positive integer  $s$ . Let  $\chi$  be a multiplicative character of order  $N$  of  $\mathbb{F}_{p^f}$ . Then,*

$$p^{-f/2} G_{p^f}(\chi) = \begin{cases} (-1)^{s-1}, & \text{if } p = 2, \\ (-1)^{s-1+(p^j+1)s/N}, & \text{if } p > 2. \end{cases}$$

The following theorems are referred to as the *Davenport-Hasse lifting formula* and the *Davenport-Hasse product formula*, respectively.

**Theorem 2.4.** ([11, Theorem 5.14]) *Let  $m$  be a positive integer. Let  $\chi$  be a nontrivial multiplicative character of  $\mathbb{F}_q$  and  $\chi'$  be the lift of  $\chi$  to  $\mathbb{F}_{q^m}$ , i.e.,  $\chi'(x) = \chi(\text{Norm}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x))$  for  $x \in \mathbb{F}_{q^m}$ , where  $\text{Norm}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$  is the norm from  $\mathbb{F}_{q^m}$  to  $\mathbb{F}_q$ . Then,*

$$G_{q^m}(\chi') = (-1)^{m-1} G_q(\chi)^m.$$

**Theorem 2.5.** ([1, Theorem 11.3.5]) *Let  $\eta$  be a multiplicative character of order  $\ell > 1$  of  $\mathbb{F}_q$ . For every nontrivial multiplicative character  $\chi$  of  $\mathbb{F}_q$ ,*

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

We will use the following formula later.

**Theorem 2.6.** ([11, Theorem 5.33]) *Let  $\psi_{\mathbb{F}_q}$  be the canonical additive character of  $\mathbb{F}_q$  with  $q$  odd, and let  $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$  with  $a_2 \neq 0$ . Then*

$$\sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(f(x)) = \psi_{\mathbb{F}_q}(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G_q(\eta),$$

where  $\eta$  is the quadratic character of  $\mathbb{F}_q$ .

### 3. BASIC LIFTING CONSTRUCTIONS

**3.1. Subdifference sets of the Singer difference sets.** Let  $p$  be a prime,  $f \geq 1$ ,  $m \geq 2$  be integers and  $q = p^f$ . Let  $L$  be a complete system of coset representatives of  $\mathbb{F}_q^*$  in  $\mathbb{F}_{q^m}^*$ . We can, and do, choose  $L$  in such a way that  $\text{Tr}_{q^m/q}(x) = 0$  or 1 for any  $x \in L$ . Let

$$L_0 = \{x \in L \mid \text{Tr}_{q^m/q}(x) = 0\} \text{ and } L_1 = \{x \in L \mid \text{Tr}_{q^m/q}(x) = 1\}.$$

Then,

$$H_0 = \{\bar{x} \in \mathbb{F}_{q^m}^*/\mathbb{F}_q^* \mid x \in L_0\}$$

represents a hyperplane of the projective space  $\text{PG}(m-1, q)$ , and it is a so-called *Singer difference set* in the cyclic group  $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ . (Here  $\bar{x} = x\mathbb{F}_q^*$  represents the projective point corresponding to the one-dimensional subspace over  $\mathbb{F}_q$  spanned by  $x$ .)

Any nontrivial multiplicative character  $\chi$  of exponent  $(q^m - 1)/(q - 1)$  of  $\mathbb{F}_{q^m}^*$  induces a character of the quotient group  $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ , which will also be denoted by  $\chi$ . Moreover, every character of  $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$  arises in this way. By a result given in [17], for any nontrivial multiplicative character  $\chi$  of exponent  $(q^m - 1)/(q - 1)$  of  $\mathbb{F}_{q^m}^*$ , we have

$$\chi(H_0) = G_{q^m}(\chi)/q.$$

Assume that  $N \mid (q^m - 1)/(q - 1)$ . Then

$$\overline{C_0} := C_0^{(N, q^m)}/\mathbb{F}_q^* \leq \mathbb{F}_{q^m}^*/\mathbb{F}_q^*.$$

Let  $S$  be a complete system of coset representatives of  $\overline{C_0}$  in  $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ , and set  $G = \{s\overline{C_0} \mid s \in S\} \simeq \mathbb{F}_{q^m}^*/C_0^{(N, q^m)}$ . For convenience, we will use  $\tilde{s}$  to denote  $s\overline{C_0}$ .

In the rest of this section, we will assume that  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular, where  $N \mid (q^m - 1)/(q - 1)$ . Such a strongly regular graph is called *cyclotomic*. The following three series of cyclotomic strongly regular graphs were known [16]:

- (1) (subfield case)  $C_0^{(N, q^m)} = \mathbb{F}_{q^d}^*$  where  $d \mid m$ ,
- (2) (semi-primitive case)  $-1 \in \langle p \rangle \leq (\mathbb{Z}/N\mathbb{Z})^*$ ,
- (3) (sporadic case)  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  has one of the eleven sets of parameters given in Table 1.

TABLE 1. Eleven sporadic examples

|       |       |       |          |       |        |           |          |          |           |           |           |
|-------|-------|-------|----------|-------|--------|-----------|----------|----------|-----------|-----------|-----------|
| $N$   | 11    | 19    | 35       | 37    | 43     | 67        | 107      | 133      | 163       | 323       | 499       |
| $q^m$ | $3^5$ | $5^9$ | $3^{12}$ | $7^9$ | $11^7$ | $17^{33}$ | $3^{53}$ | $5^{18}$ | $41^{81}$ | $3^{144}$ | $5^{249}$ |

We mention in passing that Schmidt and White [16] conjectured that besides the above three cases, there are no more cyclotomic strongly regular graphs.

**Conjecture 3.1.** *Let  $N \mid \frac{q^m-1}{q-1}$  with  $N > 1$ . If  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular, then one of (1), (2), or (3) above holds.*

This conjecture remains open. Some partial results were obtained in [16].

Assume that  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular, where  $N \mid \frac{q^m-1}{q-1}$ . Then  $|H_0 \cap s\overline{C_0}|$ ,  $s \in S$ , take exactly two values. It follows that  $|H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}| = 0$  or  $\delta$ , where  $\delta$  is a nonzero integer. For any nontrivial multiplicative character  $\chi$  of  $\mathbb{F}_{q^m}$  of exponent  $N$ ,

$$\begin{aligned} \chi(H_0) &= \sum_{s \in S} |H_0 \cap s\overline{C_0}| \chi(\tilde{s}) \\ &= \sum_{s \in S} (|H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}|) \chi(\tilde{s}) \\ &= \delta \sum_{s \in S'} \chi(\tilde{s}), \end{aligned}$$

where

$$S' = \{s \in S : |H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}| = \delta\}. \quad (3.1)$$

Thus

$$\sum_{s \in S'} \chi(\tilde{s}) = \frac{\chi(H_0)}{\delta} = \frac{G_{q^m}(\chi)}{\delta q}. \quad (3.2)$$

It follows that  $\delta$  is a power of  $p$ . Furthermore, noting that  $G_{q^m}(\chi)\overline{G_{q^m}(\chi)} = q^m$ , we see that the set  $\{\tilde{s} \mid s \in S'\} \subset G$  forms a difference set, which is called a *subdifference set* of  $H_0$  [13]. Let  $\omega$  be a primitive element of  $\mathbb{F}_{q^m}$ . Then we could choose  $S = \{\overline{1}, \overline{\omega}, \dots, \overline{\omega^{N-1}}\}$ , where  $\overline{\omega} = \omega\mathbb{F}_q^*$ . In this way, since  $S'$  is a subset of  $S$ , we define

$$I = \{0 \leq i \leq N-1 \mid \overline{\omega^i} \in S'\}. \quad (3.3)$$

In the rest of the paper, we will also call  $I$  a subdifference set in  $\mathbb{Z}_N$  of the Singer difference set.

**3.2. Two lifting constructions.** Let  $\gamma$  be a primitive element of  $\mathbb{F}_{q^{2m}}$  and set  $\omega = \gamma^{q^m+1}$ . Then,  $\omega$  is a primitive element in  $\mathbb{F}_{q^m}$ . Let  $C_j^{(N, q^{2m})} = \gamma^j \langle \gamma^N \rangle$ ,  $0 \leq j \leq N-1$ . The following lifting construction was already given in [15]. For completeness, we repeat the construction here.

**Proposition 3.2.** *Assume that  $\mathbb{F}_q^* \leq C_0^{(N, q^m)} \leq \mathbb{F}_{q^m}^*$  and  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular. Let  $I$  be the corresponding subdifference set defined in (3.3). Let*

$$E = \bigcup_{i \in I} C_i^{(N, q^{2m})}. \quad (3.4)$$

*Then  $\text{Cay}(\mathbb{F}_{q^{2m}}, E)$  is a strongly regular graph with negative Latin square type parameters  $(n^2, r(n+1), -n+r^2+3r, r^2+r)$ , where  $n = q^m$  and  $r = (q^m-1)|I|/N$ .*

**Proof:** Let  $\psi_{\mathbb{F}_{q^{2m}}}$  be the canonical additive character of  $\mathbb{F}_{q^{2m}}$  and let  $\chi'_N$  be a multiplicative character of order  $N$  of  $\mathbb{F}_{q^{2m}}$ . We will show that  $\psi_{\mathbb{F}_{q^{2m}}}(\gamma^a E)$ ,  $0 \leq a \leq N-1$ , take exactly two distinct values. By the orthogonality of characters, we compute

$$S_a = N \cdot \psi_{\mathbb{F}_{q^{2m}}}(\gamma^a E) + |I| = \sum_{j=1}^{N-1} G_{q^{2m}}(\chi_N'^{-j}) \sum_{i \in I} \chi_N'^j(\gamma^{a+i}).$$

Since  $N \mid \frac{q^m-1}{q-1}$ , there is a multiplicative character  $\chi_N$  of  $\mathbb{F}_{q^m}$  of order  $N$  such that  $\chi'_N(\gamma) = \chi_N(\omega)$ , i.e.,  $\chi'_N$  is the lift of  $\chi_N$ . By the Davenport-Hasse lifting formula, we have

$$S_a = - \sum_{j=1}^{N-1} \chi_N^j(\omega^a) G_{q^m}(\chi_N^{-j}) G_{q^m}(\chi_N^{-j}) \sum_{i \in I} \chi_N^j(\omega^i).$$

On the other hand, from the definition of  $I$ , we have

$$\sum_{i \in I} \chi_N^j(\omega^i) = \sum_{s \in S'} \chi_N^j(\bar{s}) = \frac{G_{q^m}(\chi_N^j)}{\delta q}. \quad (3.5)$$

Hence,

$$\begin{aligned} S_a &= -\frac{1}{\delta q} \sum_{j=1}^{N-1} \chi_N^j(\omega^a) G_{q^m}(\chi_N^{-j}) G_{q^m}(\chi_N^{-j}) G_{q^m}(\chi_N^j) \\ &= -\frac{q^{m-1}}{\delta} \sum_{j=1}^{N-1} \chi_N^j(\omega^a) G_{q^m}(\chi_N^{-j}) \\ &= -q^m \sum_{j=1}^{N-1} \sum_{i \in I} \chi_N^{-j}(\omega^i) \chi_N^j(\omega^a) = q^m |I| - \begin{cases} q^m N, & \text{if } a \in I, \\ 0, & \text{if } a \notin I. \end{cases} \end{aligned}$$

Thus,  $\psi_{\mathbb{F}_{q^{2m}}}(\gamma^a E) = \frac{S_a - |I|}{N}$ ,  $0 \leq a \leq N-1$ , take exactly two distinct values  $\frac{(q^m-1)|I|}{N}$  and  $\frac{(q^m-1)|I|}{N} - q^m$ . Therefore  $\text{Cay}(\mathbb{F}_{q^{2m}}, E)$  is strongly regular. The parameters of  $\text{Cay}(\mathbb{F}_{q^{2m}}, E)$  can be computed in a straightforward way. We omit the details.  $\square$

**Remark 3.3.** If  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is a cyclotomic strongly regular graph in the subfield case with  $N = \frac{q^m-1}{q-1}$ , then  $C_0^{(N, q^m)} = \mathbb{F}_q^*$ ,  $S = \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ , and  $S' = H_0$ . In this case, we find that

$$E = \{x \in \mathbb{F}_{q^{2m}}^* \mid \text{Tr}_{q^m/q}(x^{q^m+1}) = 0\},$$

where  $\text{Tr}_{q^m/q}(x^{q^m+1})$  is a nondegenerate  $\mathbb{F}_q$ -valued elliptic quadratic form on  $\mathbb{F}_{q^{2m}}$ . Therefore it is appropriate to call the lifting construction given in Proposition 3.2 an *elliptic* type lifting construction.

We give a new lifting construction, which is of ‘‘hyperbolic’’ type.

**Proposition 3.4.** *Let  $\omega$  be a primitive element of  $\mathbb{F}_{q^m}$ . Assume that  $\mathbb{F}_q^* \leq C_0^{(N, q^m)} \leq \mathbb{F}_{q^m}^*$  and  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular. Let  $I$  be the corresponding subdifferecne set defined in (3.3). Let*

$$H = \{(y, y^{-1}x\omega^\ell) \mid x \in C_0^{(N, q^m)}, y \in \mathbb{F}_{q^m}^*, \ell \in I\} \subseteq \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}. \quad (3.6)$$

*Then  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H)$  is a strongly regular graph with Latin square type parameters  $(n^2, r(n-1), n+r^2-3r, r^2-r)$ , where  $n = q^m$  and  $r = (q^m-1)|I|/N$ .*

**Proof:** Let  $\psi_{\mathbb{F}_{q^m}}$  be the canonical additive character of  $\mathbb{F}_{q^m}$  and let  $\chi_{q^m-1}$  be a multiplicative character of order  $q^m-1$  of  $\mathbb{F}_{q^m}$ . Each additive character of  $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$  has the form

$$\psi_{a,b}((x, y)) = \psi_{\mathbb{F}_{q^m}}(ax + by), \quad (x, y) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, \quad (3.7)$$

where  $(a, b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ . Then, by the definition of  $H$ , we need to compute the character values:

$$S_{a,b} := \sum_{y \in \mathbb{F}_{q^m}^*} \sum_{x \in C_0^{(N, q^m)}} \sum_{\ell \in I} \psi_{\mathbb{F}_{q^m}}(ay + bxy^{-1}\omega^\ell), \quad (0, 0) \neq (a, b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}.$$

In the case where either one of  $a$  or  $b$  is zero, it is clear that  $S_{a,b} = -(q^m-1)|I|/N$ .

Now, we assume that  $a \neq 0$  and  $b \neq 0$ . By the orthogonality of characters, we have

$$S_{a,b} = \frac{1}{(q^m-1)^2} \sum_{j,k=0}^{q^m-2} \sum_{y \in \mathbb{F}_{q^m}^*} \sum_{x \in C_0^{(N, q^m)}} \sum_{\ell \in I} G_{q^m}(\chi_{q^m-1}^{-j}) G_{q^m}(\chi_{q^m-1}^{-k}) \chi_{q^m-1}^j(a) \chi_{q^m-1}^k(bx\omega^\ell) \chi_{q^m-1}^{j-k}(y). \quad (3.8)$$

Since  $\sum_{y \in \mathbb{F}_{q^m}^*} \chi_{q^m-1}^{j-k}(y) = q^m - 1$  or  $0$  according as  $j \equiv k \pmod{q^m - 1}$  or  $j \not\equiv k \pmod{q^m - 1}$ , continuing from (3.8), we have

$$S_{a,b} = \frac{1}{q^m - 1} \sum_{j=0}^{q^m-2} \sum_{x \in C_0^{(N,q^m)}} \sum_{\ell \in I} G_{q^m}(\chi_{q^m-1}^{-j})^2 \chi_{q^m-1}^j(a) \chi_{q^m-1}^j(bx\omega^\ell). \quad (3.9)$$

Let  $\chi_N := \chi_{q^m-1}^{\frac{q^m-1}{N}}$ . Since  $\sum_{x \in C_0^{(N,q^m)}} \chi_{q^m-1}^j(x) = (q^m - 1)/N$  or  $0$  according as  $j \equiv 0 \pmod{\frac{q^m-1}{N}}$  or  $j \not\equiv 0 \pmod{\frac{q^m-1}{N}}$ , continuing from (3.9), we have

$$S_{a,b} = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{\ell \in I} G_{q^m}(\chi_N^{-j})^2 \chi_N^j(ab\omega^\ell).$$

On the other hand, by (3.5), we have  $\sum_{i \in I} \chi_N^j(\omega^i) = \frac{G_{q^m}(\chi_N^j)}{\delta q}$ . Hence, we have

$$\begin{aligned} S_{a,b} - \frac{|I|}{N} &= \frac{1}{\delta q N} \sum_{j=1}^{N-1} \chi_N^j(ab) G_{q^m}(\chi_N^{-j}) G_{q^m}(\chi_N^{-j}) G_{q^m}(\chi_N^j) \\ &= \frac{q^{m-1}}{\delta N} \sum_{j=1}^{N-1} \chi_N^j(\omega^a) G_{q^m}(\chi_N^{-j}) \\ &= \frac{q^m}{N} \sum_{j=1}^{N-1} \sum_{\ell \in I} \chi_N^{-j}(\omega^\ell) \chi_N^j(ab) = -\frac{q^m |I|}{N} + \begin{cases} q^m, & \text{if } \log_\omega(ab) \in I \pmod{N}, \\ 0, & \text{if } \log_\omega(ab) \notin I \pmod{N}. \end{cases} \end{aligned}$$

Thus  $\psi_{a,b}(H) = S_{a,b}$ ,  $(0,0) \neq (a,b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ , take exactly two distinct values  $-\frac{(q^m-1)|I|}{N}$  and  $-\frac{(q^m-1)|I|}{N} + q^m$ . Therefore  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H)$  is strongly regular. The parameters of  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H)$  can be computed in a straightforward way. We omit the details.  $\square$

**Remark 3.5.** Under the assumptions of Proposition 3.4, set

$$H' := H \cup \{(0, x) \mid x \in \mathbb{F}_{q^m}^*\} \cup \{(x, 0) \mid x \in \mathbb{F}_{q^m}^*\}.$$

Then,  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H')$  is also strongly regular. Furthermore, if  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N,q^m)})$  is a cyclotomic strongly regular graph in the subfield case with  $N = \frac{q^m-1}{q-1}$ , we have

$$H' = \{(0,0) \neq (x,y) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \mid \text{Tr}_{q^m/q}(xy) = 0\},$$

where  $\text{Tr}_{q^m/q}(xy)$  is a nondegenerate hyperbolic quadratic form from  $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$  to  $\mathbb{F}_q$ . Hence, it is appropriate to call the lifting construction in Proposition 3.4 a *hyperbolic* type lifting construction.

We now apply Propositions 3.2 and 3.4 to the known cyclotomic strongly regular graphs. We first apply the two propositions to the semi-primitive examples. In this case, we have  $|I| = 1$ .

**Corollary 3.6.** *Let  $p$  be a prime,  $N \geq 2$ ,  $q^m = p^{2js}$ , where  $s \geq 2$ ,  $N \mid (p^j + 1)$ , and  $j$  is the smallest such positive integer. For  $\epsilon \in \{1, -1\}$ , there exists an  $(n^2, r(n - \epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$  strongly regular Cayley graph with  $n = q^m$  and  $r = (q^m - 1)/N$ .*

Next we apply Propositions 3.2 and 3.4 to the subfield examples. In this case, we have  $N = \frac{q^m-1}{q^d-1}$  and  $|I| = \frac{q^{m-d}-1}{q^d-1}$ , where  $d \mid m$ .

**Corollary 3.7.** *Let  $q$  be a prime power and  $m \geq 3$  a positive integer. For  $\epsilon \in \{1, -1\}$ , there exists an  $(n^2, r(n - \epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$  strongly regular Cayley graph with  $n = q^m$  and  $r = q^{m-d} - 1$ .*

When  $d = 1$ , the strongly regular graphs obtained in Corollary 3.7 were already known [12].

Finally, we apply Propositions 3.2 and 3.4 to the eleven sporadic examples of cyclotomic strongly regular graphs. In this case, the values of  $k := |I|$  are given in [16, Table II].

**Corollary 3.8.** *For  $\epsilon \in \{1, -1\}$ , there exists an  $(n^2, r(n - \epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$  strongly regular Cayley graph with  $n = q^m$  and  $r = k(q^m - 1)/N$  in each of the following cases:*

$$(q^m, N, k) = (3^5, 11, 5), (5^9, 19, 9), (3^{12}, 35, 17), (7^9, 37, 9), (11^7, 43, 21), (17^{33}, 67, 33) \\ (3^{53}, 107, 53), (5^{18}, 133, 33), (41^{81}, 163, 81), (3^{144}, 323, 161), (5^{249}, 499, 249).$$

#### 4. HALVING THE CONNECTION SETS $E$ AND $H$ AND THEIR COMPLEMENTS

In a couple of recent papers [7, 4], motivated by existence questions concerning finite geometric objects such as  $m$ -ovoids and  $i$ -tight sets, we used a certain partition of the Singer difference set to construct strongly regular Cayley graphs with special properties which give the desired  $m$ -ovoids and  $i$ -tight sets. We now realize that the constructions can be done in a more general setting, namely, we can do the construction by partitioning a subdifference set of the Singer difference set in a certain way. In the case where the cyclotomic strongly regular graph comes from a subfield, the subdifference set of the Singer difference set is actually a Singer difference set; so in this case, we recover the previous constructions. We will also use a certain partition of the complement of a subdifference of the Singer difference sets to construct more strongly regular Cayley graphs.

Assume that  $N \geq 2$  is odd,  $N \mid \frac{q^m - 1}{q - 1}$ , and  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular. Let  $I$  be the corresponding subdifference set in  $\mathbb{Z}_N$  defined in (3.3). Let  $S_1, S_2$  be a partition of  $I$  and let  $S'_i \equiv 2^{-1}S_i \pmod{N}$  and  $S''_i \equiv 2^{-1}S'_i \pmod{N}$  for  $i = 1, 2$ . Define

$$X := 2S''_1 \cup (2S''_2 + N) \pmod{2N}. \quad (4.1)$$

Let  $J_1 := \{0, 3\}$  and  $J_2 := \{1, 2\}$ . Define

$$Y := \{Ni + 4j \pmod{4N} : (i, j) \in (J_1 \times S''_1) \cup (J_2 \times S''_2)\}. \quad (4.2)$$

It is clear that  $X \equiv 2^{-1}I \pmod{N}$  and  $Y \equiv I \pmod{N}$ .

Similarly, let  $T_1, T_2$  be a partition of  $\mathbb{Z}_N \setminus I$  and let  $T'_i \equiv 2^{-1}T_i \pmod{N}$  and  $T''_i \equiv 2^{-1}T'_i \pmod{N}$  for  $i = 1, 2$ . Define

$$\widehat{X} := 2T''_1 \cup (2T''_2 + N) \pmod{2N}. \quad (4.3)$$

Furthermore, define

$$\widehat{Y} := \{Ni + 4j \pmod{4N} : (i, j) \in (J_1 \times T''_1) \cup (J_2 \times T''_2)\}, \quad (4.4)$$

where  $J_1 = \{0, 3\}$  and  $J_2 = \{1, 2\}$ .

**4.1. Decompositions of  $\text{Cay}(\mathbb{F}_{q^{2m}}, E)$  and its complement.** In this subsection, we always assume that  $q^m \equiv 3 \pmod{4}$ . We will consider decompositions of  $\text{Cay}(\mathbb{F}_{q^{2m}}, E)$  and its complement, where  $E$  is defined in (3.4). We define

$$E_1 := \bigcup_{i \in Y} C_i^{(4N, q^{2m})}, \quad (4.5)$$

where  $C_i^{(4N, q^{2m})} := \gamma^i \langle \gamma^{4N} \rangle$ ,  $\gamma$  is a primitive element of  $\mathbb{F}_{q^{2m}}$ , and  $Y$  is defined in (4.2). Since  $Y \equiv I \pmod{N}$ , we see that  $E_1$  is a subset of  $E$ , and  $|E_1| = |E|/2$ . The (additive) character values of  $E_1$  are given by the following lemma.

**Lemma 4.1.** *Let  $\psi_{\mathbb{F}_{q^{2m}}}$  and  $\psi_{\mathbb{F}_{q^m}}$  be the canonical additive characters of  $\mathbb{F}_{q^{2m}}$  and  $\mathbb{F}_{q^m}$ , respectively. For  $a \in \mathbb{Z}_{4N}$ , define  $b \equiv 4^{-1}a \pmod{N}$  and  $c \equiv 2b \pmod{2N}$ . Then,*

$$\psi_{\mathbb{F}_{q^{2m}}}(\gamma^a E_1) = \frac{\rho_p \delta_a q^m}{2G_{q^m}(\eta)} \left( 2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in X} C_t^{(2N, q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}) \right) \\ + \frac{(q^m - 1)|I|}{2N} - \begin{cases} \frac{q^m}{2}, & \text{if } c \in 2^{-1}I \pmod{N}, \\ 0, & \text{otherwise,} \end{cases} \quad (4.6)$$



where  $\delta_a = 1$  or  $-1$  depending on whether  $a \equiv 0, N \pmod{4}$  or  $a \equiv 2, 3N \pmod{4}$ , and  $\rho_p = 1$  or  $-1$  depending on whether  $p \equiv 7 \pmod{8}$  or  $p \equiv 3 \pmod{8}$ . Furthermore,  $\eta$  is the quadratic character of  $\mathbb{F}_{q^m}$ .

This lemma is a common generalization of the results in [4] and [14]. Its proof is the same as those in [4] and [14]. We therefore omit the proof.

Next, we consider a decomposition of the complement of  $\text{Cay}(\mathbb{F}_{q^{2m}}, E)$ . Let

$$E_2 := \bigcup_{i \in \widehat{Y}} C_i^{(4N, q^{2m})}, \quad (4.7)$$

where  $\widehat{Y}$  is defined in (4.4). The (additive) character values of  $E_2$  are given by the following lemma.

**Lemma 4.2.** *With the same notation as in Lemma 4.1,*

$$\begin{aligned} \psi_{\mathbb{F}_{q^{2m}}}(\gamma^a E_2) &= \frac{\rho_p \delta_a q^m}{2G_{q^m}(\eta)} \left( 2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in \widehat{X}} C_t^{(2N, q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in \mathbb{Z}_N \setminus 2^{-1}I} C_t^{(N, q^m)}) \right) \\ &\quad + \frac{(q^m - 1)(N - |I|)}{2} - \begin{cases} 0, & \text{if } c \in 2^{-1}I \pmod{N}, \\ \frac{q^m}{2}, & \text{otherwise.} \end{cases} \end{aligned} \quad (4.8)$$

**Remark 4.3.** (i) If  $X$  defined in (4.1) satisfies that

$$2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in X} C_t^{(2N, q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}) = \begin{cases} \pm G_{q^m}(\eta), & \text{if } c \in 2^{-1}I \pmod{N}, \\ 0, & \text{otherwise,} \end{cases} \quad (4.9)$$

substituting (4.9) into (4.6), we find that the nontrivial additive character values of  $E_1$  take two distinct values  $\frac{(q^m - 1)|I|}{2N}$  and  $\frac{(q^m - 1)|I|}{2N} - q^m$ , implying that  $\text{Cay}(\mathbb{F}_{q^{2m}}, E_1)$  is strongly regular.

(ii) If  $\widehat{X}$  defined in (4.3) satisfies that

$$2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in \widehat{X}} C_t^{(2N, q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in \mathbb{Z}_N \setminus 2^{-1}I} C_t^{(N, q^m)}) = \begin{cases} 0, & \text{if } c \in 2^{-1}I \pmod{N}, \\ \pm G_{q^m}(\eta), & \text{otherwise,} \end{cases} \quad (4.10)$$

substituting (4.10) into (4.8), we find that the nontrivial additive character values of  $E_2$  take two distinct values  $\frac{(q^m - 1)(N - |I|)}{2N}$  and  $\frac{(q^m - 1)(N - |I|)}{2N} - q^m$ , implying that  $\text{Cay}(\mathbb{F}_{q^{2m}}, E_2)$  is strongly regular.

**4.2. Decompositions of  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H)$  and its complement.** In this subsection, we assume that  $q^m \equiv 1 \pmod{4}$ ,  $N$  is an odd divisor of  $\frac{q^m - 1}{q - 1}$ , and  $\gcd(N, \frac{q^m - 1}{N}) = 1$ . Define

$$H_1 := \{(xy, xy^{-1}z\omega^\ell) \mid x \in C_0^{(N, q^m)}, y \in C_0^{(\frac{q^m - 1}{N}, q^m)}, z \in C_0^{(4N, q^m)}, \ell \in Y\} \subseteq \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, \quad (4.11)$$

where  $\omega$  is a primitive element of  $\mathbb{F}_{q^m}$  defined in Subsection 3.2 and  $Y$  is defined in (4.2). In the definition of  $H_1$ , since  $x^2 z \omega^\ell \in \bigcup_{\ell \in I} C_\ell^{(N, q^m)}$ , we see that  $H_1$  is a subset of  $H$ . Moreover,  $|H_1| = |H|/2$ . The (additive) character values of  $H_1$  are given in the following lemma.

**Lemma 4.4.** *Let  $\psi_{a,b}$  be an additive character of  $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$  defined in (3.7) and  $\psi_{\mathbb{F}_{q^m}}$  be the canonical additive character of  $\mathbb{F}_{q^m}$ . For  $(a, b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \setminus \{(0, 0)\}$  with  $ab = 0$ , it holds that  $\psi_{a,b}(H_1) = -(q^m - 1)|I|/2N$ . For  $(a, b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \setminus \{(0, 0)\}$  with  $ab \neq 0$ , it holds that*

$$\begin{aligned} \psi_{a,b}(H_1) &= \frac{\eta(2\omega^c)G_{q^m}(\eta)\delta_{a,b}}{2} \left( 2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in X} C_t^{(2N, q^3)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}) \right) \\ &\quad - \frac{(q^m - 1)|I|}{2N} + \begin{cases} \frac{q^m}{2}, & \text{if } c \in 2^{-1}I \pmod{N}, \\ 0, & \text{otherwise,} \end{cases} \end{aligned} \quad (4.12)$$

where  $c$  is defined by  $\omega^c = (ab)^{\frac{N+1}{2}}$  and  $\delta_{a,b} = 1$  or  $-1$  depending on whether  $\log_\omega(a^{-1}b) \equiv 0, N \pmod{4}$  or  $\log_\omega(a^{-1}b) \equiv 2, 3N \pmod{4}$ . Furthermore,  $\eta$  is the quadratic character of  $\mathbb{F}_{q^m}$ .

This lemma is a generalization of [7, Theorem 4.1]. Since the proof is similar to that of [7, Theorem 4.2], we omit the proof.

Next, we consider a decomposition of the complement of  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H)$ . Define

$$H_2 := \{(xy, xy^{-1}z\omega^\ell) \mid x \in C_0^{(N, q^m)}, y \in C_0^{(\frac{q^m-1}{N}, q^m)}, z \in C_0^{(4N, q^m)}, \ell \in \widehat{Y}\} \subseteq \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, \quad (4.13)$$

where  $\widehat{Y}$  is defined in (4.4). The character values of  $H_2$  are given in the following lemma.

**Lemma 4.5.** *For  $(a, b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \setminus \{(0, 0)\}$  with  $ab = 0$ , it holds that  $\psi_{a,b}(H_2) = -(q^m - 1)(N - |I|)/2N$ . For  $(a, b) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \setminus \{(0, 0)\}$  with  $ab \neq 0$ , it holds that*

$$\begin{aligned} \psi_{a,b}(H_2) = \frac{\eta(2\omega^c)G_{q^m}(\eta)\delta_{a,b}}{2} & \left( 2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in \widehat{X}} C_t^{(2N, q^3)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in \mathbb{Z}_N \setminus 2^{-1}I} C_t^{(N, q^m)}) \right) \\ & - \frac{(q^m - 1)(N - |I|)}{2N} + \begin{cases} 0, & \text{if } c \in 2^{-1}I \pmod{N}, \\ \frac{q^m}{2}, & \text{otherwise,} \end{cases} \end{aligned} \quad (4.14)$$

where  $c$  is defined by  $\omega^c = (ab)^{\frac{N+1}{2}}$ .

**Remark 4.6.** Similarly to Remark 4.3, if the set  $X$  defined in (4.1) satisfies (4.9), the nontrivial additive character values of  $H_1$  take two distinct values  $-\frac{(q^m-1)|I|}{2N}$  and  $-\frac{(q^m-1)|I|}{2N} + q^m$ , implying that  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H_1)$  is strongly regular. Also, if  $\widehat{X}$  defined in (4.3) satisfies (4.10), then the nontrivial additive character values of  $H_2$  take two distinct values  $-\frac{(q^m-1)(N-|I|)}{2N}$  and  $-\frac{(q^m-1)(N-|I|)}{2N} + q^m$ , implying that  $\text{Cay}(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}, H_2)$  is strongly regular.

## 5. PARTITION OF SUBDIFFERENCE SETS AND THEIR COMPLEMENTS IN SEMI-PRIMITIVE CASE

In this section, we consider a partition of the subdifference sets  $I$  in semi-primitive case. We will use the same notation as in Section 4. We assume that  $N$  is odd and  $q^m = p^{2js}$ , where  $p$  is a prime,  $s \geq 2$ ,  $N \mid (p^j + 1)$ , and  $j$  is the smallest such positive integer. In this case,  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular and we have  $I = \{0\}$  [16]. Furthermore, by Theorem 2.3, the Gauss sums with respect to multiplicative characters of exponent  $N$  of  $\mathbb{F}_{q^m}$  can be explicitly evaluated as

$$G_{q^m}(\chi_N^i) = (-1)^{s-1} \sqrt{q^m}, \quad 1 \leq i \leq N-1. \quad (5.1)$$

**Theorem 5.1.** *With the same notation as in Section 4, under the above assumptions, the partition  $(S_1, S_2) = (\{0\}, \emptyset)$  of  $I$  satisfies the condition (4.9) of Remark 4.3 (i).*

**Proof:** By the definition (4.1) of  $X$ , we have  $X = \{0\}$ . Write

$$P_c := 2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in X} C_t^{(2N, q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}).$$

By (4.9), we need to prove that

$$P_c = \begin{cases} \pm G_{q^m}(\eta), & \text{if } c \equiv 0 \pmod{N}, \\ 0, & \text{otherwise,} \end{cases}$$

where  $\eta$  is the quadratic character of  $\mathbb{F}_{q^m}$ . Let  $\chi_N$  be a multiplicative character of order  $N$  of  $\mathbb{F}_{q^m}$ . By the orthogonality of characters, we have

$$\begin{aligned} P_c &= \frac{1}{N} \left( \sum_{i=0}^{N-1} \sum_{j=0,1} \sum_{t \in X} G_{q^m}(\chi_N^i \eta^j) \chi_N^{-i} \eta^j (\omega^{c+t}) - \sum_{i=0}^{N-1} \sum_{t \in 2^{-1}I} G_{q^m}(\chi_N^i) \chi_N^{-i} (\omega^{c+t}) \right) \\ &= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{t \in X} G_{q^m}(\chi_N^i \eta) \chi_N^{-i} \eta (\omega^{c+t}). \end{aligned} \quad (5.2)$$

By the Davenport-Hasse product formula and (5.1), we have

$$G_{q^m}(\chi_N^i \eta) = \frac{G_{q^m}(\chi_N^{2i}) G_{q^m}(\eta)}{G_{q^m}(\chi_N^i)} = G_{q^m}(\eta).$$

On the other hand, by the definition of  $X$ , we have  $\sum_{t \in X} \chi_N^{-i} \eta(\omega^t) = 1$ . Continuing from (5.2), we have

$$P_c = \frac{\eta(\omega^c) G_{q^m}(\eta)}{N} \sum_{i=0}^{N-1} \chi_N^{-i} (\omega^c) = \begin{cases} \eta(\omega^c) G_{q^m}(\eta), & \text{if } c \equiv 0 \pmod{N}, \\ 0, & \text{otherwise.} \end{cases}$$

This completes the proof of the theorem.  $\square$

Similarly to the theorem above, we have the following.

**Theorem 5.2.** *With the notations above, the partition  $(T_1, T_2) = (\mathbb{Z}_N \setminus \{0\}, \emptyset)$  of  $\mathbb{Z}_N \setminus I$  satisfies the condition (4.10) of Remark 4.3 (ii).*

Since  $q^m = p^{2js}$ , we have  $q^m \equiv 1 \pmod{4}$ . We can only apply the lifting construction of hyperbolic type. By Lemma 4.4, Remark 4.6 and Theorem 5.1, we obtain the following.

**Corollary 5.3.** *Let  $N$  be odd and  $q^m = p^{2js}$ , where  $p$  is a prime,  $s \geq 2$ ,  $N \mid (p^j + 1)$ , and  $j$  is the smallest such positive integer. Assume that  $\gcd(N, \frac{q^m - 1}{N}) = 1$ . Then, there exists a  $(q^{2m}, r(q^m - 1), q^m + r^2 - 3r, r^2 - r)$  strongly regular Cayley graph, where  $r = (q^m - 1)/2N$ .*

Similarly to the corollary above, by Lemma 4.5, Remark 4.6 and Theorem 5.2, we obtain the following corollary.

**Corollary 5.4.** *Let  $N$  be odd and  $q^m = p^{2js}$ , where  $p$  is a prime,  $s \geq 2$ ,  $N \mid (p^j + 1)$ , and  $j$  is the smallest such positive integer. Assume that  $\gcd(N, \frac{q^m - 1}{N}) = 1$ . Then, there exists a  $(q^{2m}, r(q^m - 1), q^m + r^2 - 3r, r^2 - r)$  strongly regular Cayley graph, where  $r = (N - 1)(q^m - 1)/2N$ .*

## 6. PARTITION OF SUBDIFFERENCE SETS AND THEIR COMPLEMENTS IN SPORADIC CASE

In this section, we consider partitions of the subdifference set  $I$  and its complement in the sporadic case.

**Theorem 6.1.** *Assume that  $N \geq 2$  is odd,  $N \mid \frac{q^m - 1}{q - 1}$ ,  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular and  $-2 \in \langle p \rangle \pmod{N}$ , where  $p$  is the characteristic of  $\mathbb{F}_{q^m}$ . Let  $I$  be the corresponding subdifference set defined in (3.3). Then, the partition  $(S_1, S_2) = (I, \emptyset)$  of  $I$  satisfies the condition (4.9) of Remark 4.3 (i).*

**Proof:** Let  $I' \equiv 4^{-1}I \pmod{N}$ . By the definition (4.1) of  $X$ , we have  $X \equiv 2I' \pmod{2N}$ . Write

$$P_c := 2\psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in X} C_t^{(2N, q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}).$$

Let  $\chi_N$  be a multiplicative character of  $\mathbb{F}_{q^m}$  of order  $N$  and  $\eta$  be the quadratic character of  $\mathbb{F}_{q^m}$ . Similarly to the proof of Theorem 5.1, we have

$$P_c = \frac{1}{N} \sum_{i=1}^{N-1} \sum_{t \in X} G_{q^m}(\chi_N^i \eta) \chi_N^{-i} \eta(\omega^{c+t}) + \frac{\eta(\omega^c) G_{q^m}(\eta) |I|}{N}. \quad (6.1)$$

By the Davenport-Hasse product formula, we have

$$G_{q^m}(\chi_N^i \eta) = \frac{G_{q^m}(\chi_N^{2i}) G_{q^m}(\eta)}{G_{q^m}(\chi_N^i)}.$$

On the other hand, by (3.2), for  $i \neq 0$

$$\sum_{t \in X} \chi_N^{-i} \eta(\omega^t) = \sum_{t \in 2I'} \chi_N^{-i}(\omega^t) = \frac{G_{q^m}(\chi_N^{-2^{-1}i})}{\delta q}.$$

Substituting these into (6.1), we have

$$P_c = \frac{\eta(\omega^c) G_{q^m}(\eta)}{\delta q N} \sum_{i=1}^N \frac{G_{q^m}(\chi_N^{2i}) G_{q^m}(\chi_N^{-2^{-1}i})}{G_{q^m}(\chi_N^i)} \chi_N^{-i}(\omega^c) + \frac{\eta(\omega^c) G_{q^m}(\eta) |I|}{N}. \quad (6.2)$$

By the assumption that  $-2 \in \langle p \rangle \pmod{N}$ , we have  $G_{q^m}(\chi_N^{-2^{-1}i}) = G_{q^m}(\chi_N^i)$ . Therefore, continuing from (6.2), we have

$$\begin{aligned} P_c &= \frac{\eta(\omega^c) G_{q^m}(\eta)}{\delta q N} \sum_{i=1}^N G_{q^m}(\chi_N^{2i}) \chi_N^{-i}(\omega^c) + \frac{\eta(\omega^c) G_{q^m}(\eta) |I|}{N} \\ &= \frac{\eta(\omega^c) G_{q^m}(\eta)}{N} \left( \sum_{i=1}^N \sum_{t \in I} \chi_N^{2i}(\omega^t) \chi_N^{-i}(\omega^c) + |I| \right) \\ &= \frac{\eta(\omega^c) G_{q^m}(\eta)}{N} \sum_{i=0}^N \sum_{t \in I} \chi_N^{2i}(\omega^t) \chi_N^{-i}(\omega^c) = \begin{cases} \eta(\omega^c) G_{q^m}(\eta), & \text{if } c \in 2I \pmod{N}, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Since the subdifference set  $I$  is invariant under the multiplication by  $p$  modulo  $N$ , by the assumption that  $-2^{-1} \in \langle p \rangle \pmod{N}$ , the condition  $c \in 2I \pmod{N}$  is equivalent to that  $c \in 2^{-1}I \pmod{N}$ . This completes the proof of the theorem.  $\square$

Similarly to the theorem above, we have the following.

**Theorem 6.2.** *Assume that  $N \geq 2$  is odd,  $N \mid \frac{q^m-1}{q-1}$ ,  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular and  $-2 \in \langle p \rangle \pmod{N}$ . Then the partition  $(T_1, T_2) = (\mathbb{Z}_N \setminus I, \emptyset)$  of  $\mathbb{Z}_N \setminus I$  satisfies the condition (4.10) of Remark 4.3 (ii).*

There are ten sporadic examples of cyclotomic strongly regular graphs satisfying the condition  $-2 \in \langle p \rangle \pmod{N}$ . In particular, when  $q^m \equiv 3 \pmod{4}$ , we obtain the following result.

**Corollary 6.3.** *There exists a  $(q^{2m}, r(q^m + 1), -q^m + r^2 + 3r, r^2 + r)$  strongly regular Cayley graph with  $r = k(q^m - 1)/2N$  in each of the following cases:*

$$(q^m, N, k) = (3^5, 11, 5), (11^7, 43, 21), (3^{53}, 107, 53).$$

**Proof:** It is clear that  $-2 \in \langle p \rangle \pmod{N}$  in these cases. Then, by applying Lemma 4.1, Remark 4.3 (i) and Theorem 6.1 to these examples, the corollary now follows.  $\square$

Similarly to the corollary above, by applying Lemma 4.2, Remark 4.3 (ii) and Theorem 6.2 to the three sporadic cyclotomic strongly regular graphs in Corollary 6.5, we obtain the following.

**Corollary 6.4.** *There exists a  $(q^{2m}, r(q^m + 1), -q^m + r^2 + 3r, r^2 + r)$  strongly regular Cayley graph with  $r = (N - k)(q^m - 1)/2N$  in each of the following cases:*

$$(q^m, N, k) = (3^5, 11, 5), (11^7, 43, 21), (3^{53}, 107, 53).$$

In the case where  $(q^m, N, k) = (7^9, 37, 9)$ , the condition that  $-2 \in \langle p \rangle \pmod{N}$  is not satisfied. We checked by computer that there is no partition of the subdifference set  $I$  satisfying the condition (4.9). On the other hand, we checked that there is a partition of  $\mathbb{Z}_{37} \setminus I$  satisfying the condition (4.10):  $T_1 = 2I$  and  $T_2 = \mathbb{Z}_{37} \setminus (I \cup 2I)$ . Hence, we have the following corollary.

**Corollary 6.5.** *There exists a  $(q^{2m}, r(q^m + 1), -q^m + r^2 + 3r, r^2 + r)$  strongly regular Cayley graph with  $r = (N - k)(q^m - 1)/2N$  in the case where  $(q^m, N, k) = (7^9, 37, 9)$ .*

Next, we consider the case where  $q^m \equiv 1 \pmod{4}$ .

**Corollary 6.6.** *There exists a  $(q^{2m}, r(q^m - 1), q^m + r^2 - 3r, r^2 - r)$  strongly regular Cayley graph with  $r = k(q^m - 1)/2N$  in each of the following cases:*

$$(q^m, N, k) = (3^{12}, 35, 17), (5^9, 19, 9), (17^{33}, 67, 33), (5^{18}, 133, 33), \\ (41^{81}, 163, 81), (3^{144}, 323, 161), (5^{249}, 499, 249).$$

**Proof:** It is clear that  $\gcd(N, \frac{q^m - 1}{N}) = 1$  and  $-2 \in \langle p \rangle \pmod{N}$  in these cases. Then, by applying Lemma 4.4, Remark 4.6 and Theorem 6.1 to these examples, the corollary now follows.  $\square$

Similarly to the corollary above, by applying Lemma 4.5, Remark 4.6 and Theorem 6.2 to these examples, we obtain the following corollary.

**Corollary 6.7.** *There exists a  $(q^{2m}, r(q^m - 1), q^m + r^2 - 3r, r^2 - r)$  strongly regular Cayley graph with  $r = (N - k)(q^m - 1)/2N$  in each of the following cases:*

$$(q^m, N, k) = (3^{12}, 35, 17), (5^9, 19, 9), (17^{33}, 67, 33), (5^{18}, 133, 33), \\ (41^{81}, 163, 81), (3^{144}, 323, 161), (5^{249}, 499, 249).$$

## 7. PARTITIONS OF SUBDIFFERENCE SETS AND THEIR COMPLEMENTS IN THE SUBFIELD CASE

In this section, we consider partitions of the subdifference set  $I$  and its complement in subfield case. We assume that  $m$  is odd and  $N = \frac{q^m - 1}{q - 1}$ . In this case,  $\text{Cay}(\mathbb{F}_{q^m}, C_0^{(N, q^m)})$  is strongly regular and we have

$$I := \{i \pmod{N} : \text{Tr}_{q^m/q}(w^i) = 0\}. \quad (7.1)$$

**7.1. A partition of the Singer difference set  $I$  defined in (7.1) when  $m = 3$ .** In the case where  $m = 3$ , a partition of the Singer difference set  $I$  satisfying the condition (4.9) of Remark 4.3 (i) was found in [7, Theorem 3.7]. Regarding  $\mathbb{F}_{q^3}$  as a 3-dimensional vector space over  $\mathbb{F}_q$ , we use  $\mathbb{F}_{q^3}$  as the underlying vector space of  $\text{PG}(2, q)$ . The points of  $\text{PG}(2, q)$  are  $\langle \omega^i \rangle$ ,  $0 \leq i \leq N - 1$ , and the lines of  $\text{PG}(2, q)$  are

$$L_i := \{\langle x \rangle : \text{Tr}_{q^3/q}(\omega^i x) = 0\}, \quad 0 \leq i \leq N - 1. \quad (7.2)$$

The Singer difference set  $I$  corresponds to the typical line  $L_0$ .

Consider a nondegenerate quadratic form  $f : \mathbb{F}_{q^3} \rightarrow \mathbb{F}_q$  defined by  $f(x) = \text{Tr}_{q^3/q}(x^2)$ , which defines a conic  $\mathcal{Q}$  in  $\text{PG}(2, q)$  containing  $q + 1$  points. Consequently, each line  $L$  of  $\text{PG}(2, q)$  meets  $\mathcal{Q}$  in 0, 1 or 2 points. Consider the following subset of  $\mathbb{Z}_N$ :

$$I_{\mathcal{Q}} := \{i \pmod{N} : f(\omega^i) = 0\} = \{d_0, d_1, \dots, d_q\}, \quad (7.3)$$

where the elements are numbered in any unspecified order. Thus,  $\mathcal{Q} = \{\langle \omega^{d_i} \rangle : 0 \leq i \leq q\}$ . Furthermore, by the definition of  $f$  and  $I$ ,  $I_{\mathcal{Q}} \equiv 2^{-1}I \pmod{N}$ .

For  $d_0 \in I_{\mathcal{Q}}$ , define

$$\mathcal{X} := \{\omega^{d_i} \text{Tr}_{q^3/q}(\omega^{d_0 + d_i}) : 1 \leq i \leq q\} \cup \{2\omega^{d_0}\}$$

and

$$X := \{\log_\omega(x) \pmod{2N} : x \in \mathcal{X}\} \subset \mathbb{Z}_{2N}. \quad (7.4)$$

Clearly,  $|X| = |I_{\mathcal{Q}}|$  and  $X \equiv I_{\mathcal{Q}} \pmod{N}$ . If we use any other  $d_i$  instead of  $d_0$  in the definition of  $\mathcal{X}$ , then the resulting set  $X'$  satisfies that  $X' \equiv X \pmod{2N}$  or  $X' \equiv X + N \pmod{2N}$  [7, Lemma 3.4].

The set  $X$  can be expressed as

$$X = 2S_1'' \cup (2S_2'' + N) \pmod{2N} \quad (7.5)$$

for some  $S_1'', S_2'' \subseteq \mathbb{Z}_N$  with  $|S_1''| + |S_2''| = q + 1$ . Define  $S_i' \equiv 2S_i'' \pmod{N}$  and  $S_i \equiv 2S_i' \pmod{N}$  for  $i = 1, 2$ . Then,  $S_1' \cup S_2' \equiv I_{\mathcal{Q}} \pmod{N}$  and  $S_1 \cup S_2 \equiv I \pmod{N}$ , i.e.,  $X$  induces partitions of  $I_{\mathcal{Q}}$  and  $I$ , respectively.

**Theorem 7.1.** [7, Theorem 3.7] *The set  $X$  defined in (7.4) satisfies the condition (4.9) of Remark 4.3 (i).*

As corollaries, we have the following.

**Corollary 7.2.** *For a prime power  $q \equiv 3 \pmod{4}$ , there exists a  $(q^6, r(q^3 + 1), -q^3 + r^2 + 3r, r^2 + r)$  strongly regular Cayley graph, where  $r = (q^2 - 1)/2$ .*

**Proof:** By Lemma 4.1, Remark 4.3 (i) and Theorem 7.1, the corollary now follows.  $\square$

The connection set  $E_1 \subseteq \mathbb{F}_{q^6}$  of the strongly regular Cayley graph  $\text{Cay}(\mathbb{F}_{q^6}, E_1)$  obtained in Corollary 7.2 corresponds to a  $\frac{(q+1)}{2}$ -ovoid in an elliptic quadric  $\mathcal{Q}^-(5, q)$ . See [4].

**Corollary 7.3.** *For a prime power  $q \equiv 5, 9 \pmod{12}$ , there exists a  $(q^6, r(q^3 - 1), q^3 + r^2 - 3r, r^2 - r)$  strongly regular Cayley graph, where  $r = (q^2 - 1)/2$ .*

**Proof:** It is clear that  $\gcd(N, \frac{q^3-1}{N}) = 1$  if  $N = q^2 + q + 1$  and  $q \equiv 5, 9 \pmod{12}$ . Then, by Lemma 4.4, Remark 4.3 (ii) and Theorem 7.1, the corollary now follows.  $\square$

The connection set  $H_1 \subseteq \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}$  of the strongly regular Cayley graph  $\text{Cay}(\mathbb{F}_{q^3} \times \mathbb{F}_{q^3}, H_1)$  obtained in Corollary 7.3 corresponds to a  $\frac{(q^2-1)}{2}$ -tight set in a hyperbolic quadric  $\mathcal{Q}^+(5, q)$ . See [6, 7].

It would be interesting to find a desired partition of  $I$  when  $m$  is odd and  $m > 3$ . We leave this as an open problem.

**7.2. A partition of the complement of the Singer difference set with odd  $m$ .** In this section, we consider a partition of the complement of the Singer difference set  $I \pmod{\frac{q^m-1}{q-1}}$ , where  $m > 1$  is an arbitrary odd integer. Note that the set  $2^{-1}I \pmod{\frac{q^m-1}{q-1}}$  corresponds to a nondegenerate parabolic quadric  $\mathcal{Q}(m-1, q)$  of  $\text{PG}(m-1, q)$ .

Let  $N = \frac{q^m-1}{q-1}$  and  $\omega$  be a primitive element of  $\mathbb{F}_{q^m}$ , where  $q$  is an odd prime power and  $m > 1$  is an odd integer. Define

$$\begin{aligned} A &= \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(x^2) = 0\}, \\ A_0 &= \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(x^2) \in C_0^{(2,q)}\}, \\ A_1 &= \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(x^2) \in C_1^{(2,q)}\}. \end{aligned}$$

Let  $a_1 \in A$ , and define  $H_1 = \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(a_1x) = 0\}$ . Note that  $A$  represents a nondegenerate parabolic quadric of  $\text{PG}(m-1, q)$  and  $H_1$  is a tangent hyperplane<sup>2</sup> to  $A$  at point  $\langle a_1 \rangle$ . Thus  $A \cap H_1$  is a cone of order one with vertex  $\langle a_1 \rangle$ , and  $|A \cap H_1| = q^{m-2} - 1$ . If  $m = 3$ , we stop this process. Otherwise, we continue by choosing  $a_2 \in A \cap H_1$  such that  $a_1, a_2$  are linearly independent over  $\mathbb{F}_q$ , and define  $H_2 = \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(a_2x) = 0\}$ . Then  $H_1 \cap H_2$  is a hyperplane of  $H_1$ . Note that  $A \cap H_1$  represents a degenerate quadric (a cone of order one) in  $H_1$ , and  $H_1 \cap H_2$  contains the vertex

<sup>2</sup>Strictly speaking, we should say that  $H_1 \cup \{0\}$  is a hyperplane.

$\langle a_1 \rangle$ , we see that  $A \cap H_1 \cap H_2$  is a cone of order two (cf. [8]), and  $|A \cap H_1 \cap H_2| = q^{m-3} - 1$ . More generally, we define

$$\begin{aligned} H_\ell &= \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(xa_\ell) = 0\}, \quad a_\ell \in A \cap H_1 \cap \cdots \cap H_{\ell-1}, \\ H_{\ell,0} &= \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(xa_\ell) \in C_0^{(2,q)}\}, \quad a_\ell \in A \cap H_1 \cap \cdots \cap H_{\ell-1}, \\ H_{\ell,1} &= \{x \in \mathbb{F}_{q^m}^* \mid \text{Tr}_{q^m/q}(xa_\ell) \in C_1^{(2,q)}\}, \quad a_\ell \in A \cap H_1 \cap \cdots \cap H_{\ell-1}, \end{aligned}$$

where  $2 \leq \ell \leq \frac{m-1}{2}$ . We can always choose  $a_1, \dots, a_{\frac{m-1}{2}}$  so that they are linearly independent over  $\mathbb{F}_q$ . The reason is as follows: assume that  $a_1, \dots, a_{\ell-1}$  with  $2 \leq \ell \leq \frac{m-1}{2}$  are independent; since  $a_1, \dots, a_{\ell-1} \in A \cap H_1 \cap \cdots \cap H_{\ell-1}$  and

$$|A \cap H_1 \cap \cdots \cap H_{\ell-1}| = q^{m-\ell} - 1, \quad (7.6)$$

there are at least  $m - \ell$  independent elements in  $A \cap H_1 \cap \cdots \cap H_{\ell-1}$  including  $a_1, \dots, a_{\ell-1}$ ; hence, we can choose an element  $a_\ell \in A \cap H_1 \cap \cdots \cap H_{\ell-1}$  so that  $a_1, \dots, a_\ell$  are independent over  $\mathbb{F}_q$  whenever  $\ell \leq \frac{m-1}{2}$ .

Let  $b$  be a fixed element of  $(H_1 \cap \cdots \cap H_{\frac{m-1}{2}}) \setminus A$ . Since  $H_1 \cap \cdots \cap H_{\frac{m-1}{2}}$  and  $A \cap H_1 \cap \cdots \cap H_{\frac{m-1}{2}}$  correspond to a  $\frac{(m-1)}{2}$ -flat and a  $\frac{(m-3)}{2}$ -flat, respectively, in  $\text{PG}(m-1, q)$ , the set  $(H_1 \cap \cdots \cap H_{\frac{m-1}{2}}) \setminus A$  can be represented as

$$(H_1 \cap \cdots \cap H_{\frac{m-1}{2}}) \setminus A = \{a_1x_1 + \cdots + a_{\frac{m-1}{2}}x_{\frac{m-1}{2}} + by \mid x_1, \dots, x_{\frac{m-1}{2}} \in \mathbb{F}_q, y \in \mathbb{F}_q^*\}.$$

Let  $T_1 = (A_0 \cap H_{1,0}) \cup (A_1 \cap H_{1,1})$  and more generally

$$T_\ell := (A_0 \cap H_1 \cap \cdots \cap H_{\ell-1} \cap H_{\ell,0}) \cup (A_1 \cap H_1 \cap \cdots \cap H_{\ell-1} \cap H_{\ell,1}), \quad 2 \leq \ell \leq \frac{m-1}{2},$$

and

$$B := \{a_1x_1 + \cdots + a_{\frac{m-1}{2}}x_{\frac{m-1}{2}} + by \mid x_1, \dots, x_{\frac{m-1}{2}} \in \mathbb{F}_q, y \in C_0^{(2,q)}\}.$$

Finally, define

$$D := \left( \bigcup_{\ell=1}^{\frac{(m-1)/2}{2}} T_\ell \right) \cup B.$$

It is clear that

$$\omega^N T_\ell = (A_0 \cap H_1 \cap \cdots \cap H_{\ell-1} \cap H_{\ell,1}) \cup (A_1 \cap H_1 \cap \cdots \cap H_{\ell-1} \cap H_{\ell,0})$$

and

$$\omega^N B = \{a_1x_1 + \cdots + a_{\frac{m-1}{2}}x_{\frac{m-1}{2}} + by \mid x_1, \dots, x_{\frac{m-1}{2}} \in \mathbb{F}_q, y \in C_1^{(2,q)}\}.$$

Hence,  $D \cap \omega^N D = \emptyset$  and  $D \cup \omega^N D = \mathbb{F}_{q^m}^* \setminus A$ . Thus, there exists a subset  $\widehat{X} \subseteq \mathbb{Z}_{2N}$  such that  $D = \bigcup_{t \in \widehat{X}} C_t^{(2N, q^m)}$  and  $\widehat{X} \equiv \mathbb{Z}_N \setminus 2^{-1}I \pmod{N}$ . The set  $\widehat{X}$  induces a partition of the complement of  $2^{-1}I \pmod{N}$ .

**Theorem 7.4.** *The set  $\widehat{X}$  defined above satisfies the condition (4.10) of Remark 4.3 (ii).*

To prove this theorem, we need the following lemmas.

**Lemma 7.5.** *It holds that*

$$\psi_{\mathbb{F}_{q^m}}(\omega^a T_\ell) = \begin{cases} \frac{(-1)^{i+\epsilon} q^{\frac{m-1}{2}} q^{\frac{m-1}{2}} (-1+(-1)^{j+\tau} G_q(\eta'))}{2}, & \text{if } \omega^a \in A_i \cap H_1 \cap \cdots \cap H_{\ell-1} \cap H_{\ell,j}, \quad i, j = 0, 1, \\ -\frac{q^{m-\ell-1}(q-1)}{2}, & \text{if } \omega^a \in \langle a_1, \dots, a_\ell \rangle \setminus \langle a_1, \dots, a_{\ell-1} \rangle, \\ \frac{q^{m-\ell-1}(q-1)^2}{2}, & \text{if } \omega^a \in \langle a_1, \dots, a_{\ell-1} \rangle, \\ 0, & \text{otherwise,} \end{cases}$$

where  $\eta'$  is the quadratic character of  $\mathbb{F}_q$  and  $\epsilon = 0$  or  $1$  according as  $q \equiv 1 \pmod{4}$  or  $q \equiv 3 \pmod{4}$ . Furthermore,  $\tau$  is defined by  $2 \in C_\tau^{(2,q)}$ .

The proof of this lemma is complicated. Therefore, we postpone the proof to the Appendix.

**Lemma 7.6.** *It holds that*

$$\psi_{\mathbb{F}_q^m}(\omega^a B) = \begin{cases} q^{\frac{m-1}{2}} \frac{(-1+G_q(\eta'))}{2}, & \text{if } \text{Tr}_{q^m/q}(\omega^a b) \in C_0^{(2,q)}, \omega^a \in (H_1 \cap \cdots \cap H_{\frac{m-1}{2}}) \setminus A, \\ q^{\frac{m-1}{2}} \frac{(-1-G_q(\eta'))}{2}, & \text{if } \text{Tr}_{q^m/q}(\omega^a b) \in C_1^{(2,q)}, \omega^a \in (H_1 \cap \cdots \cap H_{\frac{m-1}{2}}) \setminus A, \\ \frac{q^{\frac{m-1}{2}}(q-1)}{2}, & \text{if } \omega^a \in A \cap H_1 \cap \cdots \cap H_{\frac{m-1}{2}}, \\ 0, & \text{otherwise.} \end{cases}$$

**Proof:** We compute the character values of  $B$ :

$$\begin{aligned} \psi_{\mathbb{F}_q^m}(\omega^a B) &= \sum_{x_1, \dots, x_{\frac{m-1}{2}} \in \mathbb{F}_q} \sum_{y \in C_0^{(2,q)}} \psi_{\mathbb{F}_q^m}(\omega^a a_1 x_1) \cdots \psi_{\mathbb{F}_q^m}(\omega^a a_{\frac{m-1}{2}} x_{\frac{m-1}{2}}) \psi_{\mathbb{F}_q^m}(\omega^a b y) \\ &= \left( \prod_{i=1}^{\frac{m-1}{2}} \sum_{x_i \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(\text{Tr}_{q^m/q}(\omega^a a_i) x_i) \right) \left( \sum_{y \in C_0^{(2,q)}} \psi_{\mathbb{F}_q}(\text{Tr}_{q^m/q}(\omega^a b) y) \right). \end{aligned}$$

If  $\text{Tr}_{q^m/q}(\omega^a a_i) \neq 0$  for some  $i = 1, \dots, \frac{m-1}{2}$ , then it is clear that  $\psi_{\mathbb{F}_q^m}(\omega^a B) = 0$ . Otherwise, we have

$$\begin{aligned} \psi_{\mathbb{F}_q^m}(\omega^a B) &= q^{\frac{m-1}{2}} \sum_{y \in C_0^{(2,q)}} \psi_{\mathbb{F}_q}(\text{Tr}_{q^m/q}(\omega^a b) y) \\ &= \begin{cases} q^{\frac{m-1}{2}} \frac{(-1+G_q(\eta'))}{2}, & \text{if } \text{Tr}_{q^m/q}(\omega^a b) \in C_0^{(2,q)}, \\ q^{\frac{m-1}{2}} \frac{(-1-G_q(\eta'))}{2}, & \text{if } \text{Tr}_{q^m/q}(\omega^a b) \in C_1^{(2,q)}, \\ \frac{q^{\frac{m-1}{2}}(q-1)}{2}, & \text{if } \text{Tr}_{q^m/q}(\omega^a b) = 0. \end{cases} \end{aligned}$$

Since  $\text{Tr}_{q^m/q}(\omega^a a_1) = \cdots = \text{Tr}_{q^m/q}(\omega^a a_{\frac{m-1}{2}}) = \text{Tr}_{q^m/q}(\omega^a b) = 0$  if and only if  $\omega^a \in A \cap H_1 \cap \cdots \cap H_{\frac{m-1}{2}}$ , the assertion of the lemma follows.  $\square$

We are now ready to prove Theorem 7.4.

**Proof of Theorem 7.4:** From Lemmas 7.5 and 7.6, we have

$$\begin{aligned} \psi_{\mathbb{F}_q^m}(\omega^a \bigcup_{t \in \widehat{X}} C_t^{(2N, q^m)}) &= \psi_{\mathbb{F}_q^m}(\omega^a D) = \sum_{i=1}^{\frac{m-1}{2}} \psi_{\mathbb{F}_q^m}(\omega^a T_\ell) + \psi_{\mathbb{F}_q^m}(\omega^a B) \\ &= \begin{cases} \frac{(-1)^{i+\epsilon} q^{\frac{m-1}{2}} (-1+(-1)^{j+\tau} G_q(\eta'))}{2}, & \text{if } \omega^a \in A_i \cap H_1 \cap \cdots \cap H_{\ell-1} \cap H_{\ell,j} \\ & \text{for } \ell = 1, \dots, \frac{m-1}{2}, i, j = 0, 1, \\ \frac{q^{\frac{m-1}{2}} (-1+(-1)^i G_q(\eta'))}{2}, & \text{if } \omega^a \in (H_1 \cap \cdots \cap H_{\frac{m-1}{2}}) \setminus A \text{ and} \\ & \text{Tr}_{q^m/q}(\omega^a b) \in C_i^{(2,q)} \text{ for } i = 0, 1, \\ 0, & \text{if } \omega^a \in A. \end{cases} \end{aligned}$$

On the other hand, since  $\psi_{\mathbb{F}_q^m}(\omega^a \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}) = \psi_{\mathbb{F}_q^m}(\omega^a D) + \psi_{\mathbb{F}_q^m}(\omega^{a+N} D)$ , we have

$$\psi_{\mathbb{F}_q^m}(\omega^a \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}) = \begin{cases} -(-1)^{i+\epsilon} q^{\frac{m-1}{2}}, & \text{if } \omega^a \in A_i \setminus (H_1 \cap \cdots \cap H_{\frac{m-1}{2}}), i = 0, 1, \\ -q^{\frac{m-1}{2}}, & \text{if } \omega^a \in (H_1 \cap \cdots \cap H_{\frac{m-1}{2}}) \setminus A. \\ 0, & \text{if } \omega^a \in A. \end{cases}$$

Hence, we have

$$2\psi_{\mathbb{F}_q^m}(\omega^a \bigcup_{t \in \widehat{X}} C_t^{(2N, q^m)}) - \psi_{\mathbb{F}_q^m}(\omega^a \bigcup_{t \in 2^{-1}I} C_t^{(N, q^m)}) = \begin{cases} 0, & \text{if } a \in 2^{-1}I \pmod{N}, \\ \pm q^{\frac{m-1}{2}} G_q(\eta'), & \text{otherwise.} \end{cases}$$



Thus, we conclude that  $\widehat{X}$  satisfies the condition (4.10) in Remark 4.3 (ii).  $\square$

As corollaries, we obtain the following.

**Corollary 7.7.** *For a prime power  $q \equiv 3 \pmod{4}$  and an odd integer  $m > 1$ , there exists a  $(q^{2m}, r(q^m + 1), -q^m + r^2 + 3r, r^2 + r)$  strongly regular Cayley graph with  $r = q^{m-1}(q - 1)/2$ .*

**Proof:** By Lemma 4.1, Remark 4.3 (i) and Theorem 7.4, the corollary now follows.  $\square$

**Remark 7.8.** The strongly regular graph obtained in Corollary 7.7 has the same parameter as the affine polar graph of elliptic type. Let  $\Gamma$  be the strongly regular graph of Corollary 7.7 with  $q = 3$  and  $m = 3$ . We checked by using a computer that  $\Gamma$  is **not** isomorphic to the affine polar graph  $AP^-$  with the same parameters. In particular, the size of the full automorphism group of  $\Gamma$  (resp.  $AP^-$ ) is  $2^2 \cdot 3^7 \cdot 7$  (resp.  $2^{10} \cdot 3^{12} \cdot 5 \cdot 7$ ).

**Corollary 7.9.** *For a prime power  $q \equiv 1 \pmod{4}$  and an odd integer  $m > 1$  such that  $\gcd(q - 1, \frac{q^m - 1}{q - 1}) = 1$ , there exists a  $(q^{2m}, r(q^m - 1), q^m + r^2 - 3r, r^2 - r)$  strongly regular Cayley graph, where  $r = q^{m-1}(q - 1)/2$ .*

**Proof:** By Lemma 4.4, Remark 4.3 (ii) and Theorem 7.4, the corollary now follows.  $\square$

**Remark 7.10.** The strongly regular graph obtained in Corollary 7.9 has the same parameters as the affine polar graph of hyperbolic type. Let  $\Gamma$  be the strongly regular graph of Corollary 7.9 with  $q = 5$  and  $m = 3$ . We checked by using a computer that  $\Gamma$  is **not** isomorphic to the affine polar graph  $AP^+$  with the same parameters. In particular, the size of the full automorphism group of  $\Gamma$  (resp.  $AP^+$ ) is  $2^3 \cdot 5^6 \cdot 31$  (resp.  $2^{11} \cdot 3^2 \cdot 5^{12} \cdot 13 \cdot 31$ ).

## REFERENCES

- [1] B. Berndt, R. Evans, K.S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
- [2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*. Vol. I. Second edition. Encyclopedia of Mathematics and its Applications, 78. Cambridge University Press, Cambridge, 1999.
- [3] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, Springer, New York, 2012.
- [4] J. Bamberg, M. Lee, K. Momihara, Q. Xiang, A new infinite family of Hemisystems of the Hermitian surface, *Combinatorica*, to appear.
- [5] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.*, **18** (1986), 97–122.
- [6] J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in  $\mathcal{Q}^+(5, q)$ , *Des. Codes Cryptogr.* **78** (2016), 655–678.
- [7] T. Feng, K. Momihara, Q. Xiang, Cameron-Liebler line classes with parameter  $x = \frac{q^2 - 1}{2}$ , *J. Combin. Theory (A)* **133** (2015), 307–338.
- [8] R. A. Games, The geometry of quadrics and correlations of sequences, *IEEE Trans. Inform. Theory* **IT-32**, (1986), 423–426.
- [9] C. Godsil, G. Royle, *Algebraic Graph Theory*, GTM 207, Springer-Verlag, 2001.
- [10] E. S. Lander, *Symmetric designs: an algebraic approach*, Cambridge University Press, 1983.
- [11] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.
- [12] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.
- [13] R. L. McFarland, Sub-difference sets of Hadamard difference sets, *J. Combin. Theory (A)* **54** (1990), 112–122.
- [14] K. Momihara, New strongly regular decompositions of the complete graphs with prime power vertices, *Finite Fields Appl.* **36** (2015), 63–80.
- [15] K. Momihara, Q. Xiang, Lifting construction of strongly regular Cayley graphs, *Finite Fields Appl.* **26** (2014), 86–99.
- [16] B. Schmidt, C. White, All two-weight irreducible cyclic codes? *Finite Fields Appl.* **8** (2002), 321–367.
- [17] K. Yamamoto, On Jacobi sums and difference sets, *J. Combin. Theory (A)* **3** (1967), 146–181.

## APPENDIX: PROOF OF LEMMA 7.5

In this appendix, we give a proof of Lemma 7.5.

**Proof of Lemma 7.5.** For  $j = 0$  or  $1$ , the characteristic function  $g_{A,j}$  of  $\{x \in \mathbb{F}_{q^m} \mid \text{Tr}_{q^m/q}(x^2) \in C_j^{(2,q)}\}$  is given by

$$g_{A,j}(x) = \frac{1}{q} \sum_{d \in \mathbb{F}_q} \sum_{s \in C_j^{(2,q)}} \psi_{\mathbb{F}_{q^m}}(dx^2) \psi_{\mathbb{F}_q}(-ds). \quad (7.7)$$

Similarly, the characteristic functions  $g_{a_\ell}$  and  $g_{a_\ell,j}$  of  $\{x \mid \text{Tr}_{q^m/q}(xa_\ell) = 0\}$  and  $\{x \mid \text{Tr}_{q^m/q}(xa_\ell) \in C_j^{(2,q)}\}$  are, respectively, given by

$$g_{a_\ell}(x) = \frac{1}{q} \sum_{d \in \mathbb{F}_q} \psi_{\mathbb{F}_{q^m}}(dxa_\ell) \quad (7.8)$$

and

$$g_{a_\ell,j}(x) = \frac{1}{q} \sum_{d \in \mathbb{F}_q} \sum_{s \in C_j^{(2,q)}} \psi_{\mathbb{F}_{q^m}}(dxa_\ell) \psi_{\mathbb{F}_q}(-ds), \quad j = 0, 1. \quad (7.9)$$

We compute the character values  $\psi_{\mathbb{F}_{q^m}}(\omega^a T_\ell)$ . By the definition of  $T_\ell$ , we have

$$\psi_{\mathbb{F}_{q^m}}(\omega^a T_\ell) = \sum_{j=0,1} \sum_{x \in \mathbb{F}_{q^m}} g_{A,j}(x) g_{a_1}(x) \cdots g_{a_{\ell-1}}(x) g_{a_\ell,j}(x) \psi_{\mathbb{F}_{q^m}}(\omega^a x) \quad (7.10)$$

By substituting (7.7), (7.8) and (7.9) into (7.10), we have

$$\psi_{\mathbb{F}_{q^m}}(\omega^a T_\ell) = \frac{1}{q^{\ell+1}} \sum_{x \in \mathbb{F}_{q^m}} \sum_{j=0,1} \sum_{d_0, d_1, \dots, d_\ell \in \mathbb{F}_q} \psi_{\mathbb{F}_{q^m}}(d_0 x^2 + (\omega^a + \sum_{i=1}^{\ell} d_i a_i) x) \psi_{\mathbb{F}_q}(d_0 C_j^{(2,q)}) \psi_{\mathbb{F}_q}(d_\ell C_j^{(2,q)}). \quad (7.11)$$

We compute the right hand side of (7.11) by dividing into the two partial sums:  $\Sigma_1$  and  $\Sigma_2$ , where  $\Sigma_1$  is the contribution of the summands with  $d_0 = 0$  and  $\Sigma_2$  is the contribution of the summands with  $d_0 \neq 0$ . Thus,  $\psi_{\mathbb{F}_{q^m}}(\omega^a T_\ell) = \Sigma_1 + \Sigma_2$ .

It is clear that

$$\begin{aligned} \Sigma_1 &= \frac{q-1}{2q^{\ell+1}} \sum_{x \in \mathbb{F}_{q^m}} \sum_{j=0,1} \sum_{d_1, \dots, d_\ell \in \mathbb{F}_q} \psi_{\mathbb{F}_{q^m}}((\omega^a + \sum_{i=1}^{\ell} d_i a_i) x) \psi_{\mathbb{F}_q}(d_\ell C_j^{(2,q)}) \\ &= \begin{cases} \frac{-q^{m-\ell-1}(q-1)}{2}, & \text{if } \omega^a \in \langle a_1, \dots, a_\ell \rangle \setminus \langle a_1, \dots, a_{\ell-1} \rangle, \\ \frac{q^{m-\ell-1}(q-1)^2}{2}, & \text{if } \omega^a \in \langle a_1, \dots, a_{\ell-1} \rangle, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

We next consider the partial sum  $\Sigma_2$ . By Theorem 2.6,

$$\Sigma_2 = \frac{G_{q^m}(\eta)}{q^{\ell+1}} \sum_{j=0,1} \sum_{d_0 \in \mathbb{F}_q^*} \sum_{d_1, \dots, d_\ell \in \mathbb{F}_q} \psi_{\mathbb{F}_{q^m}}(-4^{-1} d_0^{-1} (\omega^a + \sum_{i=1}^{\ell} d_i a_i)^2) \eta(d_0) \psi_{\mathbb{F}_q}(d_0 C_j^{(2,q)}) \psi_{\mathbb{F}_q}(d_\ell C_j^{(2,q)}), \quad (7.12)$$

where  $\eta$  is the quadratic character of  $\mathbb{F}_{q^m}$ . Since  $\text{Tr}_{q^m/q}(a_i a_j) = 0$  for  $i, j \in \{1, \dots, \ell\}$ , we have

$$\text{Tr}_{q^m/q}((\omega^a + \sum_{i=1}^{\ell} d_i a_i)^2) = \text{Tr}_{q^m/q}(\omega^{2a} + 2\omega^a \sum_{i=1}^{\ell} d_i a_i).$$

Continuing from (7.12), we have

$$\Sigma_2 = \frac{G_{q^m}(\eta)}{q^{\ell+1}} \sum_{j=0,1} \sum_{h=0,1} (-1)^h \psi_{\mathbb{F}_q}(C_{j+h}^{(2,q)}) \sum_{d_1, \dots, d_\ell \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(-\text{Tr}_{q^m/q}(\omega^{2a} + 2\omega^a \sum_{i=1}^{\ell} d_i a_i) C_h^{(2,q)}) \psi_{\mathbb{F}_q}(d_\ell C_j^{(2,q)}).$$

If  $\text{Tr}_{q^m/q}(\omega^a a_i) \neq 0$  for some  $i = 1, 2, \dots, \ell - 1$ , it is clear that  $\Sigma_2 = 0$ . Furthermore, if  $\text{Tr}_{q^m/q}(\omega^a a_\ell) = 0$ , it also holds that  $\Sigma_2 = 0$ . Thus, we assume that  $\text{Tr}_{q^m/q}(\omega^a a_i) = 0$  for all  $i = 1, 2, \dots, \ell - 1$  and  $\text{Tr}_{q^m/q}(\omega^a a_\ell) \neq 0$ . In this case, we have

$$\Sigma_2 = \frac{G_{q^m}(\eta)}{q^2} \sum_{j=0,1} \sum_{h=0,1} (-1)^h \psi_{\mathbb{F}_q}(C_{j+h}^{(2,q)}) \sum_{d_\ell \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(-\text{Tr}_{q^m/q}(\omega^{2a} + 2\omega^a d_\ell a_\ell) C_h^{(2,q)}) \psi_{\mathbb{F}_q}(d_\ell C_j^{(2,q)}). \quad (7.13)$$

We compute the right hand side of (7.13) by dividing into the two partial sums:  $\Sigma_{2,0}$  and  $\Sigma_{2,1}$ , where  $\Sigma_{2,0}$  is the contribution of the summands with  $d_\ell = 0$  and  $\Sigma_{2,1}$  is the contribution of the summands with  $d_\ell \neq 0$ . Thus,  $\Sigma_2 = \Sigma_{2,0} + \Sigma_{2,1}$ .

By (2.3), we have

$$\begin{aligned} \Sigma_{2,0} &= \frac{(q-1)G_{q^m}(\eta)}{2q^2} \sum_{j=0,1} \sum_{h=0,1} (-1)^h \psi_{\mathbb{F}_q}(C_{j+h}^{(2,q)}) \psi_{\mathbb{F}_q}(-\text{Tr}_{q^m/q}(\omega^{2a}) C_h^{(2,q)}) \\ &= -\frac{(q-1)G_{q^m}(\eta)}{2q^2} \begin{cases} G_q(\eta'), & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_0^{(2,q)}, \\ -G_q(\eta'), & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_1^{(2,q)}, \\ 0, & \text{if } \text{Tr}_{q^m/q}(\omega^{2a}) = 0, \end{cases} \end{aligned}$$

where  $\eta'$  is the quadratic character of  $\mathbb{F}_q$ . On the other hand, by (2.3),

$$\begin{aligned} \Sigma_{2,1} &= \frac{G_{q^m}(\eta)}{q^2} \sum_{j,h,k=0,1} (-1)^h \psi_{\mathbb{F}_q}(C_{j+h}^{(2,q)}) \psi_{\mathbb{F}_q}(-\text{Tr}_{q^m/q}(\omega^{2a}) C_h^{(2,q)}) \psi_{\mathbb{F}_q}(-2\text{Tr}_{q^m/q}(\omega^a a_\ell) C_{h+k}^{(2,q)}) \psi_{\mathbb{F}_q}(C_{j+k}^{(2,q)}) \\ &= \frac{G_{q^m}(\eta)}{q^2} \begin{cases} \frac{G_q(\eta')(-1+G_q(\eta')^3)}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_0^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_0^{(2,q)}, \\ \frac{-G_q(\eta')(1+G_q(\eta')^3)}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_0^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_1^{(2,q)}, \\ \frac{-G_q(\eta')(-1+G_q(\eta')^3)}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_1^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_0^{(2,q)}, \\ \frac{G_q(\eta')(1+G_q(\eta')^3)}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_1^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_1^{(2,q)}, \\ 0, & \text{if } \text{Tr}_{q^m/q}(\omega^{2a}) = 0. \end{cases} \end{aligned}$$

Noting that  $G_{q^m}(\eta) = G_q(\eta')^m$  and  $G_q(\eta')^2 = (-1)^\epsilon q$ , we have

$$\begin{aligned} \Sigma_2 &= \Sigma_{2,0} + \Sigma_{2,1} \\ &= (-1)^{\epsilon \frac{m+1}{2}} q^{\frac{m-1}{2}} \begin{cases} \frac{-1+(-1)^\epsilon G_q(\eta')}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_0^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_0^{(2,q)}, \\ \frac{-1-(-1)^\epsilon G_q(\eta')}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_0^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_1^{(2,q)}, \\ \frac{1-(-1)^\epsilon G_q(\eta')}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_1^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_0^{(2,q)}, \\ \frac{1+(-1)^\epsilon G_q(\eta')}{2}, & \text{if } -\text{Tr}_{q^m/q}(\omega^{2a}) \in C_1^{(2,q)}, -2\text{Tr}_{q^m/q}(\omega^a a_\ell) \in C_1^{(2,q)}, \\ 0, & \text{if } \text{Tr}_{q^m/q}(\omega^{2a}) = 0. \end{cases} \end{aligned}$$

This completes the proof of the lemma.  $\square$

KOJI MOMIHARA, FACULTY OF EDUCATION, KUMAMOTO UNIVERSITY, 2-40-1 KUROKAMI, KUMAMOTO 860-8555, JAPAN

*E-mail address:* momihara@educ.kumamoto-u.ac.jp

QING XIANG, DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF DELAWARE, NEWARK, DE 19716, USA

*E-mail address:* qxiang@udel.edu