GENERALIZED CONSTRUCTIONS OF MENON-HADAMARD DIFFERENCE SETS

KOJI MOMIHARA† AND QING XIANG∗

ABSTRACT. We revisit the problem of constructing Menon-Hadamard difference sets. In 1997, Wilson and Xiang gave a general framework for constructing Menon-Hadamard difference sets by using a combination of a spread and four projective sets of type Q in PG(3, q). They also found examples of suitable spreads and projective sets of type Q for q = 5, 13, 17. Subsequently, Chen (1997) succeeded in finding a spread and four projective sets of type Q in PG(3, q) satisfying the conditions in the Wilson-Xiang construction for all odd prime powers q. Thus, he showed that there exists a Menon-Hadamard difference set of order 4q^2 for all odd prime powers q. However, the projective sets of type Q found by Chen have automorphisms different from those of the examples constructed by Wilson and Xiang. In this paper, we first generalize Chen’s construction of projective sets of type Q by using “semi-primitive” cyclotomic classes. This demonstrates that the construction of projective sets of type Q satisfying the conditions in the Wilson-Xiang construction is much more flexible than originally thought. Secondly, we give a new construction of spreads and projective sets of type Q in PG(3, q) for all odd prime powers q, which generalizes the examples found by Wilson and Xiang. This solves a problem left open in Section 5 of the Wilson-Xiang paper from 1997.

1. Introduction

Let G be an additively written abelian group of order v. A k-subset D of G is called a (v, k, λ) difference set if the list of differences “x − y, x, y ∈ D, x ≠ y”, represents each nonidentity element of G exactly λ times. In this paper, we revisit the problem of constructing Menon-Hadamard difference sets, namely those difference sets with parameters (v, k, λ) = (4m^2, 2m^2 − m, m^2 − m), where m is a positive integer. It is well known that a Menon-Hadamard difference set generates a regular Hadamard matrix of order 4m^2. So by constructing Menon-Hadamard difference sets in groups of order 4m^2, we obtain regular Hadamard matrices of order 4m^2.

The main problem in the study of Menon-Hadamard difference sets is: For each positive integer m, which groups of order 4m^2 contain a Menon-Hadamard difference set. We give a brief survey of results on this problem in the case where the group under consideration is abelian. First we mention a product theorem of Turyn [11]: If there are Menon-Hadamard difference sets in abelian groups H × G_1 and H × G_2, respectively, where |H| = 4 and |G_i|, i = 1, 2, are squares, then there also exists a Menon-Hadamard difference set in H × G_1 × G_2. With Turyn’s product theorem in hand, in order to construct Menon-Hadamard difference sets, one should start with the case where the order of the abelian group is 4q with q an even power of a prime. In the case where q is an even power of 2, that is, G is an abelian 2-group, the existence problem was completely solved in [8] after much work was done in [3]; it was shown that there exists a Menon-Hadamard difference set in an abelian group G of order 2^{2t+2} if and only if the exponent of G is less than or equal to 2^{t+2}.

In the case where q is an even power of an odd prime, Turyn [11] observed that there exists a Menon-Hadamard difference set in H × (Z_3)^2; hence by the product theorem, there is a Menon-Hadamard difference set in H × (Z_3)^2t for any positive integer t. On the other hand, McFarland

† Koji Momihara was supported by JSPS under Grant-in-Aid for Young Scientists (B) 17K14236 and Scientific Research (B) 15H03636.
∗ Qing Xiang was supported by an NSF grant DMS-1600850.
proved that if an abelian group of order \(4p^2\), where \(p\) is a prime, contains a Menon-Hadamard difference set, then \(p = 2\) or \(3\). After McFarland’s paper \([10]\) was published, it was conjectured \([7\text{ p. } 287]\) that if an abelian group of order \(4m^2\) contains a Menon-Hadamard difference set, then \(m = 2^r3^s\) for some nonnegative integers \(r\) and \(s\). So it was a great surprise when Xia \([13]\) constructed a Menon-Hadamard difference set in \(H \times \mathbb{Z}_p^4\) for any odd prime \(p\) congruent to 3 modulo 4. Xia’s method of construction depends on very complicated computations involving cyclotomic classes of finite fields; it was later simplified by Xiang and Chen \([14]\) by using a character theoretic approach. Moreover, in \([14]\), the authors also asked whether a certain family of 3-weight projective linear code exists or not, since such projective linear codes are needed for the construction of Menon-Hadamard difference set in the group \(H \times (\mathbb{Z}_p)^4\), where \(p\) is a prime congruent to 1 modulo 4.

Van Eupen and Tonchev \([6]\) found the required 3-weight projective linear codes when \(p = 5\), hence constructed Menon-Hadamard difference sets in \(\mathbb{Z}_2^2 \times \mathbb{Z}_4^3\), which are the first examples of abelian Menon-Hadamard difference sets in groups of order \(4p^4\), where \(p\) is a prime congruent to 1 modulo 4. Inspired by these examples, Wilson and Xiang \([12]\) gave a general framework for constructing Menon-Hadamard difference sets in the groups \(H \times G\), where \(H\) is either group of order 4 and \(G\) is an elementary abelian group of order \(q^4\), \(q\) an odd prime power, using a combination of a spread and four projective sets of type Q in PG(3, \(q\)). (See Section 2.2 for the definition of projective sets of type Q.) Wilson and Xiang \([12]\) also found examples of suitable spreads and the required projective sets of type Q when \(q = 5, 13, 17\). They used \(\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}\) as a model of the four-dimensional vector space \(V(4,q)\) over \(\mathbb{F}_q\), and considered projective sets of type Q with the automorphism

\[
T' = \begin{pmatrix}
\omega^2 & 0 \\
0 & \omega^{-2}
\end{pmatrix},
\]

where \(\omega\) is a primitive element of \(\mathbb{F}_{q^2}\). However, the existence of the required projective sets of type Q with this prescribed automorphism remained unsolved for \(q > 17\).

Immediately after \([12]\) appeared, Chen \([4]\) succeeded in showing the existence of a combination of a spread and four projective sets of type Q in PG(3, \(q\)) satisfying the conditions in the Wilson-Xiang construction for all odd prime powers \(q\). As a consequence, Chen \([4]\) obtained the following theorem by applying Turyn’s product theorem in \([11]\).

**Theorem 1.1.** Let \(p_i, i = 1, 2, \ldots, s\), be odd primes and \(t_i, i = 1, 2, \ldots, s\), be positive integers. Furthermore, let \(H\) be either group of order 4 and \(G_i, i = 1, 2, \ldots, s\), be an elementary abelian group of order \(p_i^{4t_i}\). Then, there exists a Menon-Hadamard difference set in \(H \times G_1 \times G_2 \times \cdots \times G_s\).

Here, Chen \([4]\) found projective sets of type Q in PG(3, \(q\)) with the following automorphism

\[
T = \begin{pmatrix}
\omega^2 & 0 \\
0 & \omega^2
\end{pmatrix},
\]

which is obviously different from that of the projective sets of type Q found by Wilson and Xiang \([12]\). Thus, the existence problem of projective sets of type Q in PG(3, \(q\)) with the prescribed automorphism \(T'\) remained open.

The objectives of this paper are two-fold. First, we give a generalization of Chen’s construction of projective sets of type Q by using “semi-primitive” cyclotomic classes. This demonstrates that the construction of projective sets of type Q satisfying the conditions in the Wilson-Xiang construction is much more flexible than originally thought. In particular, the proof of the candidate sets are projective sets of type Q is much simpler than that in \([4]\). Second, we show the existence of a combination of a spread and four projective sets of type Q with automorphism \(T'\) for all odd prime powers \(q\). Our construction generalizes the examples found by Wilson and Xiang in \([12]\); this solves the problem left open in Section 5 of \([12]\).
2. Preliminaries

2.1. Characters of finite fields. In this subsection, we collect some auxiliary results on characters of finite fields. We assume that the reader is familiar with basic theory of characters of finite fields as in [9 Chapter 5].

Let $p$ be a prime and $s, f$ be positive integers. We set $q = p^s$, and denote the finite field of order $q$ by $\mathbb{F}_q$. Let $\text{Tr}_{q^f/q}$ be the trace map from $\mathbb{F}_{q^f}$ to $\mathbb{F}_q$, which is defined by

$$\text{Tr}_{q^f/q}(x) = x + x^q + \cdots + x^{q^{f-1}}, \quad x \in \mathbb{F}_{q^f}.$$ 

Let $\omega$ be a fixed primitive element of $\mathbb{F}_q$, $\zeta_{p}$ a fixed (complex) primitive $p$th root of unity, and $\zeta_{q-1}$ a (complex) $q-1$th root of unity. The character $\psi_{\mathbb{F}_q}$ of the additive group of $\mathbb{F}_q$, defined by $\psi_{\mathbb{F}_q}(x) = \zeta_{q}^{\text{Tr}_{q^f/p}(x)}, \quad x \in \mathbb{F}_q$, is called the canonical additive character of $\mathbb{F}_q$. Then, each additive character is given by $\psi_a(x) = \psi_{\mathbb{F}_q}(ax), \quad x \in \mathbb{F}_q$, where $a \in \mathbb{F}_q$. On the other hand, each multiplicative character is given by $\chi_j(\omega^k) = \zeta_{q}^{jk}, \quad \ell = 0, 1, \ldots, q-2$, where $j = 0, 1, \ldots, q-2$.

For a multiplicative character $\chi$ of $\mathbb{F}_q$, the character sum defined by

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

is called a Gauss sum of $\mathbb{F}_q$. Gauss sums satisfy the following basic properties: (1) $G_q(\chi\overline{\chi}) = q$ if $\chi$ is nontrivial; (2) $G_q(\chi^{-1}) = \chi(-1)\overline{G_q(\chi)}$; (3) $G_q(\chi) = -1$ if $\chi$ is trivial.

In general, explicit evaluations of Gauss sums are difficult. There are only a few cases that the Gauss sums have been completely evaluated. The most well-known case is the quadratic case, i.e., the order of the multiplicative character involved is 2.

**Theorem 2.1.** ([9 Theorem 5.15]) Let $\eta$ be the quadratic character of $\mathbb{F}_q = \mathbb{F}_{p^s}$. Then,

$$G_q(\eta) = (-1)^{s-1} \left( \sqrt{(-1)^{p-1} p} \right)^s.$$ 

The next simple case is the so-called semi-primitive case, where there exists an integer $\ell$ such that $p^\ell \equiv -1 \pmod{N}$. Here, $N$ is the order of the multiplicative character involved. In particular, we will give the following for later use.

**Theorem 2.2.** ([9 Theorem 5.16]) Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_{q^2}$ of order $N$ dividing $q+1$. Then,

$$G_{q^2}(\chi) = \begin{cases} q, & \text{if } N \text{ odd or } \frac{q+1}{N} \text{ even,} \\ -q, & \text{if } N \text{ even and } \frac{q+1}{N} \text{ odd.} \end{cases}$$

We will also need the Davenport-Hasse product formula, which is stated below.

**Theorem 2.3.** ([2 Theorem 11.3.5]) Let $\chi'$ be a multiplicative character of order $\ell > 1$ of $\mathbb{F}_q$. For every nontrivial multiplicative character $\chi$ of $\mathbb{F}_q$,

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

Let $N$ be a positive integer dividing $q-1$. We set $C_{i}^{(N,q)} = \omega^i(\omega^N), \quad 0 \leq i \leq N-1$, which are called the $N$th cyclotomic classes of $\mathbb{F}_q$. In this paper, we need to evaluate the (additive) character values of a union of some cyclotomic classes. In particular, the character sums defined by

$$\psi_{\mathbb{F}_q}(C_{i}^{(N,q)}) = \sum_{x \in C_{i}^{(N,q)}} \psi_{\mathbb{F}_q}(x), \quad i = 0, 1, \ldots, N-1,$$
are called the $N$th Gaus**s periods of $\mathbb{F}_q$. By the orthogonality of characters, the Gauss period can be expressed as a linear combination of Gauss sums:

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

(2.1)

where $\chi$ is any fixed multiplicative character of order $N$ of $\mathbb{F}_q$. For example, if $N = 2$, we have the following from Theorem 2.1:

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

(2.2)

where $\eta$ is the quadratic character of $\mathbb{F}_q$. On the other hand, the Gauss sum with respect to a multiplicative character $\chi$ of order $N$ can be expressed as a linear combination of Gauss periods:

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

(2.3)

2.2. Known results on projective sets of type Q. Let $\text{PG}(k - 1, q)$ denote the $(k-1)$-dimensional projective space over $\mathbb{F}_q$. A set $\mathcal{S}$ of $n$ points of $\text{PG}(k - 1, q)$ is called a projective $(n, k, h_1, h_2)$ set if every hyperplane of $\text{PG}(k - 1, q)$ meets $\mathcal{S}$ in $h_1$ or $h_2$ points. In particular, a subset $\mathcal{S}$ of the point set of $\text{PG}(3, q)$ is called type Q if

$$(n, k, h_1, h_2) = \left( \frac{q^4 - 1}{4(q-1)}, 4, \frac{(q-1)^2}{4}, \frac{(q+1)^2}{4} \right).$$

In this paper, we will use the following model of $\text{PG}(3, q)$: We view $\mathbb{F}_q^2 \times \mathbb{F}_q^2$ as a 4-dimensional vector space over $\mathbb{F}_q$. For a nonzero vector $(x, y) \in (\mathbb{F}_q^2 \times \mathbb{F}_q^2) \setminus \{(0, 0)\}$, we use $\langle (x, y) \rangle$ to denote the projective point in $\text{PG}(3, q)$ corresponding to the one-dimensional subspace over $\mathbb{F}_q$ spanned by $(x, y)$. Let $\mathcal{P}$ be the set of points of $\text{PG}(3, q)$. Then, all (hyper)planes in $\text{PG}(3, q)$ are given by

$$H_{a,b} = \{ \langle (x, y) \rangle | Tr_{q^2/q}(ax + by) = 0 \}, \quad \langle (a, b) \rangle \in \mathcal{P}.$$

Let $\mathcal{S}$ be a set of points of $\text{PG}(3, q)$, and define

$$E = \{ \lambda \langle x, y \rangle | \lambda \in \mathbb{F}_q^*, \langle (x, y) \rangle \in \mathcal{S} \}.$$

Noting that each nontrivial additive character of $\mathbb{F}_q^2 \times \mathbb{F}_q^2$ is given by

$$\psi_{a,b}(\langle x, y \rangle) = \psi_{\mathbb{F}_q}(ax + by), \quad (x, y) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2,$$

where $(0, 0) \neq (a, b) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2$, we have

$$\psi_{a,b}(E) = \sum_{\lambda \in \mathbb{F}_q} \sum_{\langle (x, y) \rangle \in \mathcal{S}} \psi_{\mathbb{F}_q}(\lambda Tr_{q^2/q}(ax + by)) - |\mathcal{S}|$$

$$q |H_{a,b} \cap \mathcal{S}| - |\mathcal{S}|.$$

Hence, we have the following proposition.

**Proposition 2.4.** The set $\mathcal{S}$ is a projective set of type Q in $\text{PG}(3, q)$ if and only if $|E| = \frac{q^4 - 1}{4}$ and $\psi_{a,b}(E)$ take exactly two values $\frac{q^4 - 1}{4}$ and $\frac{-3q^4 + 1}{4}$ for all $(0, 0) \neq (a, b) \in \mathbb{F}_q^2 \times \mathbb{F}_q^2$.

The set $E \subseteq \mathbb{F}_q^2 \times \mathbb{F}_q^2$ is also called type Q if it satisfies the condition of Proposition 2.4.

A spread in $\text{PG}(3, q)$ is a collection $\mathcal{L}$ of $q^2 + 1$ pairwise skew lines; equivalently, $\mathcal{L}$ can be regarded as a collection $\mathcal{K}$ of 2-dimensional subspaces of the underlying 4-dimensional vector space $\mathbb{V}(4, q)$ over $\mathbb{F}_q$, any two of which intersect at zero only. We also call such a set $\mathcal{K}$ of 2-dimensional subspaces as a spread of $\mathbb{V}(4, q)$.

The following important theorem was given by Wilson and Xiang [12].
Theorem 2.5. Let \( \mathcal{L} = \{ L_i \mid 0 \leq i \leq q^2 \} \) be a spread of \( \text{PG}(3,q) \), and assume the existence of four pairwise disjoint projective sets \( \mathcal{S}_i, i = 1, 2, 3, 4 \), of type Q in \( \text{PG}(3,q) \) such that \( \mathcal{S}_0 \cup \mathcal{S}_2 = \bigcup_{i=0}^{q^2-1/2} L_i \) and \( \mathcal{S}_1 \cup \mathcal{S}_3 = \bigcup_{i=(q^2+1)/2}^{q^2} L_i \). Then there exists a Menon-Hadamard difference set in \( H \times G \), where \( H \) is either group of order 4 and \( G \) is an elementary abelian group of order \( q^4 \).

Remark 2.6. From Proposition 2.4 and Theorem 2.5, in order to construct a Menon-Hadamard difference set in a group of order \( q \), we need to find four disjoint sets \( C_i \subseteq (\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}) \setminus \{(0,0)\}, i = 0, 1, 2, 3 \), of type Q and a suitable spread \( \mathcal{K} = \{ K_i \mid 0 \leq i \leq q^2 \} \) consisting of 2-dimensional subspaces of \( V(4,q) \) such that \( C_0 \cup C_2 \cup \{(0,0)\} = \bigcup_{i=0}^{q^2-1/2} K_i \) and \( C_1 \cup C_3 \cup \{(0,0)\} = \bigcup_{i=(q^2+1)/2}^{q^2} K_i \).

We now review the construction of projective sets of type Q given by Chen [4]. Let \( \omega \) be a primitive element of \( \mathbb{F}_{q^2} \). Furthermore, let
\[
X = \{ x \in \mathbb{F}_{q^2} \mid \text{Tr}_{q^2/q}(x) \in C_0^{(2,q)} \}, \quad X' = \{ x\omega \mid \text{Tr}_{q^2/q}(x) \in C_0^{(2,q)} \}.
\]
Define
\[
X_1 = X \setminus (X \cap X'), \quad X_2 = X' \setminus (X \cap X'),
\]
\[
X_3 = X \cap X', \quad X_4 = \mathbb{F}_{q^2} \setminus (X_1 \cup X_2 \cup X_3),
\]
and
\[
C_0 = \{ (x,xy) \mid x \in C_0^{(2,q)}, y \in X_1 \} \cup \{ (x,xy) \mid x \in C_1^{(2,q)}, y \in X_2 \} \cup \{ (0,x) \mid x \in C_2^{(2,q)} \},
\]
\[
C_1 = \{ (x,xy) \mid x \in C_0^{(2,q)}, y \in X_3 \} \cup \{ (x,xy) \mid x \in C_1^{(2,q)}, y \in X_4 \},
\]
\[
C_2 = \{ (x,xy) \mid x \in C_1^{(2,q)}, y \in X_1 \} \cup \{ (x,xy) \mid x \in C_0^{(2,q)}, y \in X_2 \} \cup \{ (0,x) \mid x \in C_2^{(2,q)} \},
\]
\[
C_3 = \{ (x,xy) \mid x \in C_1^{(2,q)}, y \in X_3 \} \cup \{ (x,xy) \mid x \in C_0^{(2,q)}, y \in X_4 \},
\]
where \( \tau = 0 \) or 1 depending on whether \( q \equiv 1 \) or 3 (mod 4). It is clear that these type Q sets admit the automorphism \( T \).

Theorem 2.7. The sets \( C_i, i = 0, 1, 2, 3 \), are type Q. Furthermore, these sets satisfy the assumption of Remark 2.6 with respect to the spread \( \mathcal{K} \) consisting of the following 2-dimensional subspaces:
\[
K_y = \{ (x,xy) \mid x \in \mathbb{F}_{q^2} \}, \quad y \in \mathbb{F}_{q^2}, \quad \text{and} \quad K_\infty = \{ (0,x) \mid x \in \mathbb{F}_{q^2} \}.
\]

On the other hand, Wilson and Xiang [12] constructed Menon-Hadamard difference sets of order \( 4q^4 \) for \( q = 5, 13, 17 \) using the following four type Q sets:
\[
C_i = \{ (0,y) \mid y \in C_1^{(2,q)} \} \cup \{ (x,xy^{-1}\omega^j) \mid x \in \mathbb{F}_{q^2}^*, y \in C_0^{(2,q)}, j \in A_i \}
\]
\[
\quad \cup \{ (xy,xy^{-1}\omega^j) \mid x \in \mathbb{F}_{q^2}^*, y \in C_1^{(2,q)}, j \in B_i \}, \quad i = 0, 2,
\]
\[
C_i = \{ (y,0) \mid y \in C_0^{(2,q)} \} \cup \{ (x,xy^{-1}\omega^j) \mid x \in \mathbb{F}_{q^2}^*, y \in C_0^{(2,q)}, j \in A_i \}
\]
\[
\quad \cup \{ (xy,xy^{-1}\omega^j) \mid x \in \mathbb{F}_{q^2}^*, y \in C_1^{(2,q)}, j \in B_i \}, \quad i = 1, 3,
\]
for some subsets \( A_i, B_i, i = 0, 1, 2, 3 \), of \( \{0,1,\ldots,2q+1\} \), and the spread \( \mathcal{K} \) consisting of the following 2-dimensional subspaces:
\[
K_y = \{ (x,yx^q) \mid x \in \mathbb{F}_{q^2} \}, \quad y \in \mathbb{F}_{q^2}, \quad \text{and} \quad K_\infty = \{ (0,x) \mid x \in \mathbb{F}_{q^2} \}.
\]
It is clear that these type Q sets admit the automorphism \( T' \).
3. A generalization of Chen’s construction

We first fix notation used in this section. Let \( q = p^e \) be an odd prime power with \( p \) a prime, and \( m \) be a fixed positive integer satisfying \( 2m \mid (q + 1) \). Then, there exists a minimal \( \ell \) such that \( 2m \mid (p^\ell + 1) \). Write \( s = \ell t \) for some \( t \geq 1 \). Let \( \omega \) be a primitive element of \( \mathbb{F}_{q^2} \). Let \( T_i, \ i = 0, 1, \) be two arbitrary subsets of \( \mathbb{F}_q \), and

\[
S_0 = \{ x \mid \text{Tr}_{q^2/q}(x) \in T_0 \}, \quad S_1 = \{ x \mid \text{Tr}_{q^2/q}(x \omega^m) \in T_1 \}. \tag{3.1}
\]

Furthermore, let \( K \) be any \( m \)-subset of \( \{0, 1, \ldots, 2m - 1\} \) such that \( K \cap \{x + m \mod 2m \mid x \in K\} = \emptyset \). Define

\[
A_0 = S_0 \setminus S_1, \quad A_1 = S_1 \setminus S_0, \quad D_0 = \bigcup_{i \in K} C_{i}^{(2m,q^2)}, \quad D_1 = \bigcup_{i \in K} C_{i+m}^{(2m,q^2)} \tag{3.2}
\]

and

\[
\epsilon := \begin{cases} 1, & \text{if } (p^\ell + 1)/2m \text{ is even and } t \text{ is odd,} \\ 0, & \text{otherwise.} \end{cases}
\]

Remark 3.1. (i) The indicator function of \( S_i, \ i = 0, 1, \) is given by

\[
f_{S_i}(y) = \frac{1}{q^2} \sum_{c \in \mathbb{F}_q} \sum_{u \in T_i} \psi_{q^2}(cy \omega^m) \psi_{q^2}(-cu), \quad i = 0, 1.
\]

(ii) The size of each \( S_i \) is \( q |T_i| \) since \( \text{Tr}_{q^2/q} \) is a linear mapping over \( \mathbb{F}_q \).

(iii) The size of \( S_0 \cap S_1 \) is \( |T_0||T_1| \); it is clear that

\[
|S_0 \cap S_1| = \sum_{y \in \mathbb{F}_{q^2}} f_{S_0}(y)f_{S_1}(y)
= \frac{1}{q^2} \sum_{c,d \in \mathbb{F}_q} \sum_{u \in T_0} \sum_{v \in T_1} \sum_{y \in \mathbb{F}_{q^2}} \psi_{q^2}(y(c + d \omega^m)) \psi_{q^2}(-cu - dv). \tag{3.3}
\]

Since \( \omega^m \notin \mathbb{F}_q \), \( c + d \omega^m = 0 \) if and only if \( c = d = 0 \). Hence, the right-hand side of (3.3) is equal to \( |T_0||T_1| \).

(iv) Since \( 2m \mid (q + 1) \), the character values of \( D_i \subseteq \mathbb{F}_{q^2}, \ i = 0, 1, \) can be evaluated by using (2.1) and the Gauss sums in semi-primitive case (see, e.g., [3] Theorem 2): for \( b \in \mathbb{F}_{q^2}^* \),

\[
\sum_{x \in D_i} \psi_{q^2}(bx) = \begin{cases} \frac{-1-y}{2} q, & \text{if } b^{-1} \in D_0, \\ \frac{-1+y}{2} q, & \text{if } b^{-1} \in D_1. \end{cases}
\]

The following is our main result in this section.

Theorem 3.2. (1) Assume that \( |T_0| = |T_1| = (q - 1)/2 \), and define

\[
E_0 = \{(x, xy) \mid x \in D_0, y \in A_0\} \cup \{(x, xy) \mid x \in D_1, y \in A_1\} \cup \{(0, x) \mid x \in D_i\}.
\]

Then \( E_0 \) is a set of type \( Q \) in \( \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \).

(2) Assume that \( |T_0| = (q - 1)/2 \) and \( |T_1| = (q + 1)/2 \), and define

\[
E_1 = \{(x, xy) \mid x \in D_0, y \in A_0\} \cup \{(x, xy) \mid x \in D_1, y \in A_1\}.
\]

Then \( E_1 \) is a set of type \( Q \) in \( \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \).

This theorem obviously generalizes the construction of type \( Q \) sets given by Chen [4]. Indeed, we used \( D_i, i = 0, 1, \) instead of \( C_i^{(2,q^2)}, i = 0, 1, \) in the definition of \( X \) and \( X' \) (see Subsection 2.2). This new construction is much more flexible than that in [4].

To prove this theorem, we will evaluate the character values \( \psi_{a,b}(E_i), (a, b) \in (\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}) \setminus \{(0,0)\} \), by a series of the following lemmas. We first treat the case where \( b = 0 \).
Lemma 3.3. For \( b = 0 \) and \( a \neq 0 \), it holds that

\[
\psi_{a,b}(E_0) = \frac{q^2 - 1}{4}.
\]

Proof: Since \( |T_0| = |T_1| = (q - 1)/2 \), by Remark 3.1 (ii),(iii), we have \( |A_0| = |A_1| = (q^2 - 1)/4 \). Then, we have

\[
\psi_{a,0}(E_0) = \sum_{x \in D_0} \sum_{y \in A_0} \psi_{\overline{F}_{q^2}}(ax) + \sum_{x \in D_1} \sum_{y \in A_1} \psi_{\overline{F}_{q^2}}(ax) + \frac{q^2 - 1}{2} = \frac{q^2 - 1}{4} \sum_{x \in \overline{F}_{q^2}} \psi_{\overline{F}_{q^2}}(ax) + \frac{q^2 - 1}{2} = \frac{q^2 - 1}{4}.
\]

This completes the proof. \( \square \)

Lemma 3.4. For \( b = 0 \) and \( a \neq 0 \), we have

\[
\psi_{a,b}(E_1) = \begin{cases} 
\frac{q^2 - 1}{4}, & \text{if } a^{-1} \in D_\epsilon, \\
\frac{3q^2 - 1}{4}, & \text{otherwise}.
\end{cases}
\]

Proof: Since \( |T_0| = (q - 1)/2 \) and \( |T_1| = (q + 1)/2 \), by Remark 3.1 (ii),(iii), we have \( |A_0| = (q - 1)/4 \) and \( |A_1| = (q + 1)/4 \). Then, we have

\[
\psi_{a,0}(E_1) = \sum_{x \in D_0} \sum_{y \in A_0} \psi_{\overline{F}_{q^2}}(ax) + \sum_{x \in D_1} \sum_{y \in A_1} \psi_{\overline{F}_{q^2}}(ax) = \frac{(q - 1)^2}{4} \sum_{x \in \overline{F}_{q^2}} \psi_{\overline{F}_{q^2}}(ax) + q \sum_{x \in D_1} \psi_{\overline{F}_{q^2}}(ax).
\]

Finally, by Remark 3.1 (iv), (3.4) is reformulated as

\[
\psi_{a,0}(E_1) = -(q - 1)^2 + q \begin{cases} 
\frac{1+q}{2}, & \text{if } a^{-1} \in D_\epsilon, \\
\frac{q-1}{2}, & \text{otherwise}.
\end{cases}
\]

This completes the proof. \( \square \)

We next treat the case where \( b \neq 0 \). Let \( f_{S_i}, i = 0,1 \), be defined as in Remark 3.1 (i). Define

\[
U_1 = \sum_{x \in D_0} \sum_{y \in \overline{F}_{q^2}} \psi_{\overline{F}_{q^2}}(x(a + by))f_{S_0}(y),
\]

\[
U_2 = \sum_{x \in D_1} \sum_{y \in \overline{F}_{q^2}} \psi_{\overline{F}_{q^2}}(x(a + by))f_{S_1}(y),
\]

\[
U_3 = \sum_{x \in \overline{F}_{q^2}} \sum_{y \in \overline{F}_{q^2}} \psi_{\overline{F}_{q^2}}(x(a + by))f_{S_0}(y)f_{S_1}(y).
\]

Then, the character values of \( E_i, i = 0,1 \), are given by

\[
\psi_{a,b}(E_0) = U_1 + U_2 - U_3 + \sum_{x \in D_i} \psi_{\overline{F}_{q^2}}(bx)
\]

and

\[
\psi_{a,b}(E_1) = U_1 + U_2 - U_3.
\]

Lemma 3.5. If \( b \neq 0 \), it holds that

\[
U_1 = \begin{cases} 
-q|T_0| + q^2, & \text{if } -ab^{-1} \in S_0 \text{ and } b^{-1} \in D_0, \\
-q|T_0|, & \text{if } -ab^{-1} \notin S_0 \text{ and } b^{-1} \in D_0, \\
0, & \text{if } b^{-1} \in D_1.
\end{cases}
\]
Proof: If \( b \neq 0 \), we have
\[
U_1 = \frac{1}{q} \sum_{x \in D_0} \sum_{y \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q} \sum_{u \in T_0} \psi_{\mathbb{F}_q^*}(xa) \psi_{\mathbb{F}_q^*}((xb + c)y) \psi_{\mathbb{F}_q}(cu). \tag{3.7}
\]
If \( b^{-1} \in D_1 \), there are no \( x \in D_0 \) such that \( xb + c = 0 \); we have \( U_1 = 0 \). If \( b^{-1} \in D_0 \), continuing from (3.7), we have
\[
U_1 = q \sum_{c \in \mathbb{F}_q^*} \sum_{u \in T_0} \psi_{\mathbb{F}_q^*}(-acb^{-1}) \psi_{\mathbb{F}_q}(cu)
\]
\[
= -q|T_0| + q \sum_{c \in \mathbb{F}_q} \sum_{u \in T_0} \psi_{\mathbb{F}_q}(\text{Tr}_{\mathbb{F}_q^*/\mathbb{F}_q}(-ab^{-1})c - cu)
\]
\[
= -q|T_0| + q^2 \begin{cases} 
1, & \text{if } \text{Tr}_{\mathbb{F}_q^*/\mathbb{F}_q}(-ab^{-1}) \in T_0, \\
0, & \text{otherwise.}
\end{cases}
\]
This completes the proof. \( \square \)

Lemma 3.6. If \( b \neq 0 \), we have
\[
U_2 = \begin{cases} 
-q|T_1| + q^2, & \text{if } -ab^{-1} \in S_1 \text{ and } b^{-1} \in D_0, \\
-q|T_1|, & \text{if } -ab^{-1} \not\in S_1 \text{ and } b^{-1} \in D_0, \\
0, & \text{if } b^{-1} \in D_1.
\end{cases}
\]

Proof: If \( b \neq 0 \), we have
\[
U_2 = \frac{1}{q} \sum_{x \in D_1} \sum_{y \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q} \sum_{u \in T_1} \psi_{\mathbb{F}_q^*}(xa) \psi_{\mathbb{F}_q^*}((xb + c\omega^m)y) \psi_{\mathbb{F}_q}(cu). \tag{3.8}
\]
If \( b^{-1} \in D_1 \), there are no \( x \in D_1 \) such that \( xb + c\omega^m = 0 \); hence \( U_2 = 0 \). If \( b^{-1} \in D_0 \), continuing from (3.8), we have
\[
U_2 = q \sum_{c \in \mathbb{F}_q^*} \sum_{u \in T_1} \psi_{\mathbb{F}_q^*}(-acb^{-1}\omega^m) \psi_{\mathbb{F}_q}(cu)
\]
\[
= -q|T_1| + q \sum_{c \in \mathbb{F}_q} \sum_{u \in T_1} \psi_{\mathbb{F}_q}(\text{Tr}_{\mathbb{F}_q^*/\mathbb{F}_q}(-ab^{-1}\omega^m)c - cu)
\]
\[
= -q|T_1| + q^2 \begin{cases} 
1, & \text{if } \text{Tr}_{\mathbb{F}_q^*/\mathbb{F}_q}(-ab^{-1}\omega^m) \in T_1, \\
0, & \text{otherwise.}
\end{cases}
\]
This completes the proof. \( \square \)

Lemma 3.7. If \( b \neq 0 \), we have
\[
U_3 = \begin{cases} 
-|T_0||T_1| + q^2, & \text{if } -ab^{-1} \in S_0 \cap S_1, \\
-|T_0||T_1|, & \text{otherwise.}
\end{cases}
\]

Proof: Note that \( D_0 \cup D_1 = \mathbb{F}_q^* \) and \( |S_0 \cap S_1| = |T_0||T_1| \). Since \( b \neq 0 \), we have
\[
U_3 = \sum_{x \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_q^*} \psi_{\mathbb{F}_q^*}(x(a + by)) f_{S_0}(y) f_{S_1}(y) - |S_0 \cap S_1|
\]
\[
= q^2 f_{S_0}(-ab^{-1}) f_{S_1}(-ab^{-1}) - |T_0||T_1|.
\]
This completes the proof. \( \square \)
Proof of Theorem 3.2. In the case where $b = 0$, the statement follows from Lemmas 3.3 and 3.4. We now treat the case where $b \neq 0$. By the evaluations for $U_1, U_2, U_3$ in Lemmas 3.5-3.7 we have

$$U_1 + U_2 - U_3 = \begin{cases} 
-q(|T_0| + |T_1| - q) + |T_0||T_1|, & \text{if } b^{-1} \in D_0, -ab^{-1} \in S_0, -ab^{-1} \in S_1; \\
-q(|T_0| + |T_1|) + |T_0||T_1|, & \text{if } b^{-1} \in D_0, -ab^{-1} \notin S_0, -ab^{-1} \notin S_1; \\
-q^2 + |T_0||T_1|, & \text{if } b^{-1} \in D_1, -ab^{-1} \in S_0, -ab^{-1} \in S_1; \\
|T_0||T_1|, & \text{if } b^{-1} \in D_1, -ab^{-1} \notin S_0, -ab^{-1} \notin S_1. 
\end{cases}$$

(1) Since $|T_0| = |T_1| = (q - 1)/2$, by Remark 3.1 (iv), we have

$$\psi_{a,b}(E_0) = U_1 + U_2 - U_3 + \sum_{x \in D_0} \psi_{q^2}(bx)$$

$$= \begin{cases} 
-\frac{3q^2 - 1}{4}, & \text{if } b^{-1} \in D_0, -ab^{-1} \notin S_0, \text{ and } -ab^{-1} \notin S_1; \\
\frac{q^2 - 1}{4}, & \text{otherwise.}
\end{cases}$$

(2) Since $|T_0| = (q - 1)/2$ and $|T_1| = (q + 1)/2$, we have

$$\psi_{a,b}(E_1) = U_1 + U_2 - U_3$$

$$= \begin{cases} 
-\frac{3q^2 - 1}{4}, & \text{if } b^{-1} \in D_0, -ab^{-1} \notin S_0, \text{ and } -ab^{-1} \notin S_1; \\
\frac{q^2 - 1}{4}, & \text{otherwise.}
\end{cases}$$

This completes the proof of the theorem. \qed

Corollary 3.8. Let $T_i, i = 0, 1$, be arbitrary $(q - 1)/2$-subsets of $\mathbb{F}_q$ and $S_0, S_1, A_0, A_1$ be the sets defined as in (3.1) and (3.2). Furthermore, define

$$S'_0 = \{x \in \mathbb{F}_{q^2} | Tr_{q^2/q}(x \omega^m) \in \mathbb{F}_q \setminus T_1\}, \quad A'_0 = S_0 \setminus S'_0, \quad A'_1 = S'_1 \setminus S_0.$$

Then, the sets

$$C_0 = \{(x, y) | x \in D_0, y \in A_0\} \cup \{(x, y) | x \in D_1, y \in A_1\} \cup \{(0, x) | x \in D_1\},$$

$$C_1 = \{(x, y) | x \in D_0, y \in A'_0\} \cup \{(x, y) | x \in D_1, y \in A'_1\},$$

$$C_2 = \{(x, y) | x \in D_1, y \in A_0\} \cup \{(x, y) | x \in D_0, y \in A_1\} \cup \{(0, x) | x \in D_{e+1}\},$$

$$C_3 = \{(x, y) | x \in D_1, y \in A'_0\} \cup \{(x, y) | x \in D_0, y \in A'_1\}$$

are of type $Q$, where the subscript of $D_{e+1}$ is reduced modulo 2. Furthermore, these sets satisfy the assumptions of Remark 2.6 with respect to the spread consisting of the following 2-dimensional subspaces:

$$K_y = \{(x, y) | x \in \mathbb{F}_{q^2}, y \in \mathbb{F}_{q^2}\}, \quad \text{and} \quad K_\infty = \{(0, x) | x \in \mathbb{F}_{q^2}\}.$$

Proof: By Theorem 3.2, $C_0$ and $C_1$ are type Q sets. Furthermore, since $C_2 = \omega^m C_0$ and $C_3 = \omega^m C_1$, the sets $C_2$ and $C_3$ are also of type Q. Finally, $C_i, i = 0, 1, 2, 3$, satisfy the assumption of Remark 2.6 as $C_0 \cup C_2 \cup \{(0, 0)\} = (\bigcup_{y \in A_0 \cup A_1} K_y) \cup K_\infty$ and $C_1 \cup C_3 \cup \{(0, 0)\} = \bigcup_{y \in A'_0 \cup A'_1} K_y$. \qed
4. A generalization of Wilson-Xiang’s examples

4.1. The Setting. We fix notation used in this section. Let $q$ be a prime power and $\omega$ be a primitive element of $\mathbb{F}_{q^2}$. Let $c$ be any fixed odd integer in $\{0, 1, \ldots, 2q + 1\} = \mathbb{Z}_{2q+2}$.

Define the following subsets of $\{0, 1, \ldots, 2q + 1\}$:

$$I_1 = \{ i \pmod{2(q + 1)} | \text{Tr}_{q^2/q}(\omega^i) = 0 \} = \{ \frac{q+1}{2}, \frac{3(q+1)}{2} \},$$

$$I_2 = \{ i \pmod{2(q + 1)} | \text{Tr}_{q^2/q}(\omega^i) \in C_0^{(2,q)} \},$$

$$I_3 = \{ i \pmod{2(q + 1)} | \text{Tr}_{q^2/q}(\omega^i) \in C_1^{(2,q)} \},$$

$$J_i = I_i - c \pmod{2(q + 1)}, \ i = 1, 2, 3.$$

Then $|I_1| = 2$, $|I_2| = |I_3| = q$, and $I_1 \cup I_2 \cup I_3 = \mathbb{Z}_{2q+2}$. Furthermore, define

$$X_{1,c} = (I_1 \cap J_2) \cup (I_2 \cap J_1),$$
$$X_{2,c} = (I_1 \cap J_3) \cup (I_3 \cap J_1),$$
$$X_{3,c} = I_2 \cap J_2, X_{4,c} = I_3 \cap J_3,$$
$$X_{5,c} = (I_2 \cap J_3) \cup (I_3 \cap J_2).$$

It is clear that the $X_{i,c}$’s partition $\mathbb{Z}_{2q+2}$. In the appendix, we will show that the $X_{i,c}$’s have the following properties:

(P1) $X_{1,c} \equiv X_{2,c} + (q + 1) \pmod{2(q + 1)}$, $X_{3,c} \equiv X_{4,c} + (q + 1) \pmod{2(q + 1)}$;

(P2) $|X_{1,c}| = |X_{2,c}| = 2$, $|X_{3,c}| = |X_{4,c}| = \frac{q+1}{2}$, $|X_{5,c}| = q - 1$;

(P3) $X_{3,c+q+1} \cup X_{4,c+q+1} = X_{5,c}$;

(P4) $X_{1,c} + c \equiv -X_{1,c} + (q + 1) \pmod{2(q + 1)}$ or $X_{2,c} + c \equiv -X_{2,c} + (q + 1) \pmod{2(q + 1)}$ according as $q \equiv 3 \pmod{4}$ or $q \equiv 1 \pmod{4}$.

(P5) $|X_{1,c} \cap X_{1,c+q+1}| = 1$;

(P6) By the properties (P2) and (P5), we can assume that $X_{1,c} = \{\alpha, \beta\}$ and $X_{1,c+q+1} = \{\alpha, \gamma\}$. Then, $\beta \equiv \gamma + (q + 1) \pmod{2(q + 1)}$. Furthermore, $\alpha \equiv 0 \pmod{2}$ and $\beta \equiv 1 \pmod{2}$ or $\alpha \equiv 1 \pmod{2}$ and $\beta \equiv 0 \pmod{2}$ according as $q \equiv 3 \pmod{4}$ or $q \equiv 1 \pmod{4}$.

(P7) Define $R_i = \bigcup_{j \in X_{i,c}} C_j^{(2(q+1),q^2)}$, $i = 1, 2, 3, 4, 5$. Then, $R_i$ takes the character values listed in Table 1. In the language of association schemes, the Cayley graphs on $(\mathbb{F}_{q^2}, +)$ with connection sets $R_i$’s, together with the diagonal relation arising from the connection set $R_0 = \{0\}$, form a 5-class translation association scheme. Here, $Y_{i,c}$’s are subsets of $\{0, 1, \ldots, 2q + 1\}$ defined as the index sets of the dual association scheme.

(P8) $-Y_{i,c} + c \equiv Y_{i,c} \pmod{2(q + 1)}$, $i = 1, 2$;

(P9) $-Y_{3,c} \cup Y_{4,c} \equiv Y_{5,c} - c \pmod{2(q + 1)}$;

(P10) Define $R_i' = \bigcup_{j \in Y_{i,c}} C_j^{(2(q+1),q^2)}$, $i = 1, 2, 3, 4, 5$. Then, $R_i'$ takes the character values listed in Table 2.

| $a \in Y_{1,c}$ | $R_1$ | $R_2$ | $R_3$ | $R_4$ | $R_5$ |
|-----------------|--------|--------|--------|--------|--------|
| $-a \in Y_{2,c}$ | $-a - G_q(q)$ | $-a - G_q(q)$ | $(a - 1 - a G_q(q))$ | $(a - 1 - a G_q(q))$ | $-q+1$ |
| $a \in Y_{3,c}$ | $1 - G_q(q)$ | $1 - G_q(q)$ | $(1 - G_q(q))^2$ | $(1 - G_q(q))^2$ | $1 - (-1)^{\frac{q+1}{2}} q$ |
| $a \in Y_{4,c}$ | $1 - G_q(q)$ | $1 + G_q(q)$ | $(1 + G_q(q))^2$ | $(1 + G_q(q))^2$ | $1 - (-1)^{\frac{q+1}{2}} q$ |
| $a \in Y_{5,c}$ | $-1$ | $-1$ | $1 - (-1)^{\frac{q+1}{2}} q$ | $1 - (-1)^{\frac{q+1}{2}} q$ | $1 + (-1)^{\frac{q+1}{2}} q$ |

Table 1. The values of $\psi_{\mathbb{F}_{q^2}}(\omega^a R_i)$’s
4.2. The Construction. Let $X_{i,c}, Y_{i,c}, R_i, R'_i, i = 1, 2, \ldots, 5$, be sets defined as in Subsection [4.1] Let $A$ and $B$ be subsets of $\{0, 1, \ldots, 2q + 1\}$ satisfying $A \cap B = X_{3,c}$ and as multisets, $A \cup B = X_{1,c} \cup X_{3,c} \cup X_{3,c}$. It follows that $(A \backslash B) \cup (B \backslash A) = X_{1,c}$.

Let $\tau = 0$ or 1 according as $q \equiv 3$ or 1 (mod 4). Define

$$
D_0 = \{(0, y) \mid y \in C_2^{(2q^2)}\},
$$

$$
D_1 = \{(y, 0) \mid y \in C_0^{(2q^2)}\},
$$

$$
D_2 = \{(xy, xy^{-1}, \omega^i) \mid x \in \mathbb{F}_q^*, y \in C_0^{(2q^2)}, i \in A\},
$$

$$
D_3 = \{(xy, xy^{-1}, \omega^i) \mid x \in \mathbb{F}_q^*, y \in C_1^{(2q^2)}, i \in B\}. \quad (4.1)
$$

We denote the set of even (resp. odd) elements in any subset $S$ of $\{0, 1, \ldots, 2q + 1\}$ by $S_e$ (resp. $S_o$). The following is our main result in this section.

**Theorem 4.1.** (1) If $|A| = |B| = \frac{q+1}{2}$ and $|A_e| + |B_o| = |A_o| + |B_e| - 2(-1)^{\frac{2q}{2}}$, then $E_0 = D_0 \cup D_2 \cup D_3$ is a type $Q$ set in $\mathbb{F}_q^2 \times \mathbb{F}_q^2$.

(2) If $|A| = \frac{q+3}{2}, |B| = \frac{q-1}{2}$ and $|A_e| + |B_o| = |A_o| + |B_e|$, then $E_1 = D_1 \cup D_2 \cup D_3$ is a type $Q$ set in $\mathbb{F}_q^2 \times \mathbb{F}_q^2$.

This theorem generalizes the examples of type $Q$ sets found by Wilson-Xiang [12]. Indeed, these sets admit the automorphism $T'$. See Subsection 2.2.

To prove the theorem above, we will evaluate the character values of $E_i, i = 0, 1$. Define

$$
V_0 = \sum_{y \in C_2^{(2q^2)}} \psi_{\mathbb{F}_q^2}(by), \quad V_1 = \sum_{y \in C_0^{(2q^2)}} \psi_{\mathbb{F}_q^2}(ay),
$$

$$
V_2 = \frac{1}{2} \sum_{i \in A} \sum_{y \in C_2^{(2q^2)}} \sum_{x \in \mathbb{F}_q^*} \psi_{\mathbb{F}_q^2}(axy) \psi_{\mathbb{F}_q^2}(bxy^{-1}, \omega^i),
$$

$$
V_3 = \frac{1}{2} \sum_{i \in B} \sum_{y \in C_1^{(2q^2)}} \sum_{x \in \mathbb{F}_q^*} \psi_{\mathbb{F}_q^2}(axy) \psi_{\mathbb{F}_q^2}(bxy^{-1}, \omega^i).
$$

Noting that each element in $D_2$ (resp. $D_3$) appears exactly twice when $x$ runs through $\mathbb{F}_q^*$ and $y$ runs through $C_0^{(2q^2)}$ (resp. $C_1^{(2q^2)}$), we have $\psi_{a,b}(E_0) = V_0 + V_2 + V_3$ and $\psi_{a,b}(E_1) = V_1 + V_2 + V_3$.

We will evaluate these character sums by considering two cases: (i) exactly one of $a, b$ is zero; and (ii) $a \neq 0$ and $b \neq 0$. We first treat Case (i).

**Lemma 4.2.** If exactly one of $a, b$ is zero, then

$$
\psi_{a,b}(E_0) = \begin{cases} 
\frac{-q^2 - 1}{q^2 - 1}, & \text{if } a = 0 \text{ and } b \in C_1^{(2q^2)}, \\
\frac{3q^2 - 1}{q^2 - 1}, & \text{otherwise}.
\end{cases}
$$
Finally, by (2.2), the statement follows. □

Lemma 4.3. Since $\chi$ we have $\|\psi\|_{\mathbb{F}_{q^2}}(axy) = -\frac{q^2 - 1}{4}$. Hence, (4.3) is reformulated as
$$V_0 + V_2 + V_3 = q\psi_{\mathbb{F}_{q^2}}(bC_{\tau}^{(2,q^2)}) - \left(\frac{q - 1}{2}\right)^2.$$ Finally, by (2.2), the statement follows.

Lemma 4.4. If exactly one of $a, b$ is zero, then
$$\psi_{a,b}(E_1) = \begin{cases} \frac{-3q^2 - 1}{4}, & \text{if } b = 0 \text{ and } a \in C_{\tau+1}^{(2,q^2)}, \\ \frac{q^2 - 1}{4}, & \text{otherwise.} \end{cases}$$ Proof: If $a = 0$ and $b \neq 0$, it is clear that $V_1 = \frac{q^2 - 1}{2}$. Since $|A_e| + |B_o| = |A_o| + |B_e| = \frac{q^2 + 1}{2}$, we have
$$V_2 + V_3 = \frac{q - 1}{2}((|A_e| + |B_o|)\psi_{\mathbb{F}_{q^2}}(bC_0^{(2,q^2)}) + (|A_o| + |B_e|)\psi_{\mathbb{F}_{q^2}}(bC_1^{(2,q^2)})) = -\frac{q^2 - 1}{4}.$$ Hence, $\psi_{a,b}(E_1) = \frac{q^2 - 1}{4}$. If $a \neq 0$ and $b = 0$,
$$V_1 + V_2 + V_3 = \psi_{\mathbb{F}_{q^2}}(aC_0^{(2,q^2)}) + \frac{q - 1}{2}(|A|\psi_{\mathbb{F}_{q^2}}(aC_0^{(2,q^2)}) + |B|\psi_{\mathbb{F}_{q^2}}(aC_1^{(2,q^2)})).$$ Since $|A| = \frac{q^2 + 3}{2}$ and $|B| = \frac{q - 1}{2}$, (4.3) is reformulated as
$$V_1 + V_2 + V_3 = q\psi_{\mathbb{F}_{q^2}}(aC_0^{(2,q^2)}) - \left(\frac{q - 1}{2}\right)^2.$$ Finally, by (2.2), the statement follows.

We next consider Case (ii), i.e., $a \neq 0$ and $b \neq 0$.

Lemma 4.4. If $a \neq 0$ and $b \neq 0$, then
$$V_2 + V_3 = \frac{1}{4(q + 1)} \sum_{u=0,1}^{2q+1} \sum_{h=0}^{2q+1} G_q^2(\chi_{2(q+1)}^{-1} \rho^u)G_q^2(\chi_{2(q+1)}^{-1})\chi_{2(q+1)}^{ab}(\omega)\rho^u(a) \times \left(\sum_{i \in A} X_i^h(\omega^i) + \sum_{i \in B} X_i^h(\omega^i)\rho^u(\omega)\right).$$ where $\chi_{2(q+1)}$ is a multiplicative character of order $2(q+1)$ of $\mathbb{F}_{q^2}$ and $\rho$ is the quadratic character of $\mathbb{F}_{q^2}$.
Proof: Let \( \chi \) be a multiplicative character of order \( q^2 - 1 \) of \( \mathbb{F}_{q^2} \). By (2.1), we have

\[
V_2 = \frac{1}{2(q^2 - 1)^2} \sum_{i \in A} \sum_{j \in C(2,q^2)} \sum_{x \in \mathbb{F}_q^*} \sum_{j,k=0}^{q^2-2} G_{q^2}(\chi^{-j}) \chi^j(axy) G_{q^2}(\chi^{-k}) \chi^k(bxy^{-1}\omega^i)
\]

\[
= \frac{1}{2(q^2 - 1)^2} \sum_{i \in A} \sum_{j,k=0}^{q^2-2} G_{q^2}(\chi^{-j}) G_{q^2}(\chi^{-k}) \chi^j(a\chi^k(b\omega^i)) \chi^{j-k}(C_0^{(2,q^2)}) \sum_{x \in \mathbb{F}_q^*} \chi^{j+k}(x). \tag{4.5}
\]

Since \( \chi^{j-k}(C_0^{(2,q^2)}) = \frac{q^2-1}{2} \) or 0 according as \( j - k \equiv 0 \pmod{\frac{q^2-1}{2}} \) or not, continuing from (4.5), we have

\[
V_2 = \frac{1}{4(q^2 - 1)} \sum_{i \in A} \sum_{u=0,1}^{q^2-2} G_{q^2}(\chi^{-u}) G_{q^2}(\chi^{-k}) \chi^k(b\omega^i) \chi^{k+\frac{q^2-1}{2}u}(x) \sum_{x \in \mathbb{F}_q^*} \chi^{k+\frac{q^2-1}{2}u}(x). \tag{4.6}
\]

Let \( \chi_2(q+1) = \chi_{\frac{q+1}{2}} \) and \( \rho = \chi_{\frac{q+1}{4}} \). Since \( \sum_{x \in \mathbb{F}_q^*} \chi^{2k+\frac{q^2-1}{2}u}(x) = q - 1 \) or 0 according as \( 2k \equiv 0 \pmod{q - 1} \) or not, continuing from (4.6), we have

\[
V_2 = \frac{1}{4(q + 1)} \sum_{u=0,1}^{2q+1} G_{q^2}(\chi_2^{-u}) G_{q^2}(\chi_2^{-}(ab)) \chi^{h}(\omega^i) \sum_{i \in A} \chi^{h}(\omega^i).\]

Similarly, we have

\[
V_3 = \frac{1}{4(q + 1)} \sum_{u=0,1}^{2q+1} G_{q^2}(\chi_2^{-u}) G_{q^2}(\chi_2^{-}(ab)) \chi^{h}(\omega^i) \sum_{i \in B} \chi^{h}(\omega^i)\rho^u(\omega).
\]

This completes the proof of the lemma. \( \square \)

Let \( W_0 \) (resp. \( W_1 \)) be the contribution for \( u = 0 \) (resp. \( u = 1 \)) in the summations of (4.4); then \( V_2 + V_3 = W_0 + W_1 \).

Lemma 4.5. Let \( r = ab \neq 0 \). Then,

\[
W_0 = \begin{cases} \frac{-q^2+1}{4}, & \text{if } r \in \omega^c R_1 \text{ or } r \in \omega^c R_2, \\ \frac{q^2+1}{4}, & \text{if } r \in \omega^c R_2, \\ -\frac{3q^2+1}{4}, & \text{otherwise,} \end{cases}
\]

depending on whether \( q \equiv 3 \) or 1 (mod 4).

Proof: By the definition of \( W_0 \), we have

\[
W_0 = \frac{1}{4(q + 1)} \sum_{h=0}^{2q+1} G_{q^2}(\chi_2^{-h}) \chi_2^{h}(ab) \chi_2^{h}(\omega^i) \sum_{i \in A \cup B} \chi_2^{h}(\omega^i).
\]

Since \( A \cup B = X_{1,c} \cup X_{3,c} \cup X_{4,c} \) as a multiset, by the property (P7), we have

\[
\psi_{\mathbb{F}_{q^2}}(\omega^a \bigcup_{i \in A \cup B} C_i^{(2q+1),q^2}) = \begin{cases} \frac{qG_a(q)-1}{2}(=: c_1), & \text{if } a \in Y_{1,c}(=: Z_1), \\ -\frac{qG_a(q)-1}{2}(=: c_2), & \text{if } a \in Y_{2,c}(=: Z_2), \\ -1+\frac{a}{2}(=: c_3), & \text{if } a \in Y_{3,c} \cup Y_{4,c}(=: Z_3), \\ -\frac{1}{2}(=: c_4), & \text{if } a \in Y_{5,c}(=: Z_4). \end{cases}
\]
Then, by (2.3), we have
\[
G_q^{2h}(\chi_{2(q+1)}^h) \sum_{i \in A \cup B} \chi_{2(q+1)}^h(\omega^i) = \sum_{a=0}^{2q+1} \psi_{q^2}(\omega^a \bigcup_{i \in A \cup B} C_i^{(2(q+1),q^2)}) \chi_{2(q+1)}^{-h}(\omega^a)
\]

Then, by (2.1), we have
\[
W_0 = \sum_{i=1}^{4} c_i \sum_{a \in Z_i} \chi_{2(q+1)}^{-h}(\omega^a).
\]

Since $-Y_{i,c} \equiv Y_{i,c} - c \pmod{2(q+1)}$, $i = 1, 2$, from the property (P8), we have by the property (P10) that for $i = 1, 2$
\[
\sum_{a \in -Z_i} \psi_{q^2}(rC_a^{(2(q+1),q^2)}) = \begin{cases} \\
\frac{-2q+2(-1)^{-1}G_q(\eta)}{4(q+1)}, & \text{if } r \in \omega^c R_1, \\
\frac{-2q+2(-1)^{-1}G_q(\eta)}{4(q+1)}, & \text{if } r \in \omega^c R_2, \\
1 + (-1)^{-1}G_q(\eta), & \text{if } r \in \omega^c R_3, \\
1 - (-1)^{-1}G_q(\eta), & \text{if } r \in \omega^c R_4, \\
1, & \text{if } r \in \omega^c R_5.
\end{cases}
\]

Furthermore, since $-(Y_{3,c} \cup Y_{4,c}) \equiv Y_{5,c} - c \pmod{2(q+1)}$ by the property (P9), we have
\[
\sum_{a \in -Z_3} \psi_{q^2}(rC_a^{(2(q+1),q^2)}) = \sum_{a \in Y_{3,c} - c} \psi_{q^2}(rC_a^{(2(q+1),q^2)}) = \begin{cases} \\
\frac{1-q}{2}, & \text{if } r \in \omega^c (R_1 \cup R_2), \\
\frac{1+(-1)^{-1}q}{2}, & \text{if } r \in \omega^c R_3, \\
\frac{1-(-1)^{-1}q}{2}, & \text{if } r \in \omega^c (R_3 \cup R_4).
\end{cases}
\]

Similarly, we have
\[
\sum_{a \in -Z_4} \psi_{q^2}(rC_a^{(2(q+1),q^2)}) = \sum_{a \in (Y_3 \cup Y_4) - c} \psi_{q^2}(rC_a^{(2(q+1),q^2)}) = \begin{cases} \\
\frac{-q+1}{2}, & \text{if } r \in \omega^c (R_1 \cup R_2), \\
\frac{1-(-1)^{-1}q}{2}, & \text{if } r \in \omega^c R_3, \\
\frac{1+(-1)^{-1}q}{2}, & \text{if } r \in \omega^c (R_3 \cup R_4).
\end{cases}
\]

Summing up, we have
\[
W_0 = \begin{cases} \\
\frac{-q^2+1}{4}, & \text{if } r \in \omega^c R_1 \text{ or } r \in \omega^c R_2, \\
\frac{-q^2+1}{4}, & \text{if } r \in \omega^c (R_2 \cup R_4 \cup R_5) \text{ or } r \in \omega^c (R_1 \cup R_3 \cup R_5), \\
\frac{-3q^2+1}{4}, & \text{if } r \in \omega^c R_3 \text{ or } r \in \omega^c R_4,
\end{cases}
\]

according as $q \equiv 3$ or $1 \pmod{4}$. This completes the proof. \[\square\]

We next evaluate $W_1$ below.
Lemma 4.6. Let $r = ab \neq 0$. Then,

$$W_1 = -\frac{(-1)^{\frac{q+1}{2}}\rho(a)q}{4} \left( |A| - |B| + \rho(r)(|A_e| + |B_o| - |A_o| - |B_e|) \right)$$

$$+ \frac{(-1)^{\frac{q+1}{2}}\rho(a)q^2}{2} \cdot \left\{ \begin{array}{ll}
1, & \text{if } r \in \bigcup_{i=-(A\setminus B) \cup q+1} C_i^{(2(q+1),q^2)}, \\
-1, & \text{if } r \in \bigcup_{i=-(B\setminus A) \cup q+1} C_i^{(2(q+1),q^2)}, \\
0, & \text{otherwise.}
\end{array} \right.$$  

Proof: By the definition of $W_1$, we have

$$W_1 = \frac{\rho(a)}{4(q+1)} \sum_{h=0}^{2q+1} G_q^2(\chi_{2(q+1)}^{-h})G_q^2(\chi_{2(2q+1)}^{-h})(r) \left( \sum_{i \in A} \chi_{2(q+1)}^h(\omega^i) - \sum_{i \in B} \chi_{2(q+1)}^h(\omega^i) \right).$$

By applying the Davenport-Hasse product formula (Theorem 2.3) with $\chi = \chi_{2(q+1)}^{-h}$, $\chi' = \rho$, and $\ell = 2$ we have

$$G_q^2(\chi_{2(q+1)}^{-h})G_q^2(\chi_{2(2q+1)}^{-h}) = G_q^2(\rho)G_q^2(\chi_{q+1}^{-h}),$$

where $\chi_{q+1} = \chi_{2(q+1)}$ has order $q + 1$. Then, (4.7) is rewritten as

$$W_1 = \frac{\rho(a)}{4(q+1)} G_q^2(\rho) \sum_{h=0}^{2q+1} G_q^2(\chi_{q+1}^{-h})\chi_{2(q+1)}^h(r) \left( \sum_{i \in A} \chi_{2(q+1)}^h(\omega^i) - \sum_{i \in B} \chi_{2(q+1)}^h(\omega^i) \right).$$

(4.8)

We will compute $W_1$ by dividing it into three parts. Let $W_{1,1}, W_{1,2}, W_{1,3}$ denote the contributions in the sum on the right hand side of (4.8) when $h = 0$, $q+1$; other even $h$; and odd $h$, respectively. Then $W_1 = W_{1,1} + W_{1,2} + W_{1,3}$. For $W_{1,1}$, we have

$$W_{1,1} = -\frac{\rho(a)}{4(q+1)} G_q^2(\rho) \left( |A| - |B| + \rho(r)(|A_e| + |B_o| - |A_o| - |B_e|) \right).$$

Next, by Theorem 2.2 we have

$$W_{1,2} = \frac{\rho(a)q}{4(q+1)} G_q^2(\rho) \sum_{\ell=0; \ell \neq 0, \frac{q+1}{2}}^q \chi_{q+1}^\ell(r) \left( \sum_{i \in A} \chi_{q+1}^\ell(\omega^i) - \sum_{i \in B} \chi_{q+1}^\ell(\omega^i) \right).$$

(4.9)

By the property (P2),

$$\{x \mod (q+1) \mid x \in A \setminus B\} \cap \{x \mod (q+1) \mid x \in B \setminus A\} = \emptyset.$$  

Hence, continuing from (4.9), we have

$$W_{1,2} = -\frac{\rho(a)q}{4(q+1)} G_q^2(\rho) \left( |A| - |B| + \rho(r)(|A_e| + |B_o| - |A_o| - |B_e|) \right)$$

$$+ \frac{\rho(a)q}{4} G_q^2(\rho) \cdot \left\{ \begin{array}{ll}
1, & \text{if } r \in \bigcup_{i=-(A\setminus B) \cup q+1} C_i^{(q+1,q^2)}, \\
-1, & \text{if } r \in \bigcup_{i=-(B\setminus A) \cup q+1} C_i^{(q+1,q^2)}, \\
0, & \text{otherwise.}
\end{array} \right.$$
Finally, by Theorem 2.2 again, we have
\[
W_{1,3} = - \frac{\rho(a)q}{4(q + 1)} G^2_q(\rho) \sum_{h: \text{odd}} \chi_{2(q+1)}^h(r) \left( \sum_{i \in A} \chi_{2(q+1)}^h(\omega^i) - \sum_{i \in B} \chi_{2(q+1)}^h(\omega^i) \right)
\]
\[
= - \frac{\rho(a)q}{4(q + 1)} G^2_q(\rho) \sum_{h=0}^{2q+1} \chi_{2(q+1)}^h(r) \left( \sum_{i \in A} \chi_{2(q+1)}^h(\omega^i) - \sum_{i \in B} \chi_{2(q+1)}^h(\omega^i) \right)
\]
\[
+ \frac{\rho(a)q}{4(q + 1)} G^2_q(\rho) \sum_{\ell=0}^{q} \chi_{4+1}^\ell(r) \left( \sum_{i \in A} \chi_{4+1}^\ell(\omega^i) - \sum_{i \in B} \chi_{4+1}^\ell(\omega^i) \right)
\]
\[
= - \frac{\rho(a)q}{2} G^2_q(\rho) \cdot \left\{ \begin{array}{ll}
1, & \text{if } r \in \bigcup_{i \in -(A \setminus B)} C_i^{2(q+1)q^2} \\
1, & \text{if } r \in \bigcup_{i \in -(A \setminus B)} C_i^{2(q+1)q^2} \\
0, & \text{otherwise},
\end{array} \right.
\]
\[
+ \frac{\rho(a)q}{4} G^2_q(\rho) \cdot \left\{ \begin{array}{ll}
1, & \text{if } r \in \bigcup_{i \in -(A \setminus B)} C_i^{2(q+1)q^2} \\
1, & \text{if } r \in \bigcup_{i \in -(A \setminus B)} C_i^{2(q+1)q^2} \\
0, & \text{otherwise}.
\end{array} \right.
\]

Summing up, we have
\[
W_1 = W_{1,2} + W_{1,2} + W_{1,3}
\]
\[
= - \frac{\rho(a)}{4} G^2_q(\rho) \left( |A| - |B| + \rho(r)(|A_e| + |B_o| - |A_o| - |B_e|) \right)
\]
\[
+ \frac{\rho(a)q}{2} G^2_q(\rho) \cdot \left\{ \begin{array}{ll}
1, & \text{if } r \in \bigcup_{i \in -(A \setminus B)} C_i^{2(q+1)q^2} \\
0, & \text{otherwise},
\end{array} \right.
\]
\[
+ \frac{\rho(a)q^2}{4} \cdot \left\{ \begin{array}{ll}
-\frac{q^2+1}{4}, & \text{or } \frac{q^2+1}{4}, \text{if } r \in \omega^cR_1 \text{ or } r \in \omega^cR_2, \\
0, & \text{otherwise},
\end{array} \right.
\]
\[
\text{according as } q \equiv 3, 1 \pmod{4}. \text{ By the property (P4), } X_{1,c} + c \equiv -((A \setminus B) \cup (B \setminus A)) + (q + 1) \pmod{2(q+1)} \text{ or } X_{2,c} + c \equiv -((A \setminus B) \cup (B \setminus A)) + (q + 1) \pmod{2(q+1)} \text{ depending on whether } q \equiv 3, 1 \pmod{4}. \text{ Hence, continuing from } (4.10), \text{ we have}
\]
\[
V_2 + V_3 = \frac{q^2 + 1}{4} \text{ or } -\frac{3q^2 + 1}{4}.
\]

We are now ready to prove our main theorem.
Proof of Theorem 4.11: In the case where exactly one of \(a, b\) is zero, the statement follows from Lemmas 4.2 and 4.3. We treat the case where \(a \neq 0\) and \(b \neq 0\).

(1) By (2.2), \(V_0 = \frac{-\text{I} + \rho(b)}{2}\). Furthermore, by \(|A| = |B| = \frac{q^2 + 3}{2}\) and \(|A_x| + |B_o| = |A_o| + |B_o| - 2(-1)^{\frac{q-1}{2}}\), we have

\[
\frac{(-1)^{\frac{q-1}{2}}\rho(a)q}{4} \left( |A| - |B| + \rho(r)(|A_x| + |B_o| - |A_o| - |B_o|) \right) = -\frac{\rho(b)q}{2}.
\]

Hence, by (4.11), it follows that \(\psi_{a,b}(E_0) = \frac{q^2 - 1}{4}\) or \(-\frac{3q^2 - 1}{4}\).

(2) By (2.2), \(V_1 = \frac{-(-1)^{\frac{q+3}{2}}\rho(a)q}{4}\). Furthermore, by \(|A| = \frac{q^2 + 3}{2}, |B| = \frac{q^2 - 1}{2}\), and \(|A_x| + |B_o| = |A_o| + |B_e|\), we have

\[
\frac{(-1)^{\frac{q-1}{2}}\rho(a)q}{4} \left( |A| - |B| + \rho(r)(|A_x| + |B_o| - |A_o| - |B_o|) \right) = \frac{(-1)^{\frac{q-1}{2}}\rho(a)q}{2}.
\]

Hence, by (4.11), it follows that \(\psi_{a,b}(E_1) = \frac{q^2 - 1}{4}\) or \(-\frac{3q^2 - 1}{4}\). □

Corollary 4.8. Let \(A = \{\beta\} \cup X_{3,c}, B = \{\alpha\} \cup X_{3,c}, A' = X_{1,c+q+1} \cup X_{3,c+q+1}, \) and \(B' = X_{3,c+q+1}\), where \(\alpha, \beta\) are defined as in the property (P6). Then, the sets

\[
C_0 = \{(0, y) \mid y \in C_{t}(2, q^2) \} \cup \{(xy, xy^{-1} \omega^i) \mid x \in \mathbb{F}_q^*, y \in C_{0}(2, q^2), i \in A\}
\]

∪ \{(xy, xy^{-1} \omega^i) \mid x \in \mathbb{F}_q^*, i \in B\},

\[
C_1 = \{(y, 0) \mid y \in C_{t}(2, q^2) \} \cup \{(xy, xy^{-1} \omega^i) \mid x \in \mathbb{F}_q^*, y \in C_{0}(2, q^2), i \in A'\}
\]

∪ \{(xy, xy^{-1} \omega^i) \mid x \in \mathbb{F}_q^*, i \in B'\},

\[
C_2 = \{(0, y) \mid y \in C_{t+1}(2, q^2) \} \cup \{(xy, xy^{-1} \omega^i+y^2) \mid x \in \mathbb{F}_q^*, y \in C_{0}(2, q^2), i \in A\}
\]

∪ \{(xy, xy^{-1} \omega^i+y^2) \mid x \in \mathbb{F}_q^*, i \in B\},

\[
C_3 = \{(y, 0) \mid y \in C_{t}(2, q^2) \} \cup \{(xy, xy^{-1} \omega^i+y^2) \mid x \in \mathbb{F}_q^*, y \in C_{0}(2, q^2), i \in A'\}
\]

∪ \{(xy, xy^{-1} \omega^i+y^2) \mid x \in \mathbb{F}_q^*, i \in B'\}

are of type \(Q\). Furthermore, these sets satisfy the assumptions of Remark 2.6 with respect to the spread \(K\) consisting of the following 2-dimensional subspaces:

\[
K_y = \{(x, y x^q) \mid x \in \mathbb{F}_q^2, y \in \mathbb{F}_q^2, \text{ and } K_{\infty} = \{(0, x) \mid x \in \mathbb{F}_q^2\}.
\]

Proof: By the property (P6), \(|A_x| + |B_o| = |A_o| + |B_e| - 2(-1)^{\frac{q-1}{2}}\) and \(|A'_x| + |B'_o| = |A'_o| + |B'_e|\). Hence, by Theorem 4.11, \(C_0\) and \(C_1\) are type \(Q\) sets. Since \(C_2 = \{\omega x, \omega^q y \mid (x, y) \in C_0\} \) and \(C_3 = \{\omega x, \omega^q y \mid (x, y) \in C_1\}\), the sets \(C_2\) and \(C_3\) are also of type \(Q\). Furthermore, \(\bigcup_{i=1}^3 C_i = (\mathbb{F}_q^2 \times \mathbb{F}_q^2) \setminus \{(0, 0)\}\) since \(A \cup A' \cup (B + q + 1) \cup (B' + q + 1) \equiv \{0, 1, \ldots, 2q + 1\} (\text{mod } 2(q + 1))\) by the properties (P1), (P4), (P5) and (P6). Therefore, \(C_i, i = 0, 1, 2, 3\), satisfy the assumptions of Remark 2.6 as \(C_0 \cup C_2 \cup \{(0, 0)\} = (\bigcup_{y \in H_0} K_y) \cup K_{\infty}\) and \(C_1 \cup C_3 \cup \{(0, 0)\} = \bigcup_{y \in H_1} K_y\), where \(H_0 = \bigcup_{i \in -(A \cup (B + q + 1))} C_i(2(q^1)q^2)\) and \(H_1 = \bigcup_{i \in -(A' \cup (B' + q + 1))} C_i(2(q^1)q^2)\). □

Appendix

In this appendix, we prove that the sets \(X_{i,c}\) and \(Y_{i,c}, i = 1, 2, 3, 4, 5\), have the properties (P1)–(P10).

By the definition of \(X_{1,c}\), we have

\[
X_{1,c} = \left\{ \left\{ \frac{q+1}{2}, \frac{3q+11}{2} \right\} \cap \left\{ i \pmod{2(q+1)} \mid \text{Tr}_{q^2/q}(\omega^{i+c}) \in C_{0}(2, q) \right\} \right\}
\]

∪ \{\left\{ \frac{q+1}{2} - c, \frac{3q+11}{2} - c \right\} \cap \left\{ i \pmod{2(q+1)} \mid \text{Tr}_{q^2/q}(\omega^{i}) \in C_{0}(2, q) \right\} \} \}.


Hence, there are \( \epsilon, \delta \in \{-1, 1\} \) such that \( X_{1,c} = \{q+1/2 \epsilon, q+1/2 \delta - c\} \). In particular, we have

\[
\Tr_{q^2/q}(\omega^{q+1}e) \in C_0^{(2,q)} \quad \text{and} \quad \Tr_{q^2/q}(\omega^{q+1}d - c) \in C_0^{(2,q)}.
\]

**Lemma 4.9.** We have \( X_{1,c} = \{q+1/2 \epsilon, q+1/2 \delta - c\} \) for some \( (\epsilon, \delta) \in \{(1, 1), (-1, -1)\} \) or \(\{(1, 1), (1, -1)\} \) according as \( q \equiv 3 \) (mod 4) or \( q \equiv 1 \) (mod 4).

**Proof:** By (4.12), we have

\[
q+1/2 \epsilon \in C_0^{(2,q)} \quad \text{and} \quad q+1/2 \delta - c \in C_0^{(2,q)}.
\]

Putting \( \omega \equiv 1 - \omega^{q-1} \), the conditions in (4.13) are rewritten as

\[
\omega^{q+1/2 \epsilon} = \omega^{2(q+1)k} \quad \text{and} \quad \omega^{q+1/2 \delta - c} = \omega^{2(q+1)l}
\]

for some \( k, \ell \in \mathbb{Z} \). Here, \( d \) is odd if \( q \equiv 3 \) (mod 4), and \( d \) is even if \( q \equiv 1 \) (mod 4). By multiplying these equations, we have \( \omega^{q+1/2 (\epsilon + \delta) + d(q+1)} = \omega^{2(q+1)(k+\ell)} \). Then, the statement immediately follows.

\[\square\]

**Remark 4.10.** For \( X_{i,c}, i = 1, 2, 3, 4, 5 \), we observe the following facts:

1. Since \( I_2 \equiv I_3 + (q + 1) \) (mod 2(q+1)), we have \( X_{1,c} \equiv X_{2,c} + (q + 1) \) (mod 2(q+1)), \( X_{3,c} \equiv X_{4,c} + (q + 1) \) (mod 2(q+1)), and \( X_{5,c} \equiv X_{5,c} + (q + 1) \) (mod 2(q+1)). Hence, the property (P1) follows.
2. Since \( I_2 \) forms a \( (q + 1, 2, q, q+1/2) \) relative difference set (cf. [1]), we have \( |X_{3,c}| = \frac{q-1}{2} \). Then, the property (P2) follows.
3. Since \( X_{3,c+q+1} = I_2 \cap J_3 \) and \( X_{4,c+q+1} = I_3 \cap J_2 \), we have \( X_{3,c+q+1} \cup X_{4,c+q+1} = X_{5,c} \). Then, the property (P3) follows.
4. The property (P4) directly follows from Lemma 4.5.
5. By Lemma 4.9, \( X_{1,c+q+1} = \{q+1/2 \epsilon, q+1/2 \delta - c + q + 1\} \) for some \( (\epsilon, \delta) \in \{(1, 1), (-1, -1)\} \) or \(\{(1, 1), (1, -1)\} \) according to whether \( q \equiv 3 \) (mod 4) or \( q \equiv 1 \) (mod 4). Then, it is direct to see that \( X_{1,c} \cap X_{1,c+q+1} = 1 \) and \( X_{1,c} \setminus X_{1,c+q+1} \equiv (X_{1,c+q+1} \setminus X_{1,c}) + q + 1 \) (mod 2(q+1)) in all cases. More precisely, \( X_{1,c+q+1} = \{q+1/2 \epsilon + q + 1, q+1/2 \delta - c\} \) since \( q+1/2 \delta - c \in J_1 \cap I_2 \). Hence, \( X_{1,c} \setminus X_{1,c+q+1} = \{q+1/2 \epsilon\} \) and \( X_{1,c} \cap X_{1,c+q+1} = \{q+1/2 \delta - c\} \). Thus, the properties (P5) and (P6) follow.

Next, we show that the \( X_{i,c} \)'s have property (P7).

**Proposition 4.11.** Let \( R_i, i = 1, 2, 3, 4, 5 \), be defined as in Subsection 4.1. Then, \( R_i, i = 1, 2, 3, 4, 5 \), take the character values listed in Table 1. In particular, \( Y_{i,c} \)'s in Table 1 are determined as follows:

\[
Y_{1,c} = \{0, c\}, \quad Y_{2,c} = \{q + 1, c + q + 1\},
\]

\[
Y_{3,c} = \{i + c - \frac{q+1}{2} \delta \mid \Tr_{q^2/q}(\omega^i) \in C_0^{(2,q)}\} \cap \{i - \frac{q+1}{2} \epsilon \mid \Tr_{q^2/q}(\omega^i) \in C_0^{(2,q)}\},
\]

\[
Y_{4,c} = \{i + c - \frac{q+1}{2} \delta \mid \Tr_{q^2/q}(\omega^i) \in C_1^{(2,q)}\} \cap \{i - \frac{q+1}{2} \epsilon \mid \Tr_{q^2/q}(\omega^i) \in C_1^{(2,q)}\},
\]

\[
Y_{5,c} = \{i + c - \frac{q+1}{2} \delta \mid \Tr_{q^2/q}(\omega^i) \in C_0^{(2,q)}\} \cap \{i - \frac{q+1}{2} \epsilon \mid \Tr_{q^2/q}(\omega^i) \in C_0^{(2,q)}\}
\]

\[
\cup \{i + c - \frac{q+1}{2} \delta \mid \Tr_{q^2/q}(\omega^i) \in C_1^{(2,q)}\} \cap \{i - \frac{q+1}{2} \epsilon \mid \Tr_{q^2/q}(\omega^i) \in C_1^{(2,q)}\}.
\]
Proof: The character values \( \psi_{q^2}(\omega^a R_1) \), \( \omega = 0, 1, \ldots, 2q + 1 \), are evaluated as follows:

\[
\psi_{q^2}(\omega^a R_1) = \psi_{q^2}(\omega^a C_0^{(2q+1,q^2)}) + \psi_{q^2}(\omega^a C_0^{(2q+1,q^2)})
\]

\[
= \psi_{q^2}(\text{Tr}_{q^2/q}(\omega^{a+\frac{2q+1}{2}} - \frac{1}{2}G_{\eta}(q))) + \psi_{q^2}(\text{Tr}_{q^2/q}(\omega^{a+\frac{2q+1}{2}} - \frac{1}{2}G_{\eta}(q)))
\]

\[
= \left\{ \begin{array}{ll}
\frac{q-1}{2}, & \text{if } a \in I_1 - \frac{q+1}{2}\delta + c,
\frac{-1-G_{\eta}(q)}{2}, & \text{if } a \in I_2 - \frac{q+1}{2}\delta + c,
\frac{q-1}{2}, & \text{if } a \in I_3 - \frac{q+1}{2}\delta + c,
\frac{-1+G_{\eta}(q)}{2}, & \text{if } a \in I_4 - \frac{q+1}{2}\epsilon,
\frac{-1-G_{\eta}(q)}{2}, & \text{if } a \in I_5 - \frac{q+1}{2}\epsilon,
\end{array} \right.
\]

where

\[
Y_{1,c}' = ((I_1 - \frac{q+1}{2}\delta + c) \cap (I_2 - \frac{q+1}{2}\epsilon)) \cup ((I_2 - \frac{q+1}{2}\delta + c) \cap (I_1 - \frac{q+1}{2}\epsilon)),
\]

\[
Y_{2,c}' = ((I_1 - \frac{q+1}{2}\delta + c) \cap (I_3 - \frac{q+1}{2}\epsilon)) \cup ((I_3 - \frac{q+1}{2}\delta + c) \cap (I_1 - \frac{q+1}{2}\epsilon)).
\]

By (4.12), it is direct to see that

\[
(I_1 - \frac{q+1}{2}\delta + c) \cap (I_2 - \frac{q+1}{2}\epsilon) = \{c\}, \quad (I_2 - \frac{q+1}{2}\delta + c) \cap (I_1 - \frac{q+1}{2}\epsilon) = \{0\},
\]

\[
(I_1 - \frac{q+1}{2}\delta + c) \cap (I_3 - \frac{q+1}{2}\epsilon) = \{c + q + 1\}, \quad (I_3 - \frac{q+1}{2}\delta + c) \cap (I_1 - \frac{q+1}{2}\epsilon) = \{q + 1\}.
\]

Hence, we have \( Y_{1,c}' = Y_{1,c} \) and \( Y_{2,c}' = Y_{2,c} \).

The character values of \( R_2 \) is determined as \( \psi_{q^2}(\omega^a R_2) = \psi_{q^2}(\omega^a R_1) \).

We next evaluate \( \psi_{q^2}(\omega^a R_3) \), \( \omega = 0, 1, \ldots, 2q + 1 \). By Remark 3.7(i), the indicator function of \( \{x \mid \text{Tr}_{q^2/q}(x) \in C_0^{(2q)}\} \) is given by

\[
f(x) = \frac{1}{q} \sum_{s \in F_q} \sum_{y \in C_0^{(2,q)}} \psi_{q^2}(sx) \psi_q(-sy).
\]

Then,

\[
\psi_{q^2}(\omega^a R_3) = \sum_{x \in F_q} \psi_{q^2}(\omega^a x) f(x) f(x \omega^c)
\]

\[
= \frac{1}{q^2} \sum_{x \in F_q} \sum_{s,t \in F_q} \sum_{y,z \in C_0^{(2,q)}} \psi_{q^2}(x(\omega^a + s + t\omega^c)) \psi_q(-sy) \psi_q(-tz)
\]

\[
= \sum_{s,t \in F_q, \omega^a + s + t\omega^c} \psi_q(sy) \psi_q(tz).
\]

We treat the case where \( a \in Y_{1,c} \cup Y_{2,c} = \{0, c, q + 1, c + q + 1\} \). If \( a = c \), then \( s = 0 \) and \( t \in C_0^{(2,q)} \), and hence \( \psi_{q^2}(\omega^a R_3) = \frac{(q-1)(1+G_{\eta}(q))}{4} \). If \( a = c + q + 1 \), then \( s = 0 \) and \( t \in C_1^{(2,q)} \), and hence \( \psi_{q^2}(\omega^a R_3) = \frac{(q-1)(1+G_{\eta}(q))}{4} \). If \( a = 0 \), then \( t = 0 \) and \( s \in C_0^{(2,q)} \), and hence \( \psi_{q^2}(\omega^a R_3) = \frac{(q-1)(1+G_{\eta}(q))}{4} \). If \( a = q + 1 \), then \( t = 0 \) and \( s \in C_1^{(2,q)} \), and hence
ψ_{F,q}^ω(\omega^aR_3) = \frac{(q-1)(-1-G_q(n))}{4}$. Next, we treat the case where $s, t \neq 0$. Define

\begin{align*}
G_3 &= \{a (\mod 2(q+1)) \mid \omega^a = s + tw^e, s, t \in C_0^{(2,q)}\}, \\
G_4 &= \{a (\mod 2(q+1)) \mid \omega^a = s + tw^e, s, t \in C_1^{(2,q)}\}, \\
G_5 &= \{a (\mod 2(q+1)) \mid \omega^a = s + tw^e, (s, t) \in C_0^{(2,q)} \times C_1^{(2,q)} \text{ or } C_1^{(2,q)} \times C_0^{(2,q)}\}.
\end{align*}

Then, we have

$$
ψ_{F,q}^ω(\omega^aR_3) = \begin{cases} 
\frac{(1-G_q(n))^2}{4}, & \text{if } a \in G_3, \\
\frac{(1+G_q(n))^2}{4}, & \text{if } a \in G_4, \\
\frac{1-(-1+1/q)}{4}, & \text{if } a \in G_5.
\end{cases}
$$

We need to show that $G_i = Y_{i,c}$, $i = 3, 4, 5$. Let $a \in G_3$. Then, there are some $s, t \in C_0^{(2,q)}$ such that $\omega^a = s + tw^e$. Taking trace of both sides of $\omega^{a+\frac{q+1}{4}e} = s\omega^{\frac{q+1}{4}e} + tw^{e+\frac{q+1}{4}e}$, we have $\Tr_{q^2/q}(\omega^{a+\frac{q+1}{4}e}) = s\Tr_{q^2/q}(\omega^{\frac{q+1}{4}e}) + t\Tr_{q^2/q}(\omega^{e+\frac{q+1}{4}e})$. Since $\Tr_{q^2/q}(\omega^{\frac{q+1}{4}e}) = 0$ and $\Tr_{q^2/q}(\omega^{e+\frac{q+1}{4}e}) \in C_0^{(2,q)}$, we obtain $\Tr_{q^2/q}(\omega^{a+\frac{q+1}{4}e}) \in C_0^{(2,q)}$, i.e., $a \in I_2 - \frac{ q+1 }{ 2 } e$. On the other hand, taking trace of both sides of $\omega^{a+\frac{q+1}{4}(e+\frac{q+1}{4})} = s\omega^{\frac{q+1}{4}e} + tw^{e+\frac{q+1}{4}e}$, we have $\Tr_{q^2/q}(\omega^{a+\frac{q+1}{4}(e+\frac{q+1}{4})}) = s\Tr_{q^2/q}(\omega^{\frac{q+1}{4}e}) + t\Tr_{q^2/q}(\omega^{\frac{q+1}{4}(e+\frac{q+1}{4})})$. Since $\Tr_{q^2/q}(\omega^{\frac{q+1}{4}e}) = 0$ and $\Tr_{q^2/q}(\omega^{\frac{q+1}{4}(e+\frac{q+1}{4})}) \in C_0^{(2,q)}$ , we obtain $\Tr_{q^2/q}(\omega^{a+\frac{q+1}{4}(e+\frac{q+1}{4})}) \in C_0^{(2,q)}$, i.e., $a \in I_2 + c - \frac{ q+1 }{ 2 } \delta$. Thus, $a \in (I_2 - \frac{ q+1 }{ 2 } e) \cap (I_2 + c - \frac{ q+1 }{ 2 } \delta)$, and hence $G_3 \subseteq Y_{3,c}$. Noting that $|G_3| = |Y_{3,c}|$, it follows that $G_3 = Y_{3,c}$. Furthermore, since $G_2 \equiv G_3 + (q+1) (\text{mod } 2(q+1))$ and $G_5 = \{0, 1, \ldots, 2q+1\} \setminus (G_3 \cup G_4 \cup \{0, c, q+1, c+q+1\})$, we have $G_4 = Y_{4,c}$ and $G_5 = Y_{5,c}$.

Finally, the character values of $R_4$ and $R_5$ are determined as $ψ_{F,q}^ω(\omega^aR_4) = ψ_{F,q}^ω(\omega^{a+q+1}R_3)$ and $ψ_{F,q}^ω(\omega^aR_5) = -1 - \sum_{i=1}^{q} ψ_{F,q}^ω(\omega^aR_i)$. This completes the proof of the proposition.

\begin{remark}
By the definition of $Y_{i,c}$, $i = 1, 2$, in Proposition 4.11, it is clear that $-Y_{i,c} + c \equiv Y_{i,c} (\text{mod } 2(q+1))$, that is, the property (P8).
\end{remark}

Next, we show that the $Y_{i,c}$’s have property (P9).

\begin{proposition}
We have

$-(Y_{3,c} \cup Y_{4,c}) + c \equiv Y_{5,c} (\text{mod } 2(q+1)).$

\begin{proof}
Since $Y_{i,c} = G_i$ for $i = 3, 4, 5$ as in the proof of Proposition 4.11 we have

\begin{align*}
Y_{3,c} \cup Y_{4,c} &= \{a (\mod 2(q+1)) \mid \omega^a = s + tw^e, (s, t) \in S \times S \text{ or } N \times N\}, \\
Y_{5,c} &= \{a (\mod 2(q+1)) \mid \omega^a = s + tw^e, (s, t) \in S \times S \text{ or } N \times N\}.
\end{align*}

Assume that $a \in -(Y_{3,c} \cup Y_{4,c}) + c$. There are some $s', t' \in F_q$ such that $\omega^a = s' + t'w^e$. On the other hand, since $a \in -(Y_{3,c} \cup Y_{4,c}) + c$, $\omega^{-a+c} = s + tw^e$ for some $s, t \in S \times S \text{ or } N \times N$. Then, we have

$$
(\omega^{-a + c} + t)(s' + t'\omega^e) = 1. 
$$

(4.14)

By multiplying both sides of (4.14) by $\omega^{\frac{q+1}{2}e}$ and taking trace, we have

$$
ss'\Tr(\omega^{-c+\frac{q+1}{2}e}) + (ts' + st')\Tr_{q^2/q}(\omega^{\frac{q+1}{2}e}) + tt'\Tr_{q^2/q}(\omega^{c+\frac{q+1}{2}e}) = \Tr_{q^2/q}(\omega^{\frac{q+1}{2}e}).
$$

(4.15)

Since $\Tr_{q^2/q}(\omega^{\frac{q+1}{2}e}) = 0$ by the definition of $X_{1,c}$, (4.15) is reduced to

$$
-ss'u\omega^{\frac{q+1}{2}(e-\delta)} = tt',
$$

where $u = \Tr_{q^2/q}(\omega^{c+\frac{q+1}{2}e})$ and $v = \Tr_{q^2/q}(\omega^{-c+\frac{q+1}{2}e})$. Here, $u, v \in C_0^{(2,q)}$ by (4.12). Furthermore, $s^{-1} \in C_0^{(2,q)}$ by the definitions of $s, t$, and $-\omega^{\frac{q+1}{2}(e-\delta)} \in C_1^{(2,q)}$ by the definitions of $e, \delta$. Hence, either $(s', t') \in C_0^{(2,q)} \times C_1^{(2,q)}$ or $C_1^{(2,q)} \times C_0^{(2,q)}$ holds by noting that $(s', t') = (0, 0)$ is impossible.

$\square$
\end{proof}
\end{proposition}
Therefore, \( a \in Y_{5,c} \), i.e., \(- (Y_{3,c} \cup Y_{4,c}) + c \subseteq Y_{5,c}\), follows. Finally, since \(| - (Y_{3,c} \cup Y_{4,c}) + c| = |Y_{3,c} \cup Y_{4,c}| = |Y_{5,c}|\), the statement of the proposition follows. \( \square \)

Finally, we show that the \( R'_i \)'s have property (P10).

**Proposition 4.14.** Let \( R'_i \), \( i = 1, 2, 3, 4, 5 \), be defined as in Subsection 4.1. Then, \( R'_i \), \( i = 1, 2, 3, 4, 5 \), take the character values listed in Table 2.

**Proof:** Since \( Y_{i,c} - c + \frac{q+1}{2} \delta \equiv X_{i,c} - \frac{q+1}{2} \delta \) by Lemma 4.9, Remark 4.10 (5) and the definitions of \( X_{i,c}, Y_{i,c} \), \( i = 1, 2, 3, 4, 5 \), the statement follows from Proposition 4.11. \( \square \)

**REFERENCES**

[1] K. T. Arasu, J. F. Dillon, D. Jungnickel, A. Pott, The solution of the Waterloo problem, *J. Combin. Theory, Ser. A* 71 (1995), 316–331.
[2] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
[3] A. E. Brouwer, R. M. Wilson, Q. Xiang, Cyclotomy and strongly regular graphs, *J. Alg. Combin.* 10 (1999), 25–28.
[4] Y. Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields Appl.* 3 (1997), 234–256.
[5] J. A. Davis, Difference sets in abelian 2-groups, *J. Combin. Theory, Ser. A* 57 (1991), 262–286.
[6] M. van Eupen, V. D. Tonchev, Linear codes and the existence of a reversible Hadamard difference set in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4^5 \), *J. Combin. Theory, Ser. A* 79 (1997), 161–167.
[7] D. Jungnickel, *Difference Sets*. Contemporary design theory, 241–324, Wiley-Interscience. Ser. Discrete Math. Optim., Wiley-Interscience. Publ., Wiley, New York, 1992.
[8] R. G. Kraemer, Proof of a conjecture on Hadamard 2-groups, *J. Combin. Theory, Ser. A* 63 (1993), 1–10.
[9] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.
[10] R. L. McFarland, Difference sets in abelian groups of order \( 4p^2 \), *Mitt. Math. Sem. Giessen* 192 (1989), 1–70.
[11] R. J. Turyn, A special class of Williamson matrices and difference sets, *J. Combin. Theory, Ser. A* 36 (1984), 111–115.
[12] R. M. Wilson, Q. Xiang, Constructions of Hadamard difference sets, *J. Combin. Theory, Ser. A* 77 (1997), 148–160.
[13] M. Y. Xia, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory, Ser. A* 61 (1992), 230–242.
[14] Q. Xiang, Y. Q. Chen, On Xia’s construction of Hadamard difference sets, *Finite Fields Appl.* 2 (1996), 87–95.

**Faculty of Education, Kumamoto University,** 2-40-1 Kurokami, Kumamoto 860-8555, Japan
**E-mail address:** momihara@educ.kumamoto-u.ac.jp

**Department of Mathematical Sciences, University of Delaware,** Newark, DE 19716, USA
**E-mail address:** xiang@math.udel.edu