ALGEBRAIC COMBINATORICS

Mitsugu Hirasaka, Koji Momihara & Sho Suda

A new approach to the excess problem of Hadamard matrices

Mitsugu Hirasaka, Koji Momihara & Sho Suda

ABSTRACT In this paper, we give a new technique to find families of Hadamard matrices with maximum excess. In particular, we find regular or biregular Hadamard matrices with maximum excess by negating some rows and columns of known Hadamard matrices obtained from quadratic residues of finite fields. More precisely, we show that if either $(2m + 1)^2 + 2$ or $m^2 + (m + 1)^2$ is a prime power, then there exists a biregular Hadamard matrix of order $n = (2m + 1)^2 + 3$ with maximum excess. Furthermore, we give a sufficient condition for Hadamard matrices obtained from quadratic residues being transformed to regular ones in terms of four-class translation association schemes on finite fields. The core part of this paper is how to find "switching" sets of rows and columns.

1. INTRODUCTION

In this paper, we assume that the reader is familiar with the basic theories of block designs, association schemes, and characters of finite fields. We refer the reader to [5] for block designs, [2] for association schemes, and [3, 17] for characters of finite fields.

A *Hadamard matrix of order n* is an $n \times n$ $(-1, 1)$-matrix H satisfying $HH^\top = H^\top H = nI_n$, where I_n is the $n \times n$ unit matrix. It is well known that $n = 1, 2$ or a multiple of 4. Conversely, it is conjectured that a Hadamard matrix of order n exists for every positive integer n divisible by 4.

It is clear that if rows and columns of a Hadamard matrix H are permuted, the matrix remains to be a Hadamard matrix. Furthermore, the matrix obtained from a Hadamard matrix by multiplying some rows and columns by -1 also remains to be a Hadamard matrix. We say that two Hadamard matrices are *equivalent* if one can be obtained from the other by a sequence of row and column permutations and negations. This is the same as saying that two Hadamard matrices are equivalent if one can be obtained from the other by premultiplication and postmultiplication by signed permutation matrices. In this paper, we mainly treat negations of rows and columns of Hadamard matrices. In this case, the corresponding signed permutation matrices are just $(1, -1)$-diagonal matrices.

Let $\mathbf{1}_n$ denote the all-one vector of length n. A Hadamard matrix H is called *regular* if $H\mathbf{1}_n = r\mathbf{1}_n$ for some positive integer r. Write $H\mathbf{1}_n = (h_1, h_2, \ldots, h_n)^\top$. Then,

$$nr^2 = \sum_{i=1}^{n} h_i^2 = (\mathbf{1}_n^\top H^\top)(H\mathbf{1}_n) = n\mathbf{1}_n^\top \mathbf{1}_n = n^2.$$

Hence, n must be a square, namely, $n = 4m^2$, and $r = 2m$.

We say that a Hadamard matrix H is *biregular* if the entries of $H\mathbf{1}_n$ take exactly two nonnegative integers, namely, k_1 and k_2. Here, k_i, $i = 1, 2$, must be even integers in the same residue class modulo 4 by the orthogonality of the rows of H. Let m_1 (resp. m_2) be the frequency of k_1 (resp. k_2) appearing in $H\mathbf{1}_n$. Write $H\mathbf{1}_n = (h_1, h_2, \ldots, h_n)^\top$. Then,

$$m_1 + m_2 = n$$

and

$$m_1 k_1^2 + m_2 k_2^2 = \sum_{i=1}^{n} h_i^2 = (\mathbf{1}_n^\top H^\top)(H\mathbf{1}_n) = n\mathbf{1}_n^\top \mathbf{1}_n = n^2.$$

Hence,

$$(1) \qquad m_1 = \frac{n^2 - nk_2^2}{k_1^2 - k_2^2} \quad \text{and} \quad m_2 = \frac{-n^2 + nk_1^2}{k_1^2 - k_2^2}.$$

In this paper, we are interested in Hadamard matrices that can be transformed to regular or biregular ones.

We now explain one of major motivations for studying regular or biregular Hadamard matrices. Let $E(H)$ denote the sum of all entries of H. We say that $E(H)$ is the *excess* of H. Several upper bounds on $E(H)$ have been known [4, 9, 16]. We will give one of the known upper bounds on $E(H)$ below.

PROPOSITION 1.1 ([9]). *Let H be a Hadamard matrix of order n and let k be an even integer such that $k \leqslant \sqrt{n} < k + 2$. Let $t = k$ if $|n - k^2| < |n - (k+2)^2|$ and $t = k - 2$ otherwise. Then, it holds that $E(H) \leqslant n(t + 4) - 4s$, where s is the integer part of $n((t+4)^2 - n)/(8t + 16)$, with equality holds if and only if n is a square and H is regular or n is a nonsquare and the entries of $H\mathbf{1}_n$ are either in $\{k, k+4\}$ or $\{k-2, k+2\}$ depending on whether $t = k$ or $t = k - 2$, respectively.*

Note that if a Hadamard matrix H is regular or biregular with maximum excess attaining the bound of Proposition 1.1, then $H^\top$ is also regular or biregular, respectively.

The excess of Hadamard matrices has been studied in [4, 7, 8, 10, 11, 12, 13, 14, 15, 16, 21, 23]. In particular, many constructions for regular Hadamard matrices are known in relation to *Menon designs*. On the other hand, as far as the authors know, there are only a few papers that theoretically treat biregular Hadamard matrices with maximum excess [12, 14]. In fact, in most of papers treating biregular Hadamard matrices with maximum excess, new examples have been found by using computer. Furthermore, in [12, 14], the authors modified known composition constructions of Hadamard matrices to obtain biregular ones with maximum excess. In particular, [14], it was shown that there is a biregular Hadamard matrix of order $n = (2m + 1)^2 + 3$ with maximum excess attaining the bound of Proposition 1.1 if m is a prime power and $m^2 + m + 1$ is a prime. In this paper, we will also treat Hadamard matrices of order $n = (2m + 1)^2 + 3$. However, our approach is completely different from those in [12, 14]. We will transform Hadamard matrices obtained from quadratic residues of finite fields to become regular or biregular by negating some rows and columns. The core part of this paper is to find such "switching" sets of rows and columns.

We now briefly explain two known constructions of Hadamard matrices based on quadratic residues of finite fields and our main results.

Let $\mathbb{F}_q$ be the finite field of order q and C be the set of nonzero squares of $\mathbb{F}_q$. We start from the following known construction of Hadamard matrices. Assume that $q \equiv 3 \pmod 4$. Let M be a $q \times q$ $(1, -1)$-matrix whose rows and columns are labeled by the elements of $\mathbb{F}_q$ and entries are defined by

$$M_{i,j} = \begin{cases} 1, & \text{if } j - i \in C \cup \{0\}, \\ -1, & \text{if } j - i \in \mathbb{F}_q \smallsetminus (C \cup \{0\}). \end{cases}$$

Define

$$(2) \qquad\qquad H = \begin{pmatrix} -1 & \mathbf{1}_q^\top \\ \mathbf{1}_q & M \end{pmatrix}.$$

Then H forms a Hadamard matrix of order $n = q + 1$. We will prove the following theorem in Section 4.

THEOREM 1.2. *If $q = (2m + 1)^2 + 2$ is a prime power, then there exists a biregular Hadamard matrix of order $n = (2m+1)^2 + 3$ with maximum excess attaining the bound of Proposition* 1.1. *In particular, the matrix H defined in* (2) *can be transformed to a biregular Hadamard matrix with maximum excess by negating some rows and columns.*

Next, we consider the case where $q \equiv 1 \pmod 4$. Let M be a $q \times q$ $(0, 1, -1)$-matrix whose rows and columns are labeled by the elements of $\mathbb{F}_q$ and entries are defined by

$$M_{i,j} = \begin{cases} 0, & \text{if } j - i = 0, \\ 1, & \text{if } j - i \in C, \\ -1, & \text{if } j - i \in \mathbb{F}_q \smallsetminus (C \cup \{0\}). \end{cases}$$

Define $M_1 = M + I_q$, $M_2 = M - I_q$, and $M_3 = -M_1$. Furthermore, define

$$(3) \qquad\qquad H = \begin{pmatrix} 1 & -1 & \mathbf{1}_q^\top & \mathbf{1}_q^\top \\ -1 & -1 & \mathbf{1}_q^\top & -\mathbf{1}_q^\top \\ \mathbf{1}_q & \mathbf{1}_q & M_1 & M_2 \\ \mathbf{1}_q & -\mathbf{1}_q & M_2 & M_3 \end{pmatrix}.$$

Then, H forms a Hadamard matrix of order $n = 2q + 2$. We will prove the following theorem in Section 5.

THEOREM 1.3. *If $q = m^2 + (m + 1)^2$ is a prime power, then there exists a biregular Hadamard matrix of order $n = (2m+1)^2 + 3$ with maximum excess attaining the bound of Proposition* 1.1. *In particular, the matrix H defined in* (3) *can be transformed to a biregular Hadamard matrix with maximum excess by negating some rows and columns.*

We also show the following theorem to obtain a regular Hadamard matrix from H defined in (3).

THEOREM 1.4. *Let $q = 2m^2 - 1$ be a prime power with m odd. Let $X_0 = \{0\}$, and assume that there are subsets X_i, $i = 1, 2, 3, 4$, of $\mathbb{F}_{q^2}$ partitioning $\mathbb{F}_{q^2} \smallsetminus \{0\}$ satisfying the following conditions:*

(1) *$X_1 = \omega^{2m^2} X_3$ and $X_2 = \omega^{2m^2} X_4$, where ω is a fixed primitive element of $\mathbb{F}_{q^2}$;*
(2) *Each X_i, $i = 1, 2, 3, 4$, is a union of cosets of the multiplicative subgroup of index $4m^2$ of $\mathbb{F}_{q^2}$;*
(3) *$(\mathbb{F}_{q^2}, \{R_i\}_{i=0}^4)$ is a four-class translation association scheme with a prescribed first eigenmatrix. Here, for $i = 0, 1, 2, 3, 4$, $(x, y) \in R_i$ if and only if $x - y \in X_i$.*

Then, there exists a regular Hadamard matrix of order $n = 4m^2$. In particular, the matrix H defined in (3) can be transformed to a regular Hadamard matrix by negating some rows and columns.

We will explain this theorem in details in Section 6. Roughly speaking, this theorem implies that a four-class translation association scheme on $(\mathbb{F}_{q^2}, +)$ yields a regular Hadamard matrix of order $n = 2(q + 1)$. Thus, we find a nontrivial relationship between regular Hadamard matrices and association schemes.

2. Preliminaries

2.1. **Block designs and t-intersection sets.** Let P be a finite set of v elements, called *points*, and $\mathcal{B}$ be a family of b subsets of P, called *blocks*. We define $\mathcal{F} = \{(p, B) \in P \times \mathcal{B} : p \in B\}$. Elements in $\mathcal{F}$ are called *flags*. The triple $(P, \mathcal{B}, \mathcal{F})$ is called a *block design*. We say that $(\mathcal{B}, P, \mathcal{F}^\perp)$ with $\mathcal{F}^\perp = \{(B, p) : (p, B) \in \mathcal{F}\}$ is the *dual* of $(P, \mathcal{B}, \mathcal{F})$. For convenience, we also say that the pair $(P, \mathcal{B})$ is a *block design*.

Let $(P, \mathcal{B})$ be a block design and M be the incidence matrix of $(P, \mathcal{B})$, whose (p, B)th entry is 1 if $(p, B) \in \mathcal{F}$ (equivalently, $p \in B$) and 0 otherwise. A block design $(P, \mathcal{B})$ with incidence matrix M is called a *pairwise balanced design* if there is a positive integer λ such that each off-diagonal entry of $MM^\top$ is λ. In addition, if $M\mathbf{1}_b = r\mathbf{1}_v$ for some integer r, it is called an (r, λ)-*design*. Furthermore, if an (r, λ)-design satisfies that $\mathbf{1}_v^\top M = k\mathbf{1}_b$, it is called a 2-*design*. In particular, if $v = b$, it is called *symmetric*.

Let H be a regular Hadamard matrix of order $n = 4m^2$. Then, the $(0, 1)$-matrix $M = (-H + J_n)/2$ satisfies that

$$MM^\top = \frac{HH^\top - HJ_n - J_nH^\top + J_nJ_n}{4} = m^2 I_n + (m^2 - m)J_n,$$

where J_n is the $n \times n$ all-one matrix. This implies that M is an incidence matrix of a symmetric 2-design with parameters $(v, k, \lambda) = (4m^2, 2m^2 - m, m^2 - m)$, the so-called *Menon design*.

Let H be a biregular Hadamard matrix of order n. We can assume that

$$H\mathbf{1}_n = \begin{pmatrix} k_1\mathbf{1}_{m_1} \\ k_2\mathbf{1}_{m_2} \end{pmatrix}$$

by suitably permuting rows. Let H_1 (resp. H_2) be the upper $m_1 \times n$ (resp. lower $m_2 \times n$) matrix of H. Then, each $M_i = (-H_i + J_{m_i,n})/2$, $i = 1, 2$, satisfies that

$$M_iM_i^\top = \frac{nH_iH_i^\top - H_iJ_{m_i,n}^\top - J_{m_i,n}H_i^\top + J_{m_i,n}J_{m_i,n}^\top}{4} = \frac{nI_{m_i} + (n - 2k_i)J_{m_i}}{4},$$

where $J_{m_i,n}$ is the $m_i \times n$ all-one matrix. Hence, each M_i is the incidence matrix of a pairwise balanced design. In particular, each M_i satisfies that $M_i\mathbf{1}_n = (n - k_i)/2$. Hence, it is an $((n - k_i)/2, (n - 2k_i)/4)$-design.

We introduce the concept of t-intersection sets for block designs. We refer the reader to [19] for details of two-intersection sets. Let $(P, \mathcal{B})$ be a block design with incidence matrix M and D be a j-subset of P. We say that D is a *t-intersection set with parameters* $(j; \{\alpha_1, \alpha_2, \ldots, \alpha_t\})$ *for* $(P, \mathcal{B})$ if

$$\{|B \cap D| : B \in \mathcal{B}\} = \{\alpha_1, \alpha_2, \ldots, \alpha_t\}.$$

Let $\mathbf{x}$ be the $(0, 1)$-vector of length v, whose ith entry is 1 if $i \in D$ and 0 otherwise. We call $\mathbf{x}$ the *support vector* of D in P. Then, D is a t-intersection set with parameters $(j; \{\alpha_1, \alpha_2, \ldots, \alpha_t\})$ for $(P, \mathcal{B})$ if and only if all entries of $\mathbf{x}^\top M$ are in $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ and $\mathbf{x}^\top \mathbf{1}_v = j$. We define the *duals* of D as

(4) $$D_{\alpha_i}^\perp = \{B : B \in \mathcal{B}, |B \cap D| = \alpha_i\}, \quad i = 1, 2, \ldots, t.$$

In this paper, we treat t-intersection sets with $t \leqslant 4$ for a block design obtained from translations of the set of squares in a finite field. In particular, we will transform a (non-regular) Hadamard matrix to become regular or biregular by negating columns and rows corresponding to a t-intersection set and its dual, respectively.

2.2. ASSOCIATION SCHEMES. Let X be a finite set, and a set of relations $R_0, R_1, \ldots, R_d$ be a partition of $X \times X$ such that $R_0 = \{(x, x) : x \in X\}$, and for each $i \in \{0, 1, \ldots, d\}$, ${}^t R_i = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where ${}^t R_i = \{(x, y) \in X \times X : (y, x) \in R_i\}$. We call $(X, \{R_i\}_{i=0}^d)$ a *d-class association scheme* if for all $i, j, k \in \{0, 1, \ldots, d\}$ there is an integer $p_{i,j}^k$ such that for all $(x, y) \in R_k$,

$$|\{z \in X : (x, z) \in R_i, (z, y) \in R_j)\}| = p_{i,j}^k.$$

These constants are called *intersection numbers*. If $p_{i,j}^k = p_{j,i}^k$ for all $h, i, j \in \{0, 1, \ldots, d\}$, it is called *commutative*. If ${}^t R_i = R_i$ for all $i \in \{0, 1, 2, \ldots, d\}$, then it is called *symmetric*. A symmetric association scheme is necessarily commutative. In this paper, we will treat symmetric association schemes.

We denote by A_i the adjacency matrix of R_i for each i, whose (x, y)th entry is 1 if $(x, y) \in R_i$ and 0 otherwise. The condition above is equivalent to that

$$A_i A_j = \sum_{k=0}^d p_{i,j}^k A_k.$$

The *Bose–Mesner algebra* for an association scheme $(X, \{R_i\}_{i=0}^d)$ is defined as $\mathcal{A} = \langle A_0, A_1, \ldots, A_d \rangle$. Since each R_i is symmetric, $\mathcal{A}$ is commutative. Then, there exists a set of minimal idempotents $E_0 = \frac{1}{|X|} J_{|X|}, E_1, \ldots, E_d$, which also form a basis of the algebra. The matrix P such that

$$(A_0, A_1, \ldots, A_d) = (E_0, E_1, \ldots, E_d) P$$

is called the *first eigenmatrix* (or *character table*) of $(X, \{R_i\}_{i=0}^d)$. On the other hand, the matrix Q such that

$$(A_0, A_1, \ldots, A_d) Q = |X|(E_0, E_1, \ldots, E_d)$$

is called the *second eigenmatrix* of $(X, \{R_i\}_{i=0}^d)$.

A *translation association scheme* is an association scheme $(X, \{R_i\}_{i=0}^d)$ for which the underlying set X is identified with an abelian group, and for all relations R_i's, $(x, y) \in R_i$ implies $(x + z, y + z) \in R_i$ for all $z \in X$. Then, there is a partition $D_0 = \{0\}, D_1, \ldots, D_d$ of X such that for each $i = 0, 1, \ldots, d$,

$$R_i = \{(x, x + y) : x \in X, y \in D_i\}.$$

For a translation association scheme $(X, \{R_i\}_{i=0}^d)$, there is an equivalence relation defined on the character group $X^\perp$ of X as follows: $\chi \sim \chi'$ if and only if $\chi(D_i) = \chi'(D_i)$ for all $i = 0, 1, \ldots, d$. Here, $\chi(D_i) := \sum_{x \in D_i} \chi(x)$. Denote by $D_0', D_1' \ldots, D_d'$ the equivalence classes, where D_0' consists of only the trivial character. Define the relation R_i' on $X^\perp$ as

$$R_i' = \{(\chi, \chi \chi') : \chi \in X^\perp, \chi' \in D_i'\}.$$

Then, $(X^\perp, \{R_i'\}_{i=0}^d)$ forms a translation association scheme, called the *dual* of $(X, \{R_i\}_{i=0}^d)$. We remark that the entries of the ith column of the first eigenmatrix of $(X, \{R_i\}_{i=0}^d)$ are given by the $d + 1$ character values $\chi(D_i)$, where $\chi \in D_j'$, $j = 0, 1, 2 \ldots, d$. Furthermore, the first eigenmatrix of the dual scheme is equal to the second eigenmatrix of $(X, \{R_i\}_{i=0}^d)$.

Given two association schemes $(X, \{R_i\}_{i=0}^d)$ and $(X, \{R_i'\}_{i=0}^e)$, if for each $i = 0, 1, \ldots, d$, $R_i \subseteq R_j'$ for some j, then $(X, \{R_i\}_{i=0}^d)$ is called a *fission scheme* of

$(X, \{R_i'\}_{i=0}^e)$, and $(X, \{R_i'\}_{i=0}^e)$ is called a *fusion scheme* of $(X, \{R_i\}_{i=0}^d)$. We will use the following well-known criterion due to Bannai [1] and Muzychuk [20], called the *Bannai–Muzychuk criterion*.

PROPOSITION 2.1. *Let P be the first eigenmatrix of an association scheme $(X, \{R_i\}_{i=0}^d)$, and let $\Lambda_0 := \{0\}, \Lambda_1, \ldots, \Lambda_e$, be a partition of $\{0, 1, \ldots, d\}$. Then, $(X, \{\bigcup_{j \in \Lambda_i} R_j\}_{i=0}^e)$ forms an association scheme if and only if there exists a partition $\{\Delta_0 = \{0\}, \Delta_1, \ldots, \Delta_e\}$ of $\{0, 1, \ldots, d\}$ such that (Δ_i, Λ_j)-block of P has a constant row sum. Moreover, the constant row sum of the (Δ_i, Λ_j)-block is the (i, j)th entry of the first eigenmatrix of $(X, \{\bigcup_{j \in \Lambda_i} R_j\}_{i=0}^e)$.*

2.3. CHARACTERS OF FINITE FIELDS. Let p be a prime, f a positive integer, and set $q = p^f$. For a positive integer m, let $\zeta_m = \exp(\frac{2\pi i}{m})$ denote the primitive mth root of unity. Let $\mathbb{F}_q$ denote the finite field of order q and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$. For a positive integer e dividing $q - 1$ and a fixed primitive element ω of $\mathbb{F}_q$, define

$$C_i^{(e,q)} := \omega^i \langle \omega^e \rangle, \quad i = 0, 1, \ldots, e - 1,$$

where the subscript i is taken modulo e. The canonical additive character $\psi_{\mathbb{F}_q}$ of $\mathbb{F}_q$ is defined by

$$\psi_{\mathbb{F}_q}(x) = \zeta_p^{\mathrm{Tr}_{q/p}(x)}, \ x \in \mathbb{F}_q,$$

where $\mathrm{Tr}_{q/p}$ is the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ defined by

$$\mathrm{Tr}_{q/p}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{f-1}}.$$

Define $R_0 = \{(x, x) : x \in \mathbb{F}_q\}$ and $R_i := \{(x, y) : x - y \in C_{i-1}^{(e,q)}\}$, $i = 1, 2, \ldots, e$. Then, $(\mathbb{F}_q, \{R_i\}_{i=0}^e)$ is an e-class translation association scheme, called the *cyclotomic scheme*. The first eigenmatrix P of the e-class cyclotomic scheme is given by the $(e + 1) \times (e + 1)$ matrix (with the rows of P arranged in a certain way)

$$P = \begin{pmatrix} 1 & k & k & \cdots & k \\ 1 & \eta_0 & \eta_1 & \cdots & \eta_{e-1} \\ 1 & \eta_1 & \eta_2 & \cdots & \eta_0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \eta_{e-1} & \eta_0 & \cdots & \eta_{e-2} \end{pmatrix},$$

where $k = \frac{q-1}{e}$ and η_i, $i = 0, 1, \ldots, e - 1$, are given by

$$\eta_i = \sum_{x \in C_i^{(e,q)}} \psi_{\mathbb{F}_q}(x),$$

the so-called *Gauss periods* of order e of $\mathbb{F}_q$.

For a multiplicative character χ and the canonical additive character $\psi_{\mathbb{F}_q}$ of $\mathbb{F}_q$, we define the *Gauss sum* by

$$G_q(\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi_{\mathbb{F}_q}(x) \in \mathbb{Z}[\zeta_{q-1}, \zeta_p].$$

We will use the following basic properties of Gauss sums without preamble.

(1) $G_q(\chi)\overline{G_q(\chi)} = q$ if χ is nontrivial;
(2) $G_q(\chi^{-1}) = \chi(-1)\overline{G_q(\chi)}$;
(3) $G_q(\chi) = -1$ if χ is trivial.

For a nontrivial multiplicative character χ of $\mathbb{F}_q$ and $x \in \mathbb{F}_q^*$, by the orthogonality of characters [17, (5.16), p. 195], it holds that

$$(5) \qquad \chi(x) = \frac{\chi(-1)G_q(\chi)}{q} \sum_{a \in \mathbb{F}_q^*} \chi^{-1}(a)\psi_{\mathbb{F}_q}(ax).$$

On the other hand, the Gauss period $\psi_{\mathbb{F}_q}(C_i^{(e,q)})$ can be expressed as a linear combination of Gauss sums:

$$(6) \qquad \psi_{\mathbb{F}_q}(C_i^{(e,q)}) = \frac{1}{e} \sum_{j=0}^{e-1} G_q(\chi^j)\chi^{-j}(\omega^i), \ 0 \leqslant i \leqslant e - 1,$$

where χ is a multiplicative character of order e of $\mathbb{F}_q$. For example, if $e = 2$, we have

$$(7) \qquad \psi_{\mathbb{F}_q}(C_i^{(2,q)}) = \frac{-1 + (-1)^i G_q(\eta)}{2}, \quad i = 0, 1,$$

where η is the quadratic character of $\mathbb{F}_q$. In particular, the quadratic Gauss sum is explicitly evaluated as follows.

THEOREM 2.2. [17, Theorem 5.15] *Let $q = p^f$ be a prime power with p a prime and η be the quadratic character of $\mathbb{F}_q$. Then,*

$$G_q(\eta) = \begin{cases} (-1)^{f-1}q^{1/2}, & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{f-1}\zeta_4^f q^{1/2}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We will use the following formula on Gauss sums of order 8 of $\mathbb{F}_{q^2}$.

THEOREM 2.3 ([18, Theorem 1.5]). *Let $q = p^f \equiv 3 \pmod 8$ be a prime power with p a prime and χ_8 be a multiplicative character of $\mathbb{F}_{q^2}$. Furthermore, let η be the quadratic character of $\mathbb{F}_q$. Then, $G_{q^2}(\chi_8)/G_q(\eta) \in \mathbb{Z}[\sqrt{-2}]$. In particular, if $q = a^2 + 2b^2$ is a proper representation of q with $a, b \in \mathbb{Z}$ and $p \nmid a + b\sqrt{-2}$. Then,*

$$G_{q^2}(\chi_8) = G_q(\eta)(a + b\sqrt{-2}),$$

where the signs of a, b are ambiguously determined.

Note that only the case where q is a prime in the theorem above was treated in [18]. It is easy to generalize the claim to the case where q is a prime power by noting that $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization domain. In this paper, we do not need to care about the signs of a, b.

Furthermore, we need the following formula on Gauss sums, the so-called *Davenport–Hasse lifting formula*.

THEOREM 2.4 ([3, Theorem 11.5.2]). *Let χ' be a nontrivial multiplicative character of $\mathbb{F}_q$ and let χ be the lift of χ' to $\mathbb{F}_{q^d}$, i.e., $\chi(\alpha) = \chi'(\text{Norm}_{q^d/q}(\alpha))$ for $\alpha \in \mathbb{F}_{q^d}$, where $d \geqslant 2$ is an integer. Then*

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

Next, we define *Jacobi sums*. For multiplicative characters χ_1 and χ_2 of $\mathbb{F}_q$, define

$$J_q(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1 - x) \in \mathbb{Z}[\zeta_{q-1}].$$

Here, we extend the domain of multiplicative characters χ of $\mathbb{F}_q$ to all elements of $\mathbb{F}_q$ by setting $\chi(0) = 1$ or $\chi(0) = 0$ depending on whether χ is trivial or not. There is the following relationship between Jacobi sums and Gauss sums:

$$(8) \qquad J_q(\chi_1, \chi_2) = \frac{G_q(\chi_1)G_q(\chi_2)}{G_q(\chi_1\chi_2)},$$

where $\chi_1, \chi_2, \chi_1\chi_2$ are nontrivial. In this paper, we will use the following formula on Jacobi sums.

Theorem 2.5 ([22]). *Let $q = p^f \equiv 1 \pmod 4$ be a prime power with p a prime. Let η be the quadratic character of $\mathbb{F}_q$ and χ a multiplicative character of order 4 of $\mathbb{F}_q$. Then, $J_q(\eta, \chi) \in \mathbb{Z}[\zeta_4]$. In particular, if $p \equiv 1 \pmod 4$ and $q = a^2 + b^2$ is a proper representation of q with a an odd integer and $p \nmid a + b\zeta_4$. Then,*

$$J_q(\eta, \chi) = a + b\zeta_4,$$

where the signs of a, b are ambiguously determined. If $p \equiv 3 \pmod 4$, f is even and $J_q(\eta, \chi) = -(-q)^{f/2}$.

In this paper, we do not need to care about the signs of a, b in the theorem above.

3. Some properties of t-intersection sets

In this paper, we treat t-intersection sets for block designs obtained from quadratic residues of $\mathbb{F}_q$. Let q be an odd prime power and e be a positive integer dividing $q^2 - 1$ such that $e/\gcd(e, q+1) = 2$. Then, the restriction of a multiplicative character of order e of $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ is of order 2. Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$, and let $C_i^{(e,q^2)} = \omega^i \langle \omega^e \rangle$, $i = 0, 1, \ldots, e - 1$.

Let H be an $e/2$-subset of $\{0, 1, \ldots, e - 1\}$ such that $H \equiv \{0, 1, \ldots, e/2 - 1\}$ $(\bmod \ e/2)$. For a fixed positive integer ℓ not divisible by $q + 1$, define

$$(9) \qquad D_{\ell,H} = \left\{ x \in \mathbb{F}_q \ : \ 1 + x\omega^\ell \in \bigcup_{i \in H} C_i^{(e,q^2)} \right\}.$$

We will use the set $D_{\ell,H}$ to construct t-intersection sets. In this section, we are interested in the sizes of $D_{\ell,H}$ and $D_{\ell,H} \cap (C_0^{(2,q)} + s)$, $s \in \mathbb{F}_q$.

We will use the following lemmas.

Lemma 3.1. *With notations as above, let χ_e be a multiplicative character of order e of $\mathbb{F}_{q^2}$ and η be the quadratic character of $\mathbb{F}_q$. Then,*

$$\sum_{x \in \mathbb{F}_q} \chi_e(1 + \omega^\ell x) = \frac{\chi_e(-1)G_{q^2}(\chi_e)G_q(\eta)}{q} \chi_e(\omega^{-q\ell})\chi_e(\omega^{\ell q} - \omega^\ell).$$

Proof. By (5), we have

$$(10) \qquad \sum_{x \in \mathbb{F}_q} \chi_e(1 + \omega^\ell x) = \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q^2} \sum_{a \in \mathbb{F}_{q^2}^*} \chi_e^{-1}(a)\psi_{\mathbb{F}_{q^2}}(a) \sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_{q^2}}(a\omega^\ell x).$$

Furthermore,

$$\sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_{q^2}}(a\omega^\ell x) = \sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(x\,\mathrm{Tr}_{q^2/q}(a\omega^\ell)) = \begin{cases} 0, & \text{if } \mathrm{Tr}_{q^2/q}(a\omega^\ell) \neq 0, \\ q, & \text{if } \mathrm{Tr}_{q^2/q}(a\omega^\ell) = 0, \end{cases}$$

where $\mathrm{Tr}_{q^2/q}$ is the relative trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$, i.e., $\mathrm{Tr}_{q^2/q}(x) := x + x^q$ for $x \in \mathbb{F}_{q^2}$. It is clear that $\mathrm{Tr}_{q^2/q}(a\omega^\ell) = 0$ if and only if a has the form $a = y\omega^{-\ell + \frac{q+1}{2}}$ with $y \in \mathbb{F}_q$. Hence, continuing from (10), we have

$$\sum_{x \in \mathbb{F}_q} \chi_e(1 + \omega^\ell x) = \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q} \sum_{y \in \mathbb{F}_q^*} \chi_e^{-1}(y\omega^{-\ell + \frac{q+1}{2}})\psi_{\mathbb{F}_{q^2}}(y\omega^{-\ell + \frac{q+1}{2}})$$

$$(11) \qquad = \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q} \sum_{y \in \mathbb{F}_q^*} \chi_e^{-1}(y)\chi_e^{-1}(\omega^{-\ell + \frac{q+1}{2}})\psi_{\mathbb{F}_q}(y\,\mathrm{Tr}_{q^2/q}(\omega^{-\ell + \frac{q+1}{2}})).$$

Since $\mathrm{Tr}_{q^2/q}(\omega^{-\ell+\frac{q+1}{2}}) = \omega^{-\ell+\frac{q+1}{2}}\omega^{-\ell q}(\omega^{\ell q} - \omega^{\ell})$ is a nonzero element in $\mathbb{F}_q$, continuing from (11), we have

$$\sum_{x\in\mathbb{F}_q}\chi_e(1+\omega^\ell x) = \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q}\sum_{y\in\mathbb{F}_q^*}\chi_e^{-1}(y\,\mathrm{Tr}_{q^2/q}(\omega^{-\ell+\frac{q+1}{2}}))$$

$$\times \psi_{\mathbb{F}_q}(y\,\mathrm{Tr}_{q^2/q}(\omega^{-\ell+\frac{q+1}{2}}))\chi_e(\omega^{-q\ell})\chi_e(\omega^{\ell q} - \omega^\ell)$$

$$= \frac{\chi_e(-1)G_{q^2}(\chi_e)G_q(\eta)}{q}\chi_e(\omega^{-q\ell})\chi_e(\omega^{\ell q} - \omega^\ell).$$

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

LEMMA 3.2. *With notations as in Lemma 3.1, it holds that for any $s \in \mathbb{F}_q$*

$$\sum_{x\in\mathbb{F}_q\smallsetminus\{s\}}\chi_e(1+\omega^\ell x)\eta(x-s) = \frac{G_{q^2}(\chi_e)G_q(\eta)}{q}\chi_e^{-1}(1+\omega^{q\ell}s)\chi_e(\omega^{\ell q}-\omega^\ell) - \chi_e(\omega^\ell).$$

Proof. Since $\chi_{e|\mathbb{F}_q} = \eta$, we have

$$\sum_{x\in\mathbb{F}_q\smallsetminus\{s\}}\chi_e(1+\omega^\ell x)\eta(x-s) = \sum_{y\in\mathbb{F}_q^*}\chi_e(1+\omega^\ell(y+s))\chi_e^{-1}(y)$$

$$= \sum_{y\in\mathbb{F}_q^*}\chi_e(y^{-1}(1+\omega^\ell s)+\omega^\ell)$$

$$(12) \qquad\qquad = \sum_{y\in\mathbb{F}_q}\chi_e(y(1+\omega^\ell s)+\omega^\ell) - \chi_e(\omega^\ell).$$

Similar to Lemma 3.1, we have

$$(13) \quad \sum_{y\in\mathbb{F}_q}\chi_e(y(1+\omega^\ell s)+\omega^\ell)$$

$$= \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q^2}\sum_{a\in\mathbb{F}_{q^2}^*}\chi_e^{-1}(a)\psi_{\mathbb{F}_{q^2}}(a\omega^\ell)\sum_{y\in\mathbb{F}_q}\psi_{\mathbb{F}_{q^2}}(ay(1+\omega^\ell s)).$$

Here,

$$\sum_{y\in\mathbb{F}_q}\psi_{\mathbb{F}_{q^2}}(ay(1+\omega^\ell s)) = \sum_{y\in\mathbb{F}_q}\psi_{\mathbb{F}_q}(y\,\mathrm{Tr}_{q^2/q}(a(1+\omega^\ell s)))$$

$$= \begin{cases} 0, & \text{if } \mathrm{Tr}_{q^2/q}(a(1+\omega^\ell s)) \neq 0, \\ q, & \text{if } \mathrm{Tr}_{q^2/q}(a(1+\omega^\ell s)) = 0. \end{cases}$$

It is clear that $\mathrm{Tr}_{q^2/q}(a(1+\omega^\ell s)) = 0$ if and only if a has the form $a = y(1+\omega^\ell s)^{-1}\omega^{\frac{q+1}{2}}$ with $y \in \mathbb{F}_q$. Continuing from (13), we have

$$\sum_{y\in\mathbb{F}_q}\chi_e(y(1+\omega^\ell s)+\omega^\ell)$$

$$= \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q}\sum_{y\in\mathbb{F}_q^*}\chi_e^{-1}(y(1+\omega^\ell s)^{-1}\omega^{\frac{q+1}{2}}))\psi_{\mathbb{F}_{q^2}}(y(1+\omega^\ell s)^{-1}\omega^{\ell+\frac{q+1}{2}})$$

$$(14)$$

$$= \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q}\sum_{y\in\mathbb{F}_q^*}\chi_e^{-1}(y(1+\omega^\ell s)^{-1}\omega^{\frac{q+1}{2}})\psi_{\mathbb{F}_q}(y\,\mathrm{Tr}_{q^2/q}((1+\omega^\ell s)^{-1}\omega^{\ell+\frac{q+1}{2}})).$$

Since $\mathrm{Tr}_{q^2/q}((1+\omega^\ell s)^{-1}\omega^{\ell+\frac{q+1}{2}}) = -(1+\omega^\ell s)^{-1}\omega^{\frac{q+1}{2}}(\omega^{\ell q}-\omega^\ell)(1+\omega^\ell s)^{-q}$ is a nonzero element in $\mathbb{F}_q$, continuing from (14), we have

$$\sum_{y\in\mathbb{F}_q}\chi_e(y(1+\omega^\ell s)+\omega^\ell)$$

$$= \frac{\chi_e(-1)G_{q^2}(\chi_e)}{q}\sum_{y\in\mathbb{F}_q^*}\chi_e^{-1}(y)\psi_{\mathbb{F}_q}(y)\chi_e(-1)\chi_e^{-1}(1+\omega^{q\ell}s)\chi_e(\omega^{\ell q}-\omega^\ell)$$

$$= \frac{G_{q^2}(\chi_e)G_q(\eta)}{q}\chi_e^{-1}(1+\omega^{q\ell}s)\chi_e(\omega^{\ell q}-\omega^\ell).$$

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

We now evaluate the size of $D_{\ell,H}$.

PROPOSITION 3.3. *The sizes of $D_{\ell,H}$ defined in* (9) *is given by*

$$(15) \quad |D_{\ell,H}| = \frac{q}{2} + \frac{\chi_e(-1)G_q(\eta)}{eq}\sum_{i=0}^{e/2-1}A_{2i+1}G_{q^2}(\chi_e^{2i+1})\chi_e^{-(2i+1)}(\omega^{q\ell})\chi_e^{2i+1}(\omega^{\ell q}-\omega^\ell),$$

where $A_i = \sum_{j\in H}\zeta_e^{-ji}$.

Proof. The characteristic function of $\bigcup_{j\in H}C_j^{(e,q^2)}$ is given as

$$(16) \qquad\qquad f(x) = \frac{1}{e}\sum_{j\in H}\sum_{i=0}^{e-1}\zeta_e^{-ji}\chi_e^i(x), \quad x\in\mathbb{F}_{q^2}^*.$$

The size of $D_{\ell,H}$ is expressed as

$$|D_{\ell,H}| = \sum_{x\in\mathbb{F}_q}f(1+\omega^\ell x) = \frac{1}{e}\sum_{i=0}^{e-1}A_i\sum_{x\in\mathbb{F}_q}\chi_e^i(1+x\omega^\ell).$$

Since $H\equiv\{0,1,\ldots,e/2-1\}\pmod{e/2}$, we have $A_i = 0$ if i is even with $i\neq 0$. Furthermore, by Lemma 3.1, it holds that

$$|D_{\ell,H}| = \frac{q}{2} + \frac{\chi_e(-1)G_q(\eta)}{eq}\sum_{i=0}^{e/2-1}A_{2i+1}G_{q^2}(\chi_e^{2i+1})\chi_e^{-(2i+1)}(\omega^{q\ell})\chi_e^{2i+1}(\omega^{\ell q}-\omega^\ell).$$

This completes the proof. $\qquad\square$

We now give another representation for the size of $D_{\ell,H}$ below.

PROPOSITION 3.4. *The sizes of $D_{\ell,H}$ defined in* (9) *is given by*

$$|D_{\ell,H}| = \frac{q}{2} + \frac{\chi_e(-1)G_q(\eta)}{2q} + \frac{\chi_e(-1)G_q(\eta)}{q}\sum_{j\in H}\psi_{\mathbb{F}_{q^2}}(\omega^{q\ell}(\omega^{\ell q}-\omega^\ell)^{-1}C_j^{(e,q^2)}).$$

Proof. By the orthogonality of characters, we have

$$\frac{1}{e}\sum_{i=0}^{e-1}A_iG_{q^2}(\chi_e^i)\chi_e^{-i}(\omega^{q\ell})\chi_e^i(\omega^{\ell q}-\omega^\ell) = \sum_{j\in H}\psi_{\mathbb{F}_{q^2}}(\omega^{q\ell}(\omega^{\ell q}-\omega^\ell)^{-1}C_j^{(e,q^2)}).$$

Hence, continuing from (15), we have

$$|D_{\ell,H}| = \frac{q}{2} + \frac{\chi_e(-1)G_q(\eta)}{2q} + \frac{\chi_e(-1)G_q(\eta)}{q}\sum_{j\in H}\psi_{\mathbb{F}_{q^2}}(\omega^{q\ell}(\omega^{\ell q}-\omega^\ell)^{-1}C_j^{(e,q^2)}).$$

This completes the proof. $\qquad\square$

It is remarkable that this proposition implies that the size of $D_{\ell,H}$ can be evaluated from one of the nontrivial character values of $\bigcup_{i\in H} C_i^{(e,q^2)}$.

We now evaluate the sizes of $D_{\ell,H} \cap (C_0^{(2,q)} + s)$, $s \in \mathbb{F}_q$.

PROPOSITION 3.5. *The size N_s of $D_{\ell,H} \cap (C_0^{(2,q)} + s)$ is given by*

$$(17) \quad N_s = \frac{q-1}{4} - \frac{1}{2e} \sum_{i=0}^{e/2-1} A_{2i+1}(\chi_e^{2i+1}(1+\omega^\ell s) + \chi_e^{2i+1}(\omega^\ell))$$

$$+ \frac{G_q(\eta)}{2eq} \sum_{i=0}^{e/2-1} A_{2i+1} G_{q^2}(\chi_e^{2i+1}) \chi_e^{2i+1}(\omega^{\ell q} - \omega^\ell)$$

$$\times (\chi_e^{-(2i+1)}(1+\omega^{q\ell}s) + \chi_e^{-(2i+1)}(-\omega^{q\ell})).$$

Proof. The characteristic function of $C_0^{(2,q)}$ is given as

$$g(x) = \frac{1}{2}(\eta(x) + 1), \quad x \in \mathbb{F}_q^*.$$

The size N_s of the set $D_{\ell,H} \cap (C_0^{(2,q)} + s)$ is expressed as

$$N_s = \sum_{x\in\mathbb{F}_q\setminus\{s\}} f(1+\omega^\ell x)g(x-s).$$

By the definitions of $g(x)$ and $f(x)$, we have

$$(18) \qquad N_s = \frac{1}{2e} \sum_{x\in\mathbb{F}_q\setminus\{s\}} (\eta(x-s)+1)\left(e/2 + \sum_{i=0}^{e/2-1} A_{2i+1}\chi_e^{2i+1}(1+\omega^\ell x)\right).$$

Let $N_{s,1}^{(i)} = \sum_{x\in\mathbb{F}_q\setminus\{s\}} \chi_e^i(1+\omega^\ell x)$ and $N_{s,2}^{(i)} = \sum_{x\in\mathbb{F}_q\setminus\{s\}} \chi_e^i(1+\omega^\ell x)\eta(x-s)$. Then, continuing from (18),

$$N_s = \frac{q-1}{4} + \frac{1}{2e} \sum_{i=0}^{e/2-1} A_{2i+1}(N_{s,1}^{(2i+1)} + N_{s,2}^{(2i+1)}).$$

By Lemmas 3.1 and 3.2, we have for odd i

$$N_{s,1}^{(i)} + N_{s,2}^{(i)}$$
$$= \frac{G_{q^2}(\chi_e^i)G_q(\eta)}{q}\chi_e^i(\omega^{\ell q}-\omega^\ell)(\chi_e^{-i}(1+\omega^{q\ell}s)+\chi_e^{-i}(-\omega^{q\ell})) - (\chi_e^i(1+\omega^\ell s)+\chi_e^i(\omega^\ell)).$$

Then, the assertion of the proposition follows. $\square$

The following is another representation for the sizes of $D_{\ell,H} \cap (C_0^{(2,q)} + s)$, $s \in \mathbb{F}_q$.

PROPOSITION 3.6. *The size N_s of $D_{\ell,H} \cap (C_0^{(2,q)} + s)$ is given by*

$$N_s = \frac{G_q(\eta)}{2q}\left(1 + \sum_{i\in H} \psi_{\mathbb{F}_{q^2}}((\omega^{\ell q}-\omega^\ell)^{-1}(1+\omega^{q\ell}s)C_i^{(e,q^2)})\right.$$

$$\left.+ \sum_{i\in H} \psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q}-\omega^\ell)^{-1}\omega^{q\ell}C_i^{(e,q^2)})\right) + \frac{q-1}{4} + \frac{1-\xi_s-\xi_\ell}{2},$$

where $\xi_s = 1$ if $1+\omega^\ell s \in \bigcup_{j\in H} C_j^{(e,q^2)}$ and 0 otherwise, and $\xi_\ell = 1$ if $\omega^\ell \in \bigcup_{j\in H} C_j^{(e,q^2)}$ and 0 otherwise.

Proof. By the orthogonality of characters, we have

$$\frac{1}{e}\sum_{i=0}^{e-1} A_i G_{q^2}(\chi_e^i)\chi_e^i(\omega^{\ell q} - \omega^\ell)\chi_e^{-i}(1 + \omega^{q\ell}s) = \sum_{i\in H}\psi_{\mathbb{F}_{q^2}}((\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s)C_i^{(e,q^2)})$$

and

$$\frac{1}{e}\sum_{i=0}^{e-1} A_i G_{q^2}(\chi_e^i)\chi_e^i(\omega^{\ell q} - \omega^\ell)\chi_e^{-i}(-\omega^{q\ell}) = \sum_{i\in H}\psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q} - \omega^\ell)^{-1}\omega^{q\ell}C_i^{(e,q^2)}).$$

Furthermore, we note that

$$\frac{1}{2e}\sum_{i=0}^{e/2-1} A_{2i+1}(\chi_e^i(1 + \omega^\ell s) + \chi_e^i(\omega^\ell)) = \frac{-1 + \xi_s + \xi_\ell}{2}.$$

Then, by Proposition 3.5, the assertion of the proposition follows. $\qquad\square$

Similar to Proposition 3.4, the proposition above implies that the sizes of $D_{\ell,H} \cap (C_0^{(2,q)} + s)$, $s \in \mathbb{F}_q$, can be expressed in terms of character values of $\bigcup_{i\in H} C_i^{(e,q^2)}$.

4. Construction of biregular Hadamard matrices with maximum excess: the case where $(2m+1)^2 + 2$ is a prime power

In this section, we will prove Theorem 1.2. In particular, in Subsection 4.1, we give a construction of biregular Hadamard matrices of order $n = (2m+1)^2 + 3$ under the assumption of the existence of four-intersection sets. In Subsection 4.2, we construct four-intersection sets with prescribed intersection numbers from the finite field of order $q = (2m+1)^2 + 2$.

4.1. Construction of biregular Hadamard matrices from quadratic residues of $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$. Let $q \equiv 3 \pmod 4$ be a prime power. Let $P = \mathbb{F}_q$ and

$$(19) \qquad \mathcal{B} = \{\{x + a : x \in C_0^{(2,q)} \cup \{0\}\} : a \in \mathbb{F}_q\}.$$

Then, $(P, \mathcal{B})$ is a symmetric 2-design, the so-called *Paley design*. Let M be a $q \times q$ $(1,-1)$-matrix whose rows and columns are labeled by the elements of $\mathbb{F}_q$ and entries are defined by

$$M_{i,j} = \begin{cases} 1, & \text{if } j - i \in C_0^{(2,q)} \cup \{0\}, \\ -1, & \text{if } j - i \in \mathbb{F}_q \smallsetminus (C_0^{(2,q)} \cup \{0\}). \end{cases}$$

Define

$$(20) \qquad H = \begin{pmatrix} -1 & \mathbf{1}_q^\top \\ \mathbf{1}_q & M \end{pmatrix}.$$

Then, H forms a Hadamard matrix of order $n = q + 1$. We now transform H to a biregular Hadamard matrix with maximum excess by negating some rows and columns of H.

Proposition 4.1. *Let $q = (2m+1)^2 + 2$ be a prime power and $(P, \mathcal{B})$ be the block design defined in (19). Assume that there is a four-intersection set with parameters $(2m^2 + m + 2; \{m^2 + 1, m^2 + 2, m^2 + m + 1, m^2 + m + 2\})$ for $(P, \mathcal{B})$. Then, there exists a biregular Hadamard matrix H' of order $n = (2m+1)^2 + 3$ such that $H'\mathbf{1}_n$ has entries in $\{2m - 2, 2m + 2\}$.*

Proof. Let D be the assumed four-intersection set and H be the Hadamard matrix defined in (20). Define

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (m^2 + 1, m^2 + 2, m^2 + m + 1, m^2 + m + 2).$$

Let $\mathbf{x}$ be the support vector of D in P. Furthermore, let A (resp. $A^\perp$) be the $q \times q$-diagonal matrix, whose entries are defined by $A_{i,i} = -1$ if $i \in D$ and 1 otherwise (resp. $A_{i,i}^\perp = -1$ if $i \in D_{\alpha_3}^\perp \cup D_{\alpha_4}^\perp$ and 1 otherwise). Define

$$B = \begin{pmatrix} 1 & \mathbf{0}_q^\top \\ \mathbf{0}_q & A \end{pmatrix}, \quad B^\perp = \begin{pmatrix} 1 & \mathbf{0}_q^\top \\ \mathbf{0}_q & A^\perp \end{pmatrix},$$

where $\mathbf{0}_q$ is the all-zero vector of length q. Then, $H' = B^\perp H B$ is the desired Hadamard matrix.

We now show that $B^\perp H B \mathbf{1}_{q+1}$ has entries in $\{2m-2, 2m+2\}$. By the definitions of B, $B^\perp$ and H, we have

$$B^\perp H B \mathbf{1}_{q+1} = \begin{pmatrix} 1 & \mathbf{0}_q^\top \\ \mathbf{0}_q & A^\perp \end{pmatrix} \begin{pmatrix} -1 & \mathbf{1}_q^\top \\ \mathbf{1}_q & M \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0}_q^\top \\ \mathbf{0}_q & A \end{pmatrix} \begin{pmatrix} 1 \\ \mathbf{1}_q \end{pmatrix}$$

$$= \begin{pmatrix} -1 + \mathbf{1}_q^\top A \mathbf{1}_q \\ A^\perp (\mathbf{1}_q + M A \mathbf{1}_q) \end{pmatrix}.$$

Since $|D| = 2m^2 + m + 2$, we have $-1 + \mathbf{1}_q^\top A \mathbf{1}_q = 2m - 2$. Furthermore, since D is a four-intersection set with parameters $(2m^2 + m + 2; \{m^2 + 1, m^2 + 2, m^2 + m + 1, m^2 + m + 2\})$ for $(P, \mathcal{B})$, we have

$$\left(\frac{1}{2}(M + J_q) \mathbf{x} \right)_i = \begin{cases} m^2 + 1, & \text{if } i \in D_{\alpha_1}^\perp, \\ m^2 + 2, & \text{if } i \in D_{\alpha_2}^\perp, \\ m^2 + m + 1, & \text{if } i \in D_{\alpha_3}^\perp, \\ m^2 + m + 2, & \text{if } i \in D_{\alpha_4}^\perp, \end{cases}$$

where $D_{\alpha_i}^\perp$ is defined in (4). Hence,

$$A^\perp (\mathbf{1}_q + M A \mathbf{1}_q)_i = A^\perp (\mathbf{1}_q + M \mathbf{1}_q - 2M\mathbf{x})_i = \begin{cases} 2m + 2, & \text{if } i \in D_{\alpha_1}^\perp \cup D_{\alpha_4}^\perp, \\ 2m - 2, & \text{if } i \in D_{\alpha_2}^\perp \cup D_{\alpha_3}^\perp. \end{cases}$$

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

4.2. Construction of four-intersection sets satisfying the condition of Proposition 4.1. Let $q = (2m+1)^2 + 2$ be a prime power. We will use the notations in Section 3 with $e = 8$. Let χ_8 be a multiplicative character of order 8 of $\mathbb{F}_{q^2}$ and η be the quadratic character of $\mathbb{F}_q$. Note that the restriction of χ_8 to $\mathbb{F}_q$ is of order 2, i.e., $\chi_{8|\mathbb{F}_q} = \eta$. Assume that $\chi_8(\omega) = \zeta_8 = \sqrt{2}(1 + \zeta_4)/2$. By Theorem 2.3, there are $\epsilon, \delta \in \{-1, 1\}$ such that $G_{q^2}(\chi_8) = G_q(\eta)(\epsilon(2m+1) + \delta\sqrt{-2})$.

Let ℓ be an integer not divisible by $q + 1$. For any fixed $h' \in \{0, 1, 2, 3\}$, let $h = 2h' + (1 - \epsilon\delta)/2 \in \{0, 1, \ldots, 7\}$. Furthermore, fix ℓ satisfying the following conditions:

$$(21) \qquad \chi_8(\omega^\ell) = \zeta_8^{2 - 5\epsilon\delta - 6h'}, \quad \chi_8(\omega^{\ell q} - \omega^\ell) = -\zeta_4^\delta.$$

In the following remark, we show that such a pair $(h', \ell) \in \{0, 1, 2, 3\} \times \{0, 1, \ldots, q^2 - 2\}$ exists.

REMARK 4.2. In this remark, we see that the set

$$\left\{ (h', \ell) : (q + 1) \nmid \ell, \chi_8(\omega^\ell) = \zeta_8^{2 - 5\epsilon\delta - 6h'}, \chi_8(\omega^{\ell q} - \omega^\ell) = -\zeta_4^\delta \right\}$$

is nonempty. Note that $\omega^{\ell q} - \omega^{\ell} = -\omega^{-\frac{q+1}{2}} \operatorname{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}})$ is a square but not a fourth power in $\mathbb{F}_{q^2}$. Hence, the condition that $\chi_8(\omega^{\ell q} - \omega^{\ell}) = -\zeta_4^{\delta}$ is equivalent to that

$$\eta(\operatorname{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}})) = \zeta_4^{\delta + (m^2 + m + 1)}.$$

On the other hand, the condition $\chi_8(\omega^{\ell}) = \zeta_8^{2-5\epsilon\delta - 6h'}$ for $h' \in \{0, 1, 2, 3\}$ is equivalent to that $\omega^{\ell} \in C_1^{(2,q^2)}$. This is valid whenever ℓ is odd. Then, the condition $(q + 1) \nmid \ell$ is satisfied. Therefore, it is enough to see that each of the sets

$$T_i = \left\{ \omega^{\ell} \in C_1^{(2,q^2)} \ : \ \operatorname{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}}) \in C_i^{(2,q)} \right\}, \quad i = 0, 1,$$

is nonempty. In [19, Remark 2], it was shown that

$$(22) \qquad |T_i| = -\frac{q-1}{2q} \sum_{x \in C_1^{(2,q^2)}} \psi_{\mathbb{F}_{q^2}}(x\omega^{\frac{q+1}{2}}) + \frac{(q-1)(q^2-1)}{4q}.$$

By (7) and Theorem 2.2, continuing from (22), we have

$$|T_i| = -\frac{q-1}{2q} \left(\frac{-1 - G_{q^2}(\eta)}{2} \right) + \frac{(q-1)(q^2-1)}{4q} = \frac{q^2-1}{4} > 0.$$

Hence, each T_i is nonempty.

THEOREM 4.3. *Let $q = (2m+1)^2 + 2$ be a prime power, and let h and ℓ be integers defined as above. Write $H = \{h + i \pmod 8 : i = 0, 1, 2, 3\}$ and define*

$$D_{\ell, H} = \left\{ x \in \mathbb{F}_q \ : \ 1 + x\omega^{\ell} \in \bigcup_{i \in H} C_i^{(8,q^2)} \right\}.$$

Then, it holds that $|D_{\ell, H}| = 2m^2 + m + 2$ and

$$\{|D_{\ell, H} \cap ((C_0^{(2,q)} \cup \{0\}) + s)| : s \in \mathbb{F}_q\} = \{m^2 + 1, m^2 + 2, m^2 + m + 1, m^2 + m + 2\}.$$

Proof. We first evaluate the size of $D_{\ell, H}$. Let $A_i = \sum_{j=0}^{3} \zeta_8^{-(h+j)i}$. By Proposition 3.3, we have

$$(23) \qquad |D_{\ell, H}| = \frac{q}{2} - \frac{G_q(\eta)}{8q} \sum_{i=0}^{3} A_{2i+1} G_{q^2}(\chi_8^{2i+1}) \chi_8^{-(2i+1)}(\omega^{q\ell}) \chi_8^{2i+1}(\omega^{\ell q} - \omega^{\ell}).$$

Here, $G_{q^2}(\chi_8) G_q(\eta) = -q(\epsilon(2m+1) + \delta\sqrt{-2})$ by Theorem 2.3. Substituting $G_{q^2}(\chi_8) G_q(\eta) = -q(\epsilon(2m+1) + \delta\sqrt{-2})$, $\chi_8(\omega^{\ell}) = \zeta_8^{2-5\epsilon\delta - 6h'}$ and $\chi_8(\omega^{\ell q} - \omega^{\ell}) = -\zeta_4^{\delta}$ into (23), it is direct to see that $|D_{\ell, h}| = 2m^2 + m + 2$.

Next, we evaluate the size N_s of the set $D_{\ell, H} \cap ((C_0^{(2,q)} \cup \{0\}) + s)$. By Proposition 3.5,

$$(24) \quad N_s = \frac{1}{8} \left(4 + \sum_{i=1,3,5,7} A_i \chi_8^i(1 + \omega^{\ell} s) \right) + \frac{q-1}{4}$$

$$- \frac{1}{16} \sum_{i=0}^{3} A_{2i+1}(\chi_8^{2i+1}(1 + \omega^{\ell} s) + \chi_8^{2i+1}(\omega^{\ell}))$$

$$+ \frac{G_q(\eta)}{16q} \sum_{i=0}^{3} A_{2i+1} G_{q^2}(\chi_8^{2i+1}) \chi_8^{2i+1}(\omega^{\ell q} - \omega^{\ell})$$

$$\times (\chi_8^{-(2i+1)}(1 + \omega^{q\ell} s) - \chi_8^{-(2i+1)}(\omega^{q\ell})).$$

Substituting $G_{q^2}(\chi_8)G_q(\eta) = -q(\epsilon(2m+1) + \delta\sqrt{-2})$, $\chi_8(\omega^\ell) = \zeta_8^{2-5\epsilon\delta-6h'}$, and $\chi_8(\omega^{\ell q} - \omega^\ell) = -\zeta_4^\delta$ into (24), we can evaluate N_s as

$$(25) \quad N_s = \begin{cases} m^2+m+2, & \text{if } \epsilon\delta = 1 \text{ and } \chi_8(1+\omega^\ell s) \in \{\zeta_8^{2h'}, \zeta_8^{2h'+3}, \zeta_8^{2h'+6}\}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_8(1+\omega^\ell s) \in \{\zeta_8^{2h'+1}, \zeta_8^{2h'+4}, \zeta_8^{2h'+6}\}, \\ m^2+2, & \text{if } \epsilon\delta = 1 \text{ and } \chi_8(1+\omega^\ell s) = \zeta_8^{2h'+1}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_8(1+\omega^\ell s) = \zeta_8^{2h'+3}, \\ m^2+1, & \text{if } \epsilon\delta = 1 \text{ and } \chi_8(1+\omega^\ell s) \in \{\zeta_8^{2h'+2}, \zeta_8^{2h'+4}, \zeta_8^{2h'+7}\}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_8(1+\omega^\ell s) \in \{\zeta_8^{2h'}, \zeta_8^{2h'+2}, \zeta_8^{2h'+5}\}, \\ m^2+m+1, & \text{if } \epsilon\delta = 1 \text{ and } \chi_8(1+\omega^\ell s) = \zeta_8^{2h'+5}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_8(1+\omega^\ell s) = \zeta_8^{2h'+7}. \end{cases}$$

Thus, $N_s \in \{m^2+1, m^2+2, m^2+m+1, m^2+m+2\}$. $\qquad\square$

The theorem above implies that $D_{\ell,H}$ is a four-intersection set satisfying the condition of Proposition 4.1. Then, our main Theorem 1.2 follows.

5. Construction of biregular Hadamard matrices with maximum excess: the case where $m^2 + (m+1)^2$ is a prime power

In this section, we will prove Theorem 1.3. In particular, in Subsection 5.1, we give a construction of biregular Hadamard matrices of order $n = (2m+1)^2 + 3$ under the assumption of the existence of four-intersection sets. In Subsection 5.2, we construct four-intersection sets with prescribed intersection numbers from the finite field of order $q = m^2 + (m+1)^2$.

5.1. Construction of biregular Hadamard matrices from quadratic residues of $\mathbb{F}_q$ with $q \equiv 1 \pmod 4$. Let $q \equiv 1 \pmod 4$ be a prime power. Let M be a $q \times q$ $(0,1,-1)$-matrix whose rows and columns are labeled by the elements of $\mathbb{F}_q$ and entries are defined by

$$M_{i,j} = \begin{cases} 0, & \text{if } j - i = 0, \\ 1, & \text{if } j - i \in C_0^{(2,q)}, \\ -1, & \text{if } j - i \in \mathbb{F}_q \smallsetminus (C_0^{(2,q)} \cup \{0\}). \end{cases}$$

Define $M_1 = M + I_q$, $M_2 = M - I_q$, and $M_3 = -M_1$. Furthermore, define

$$(26) \quad H = \begin{pmatrix} 1 & -1 & \mathbf{1}_q^\top & \mathbf{1}_q^\top \\ -1 & -1 & \mathbf{1}_q^\top & -\mathbf{1}_q^\top \\ \mathbf{1}_q & \mathbf{1}_q & M_1 & M_2 \\ \mathbf{1}_q & -\mathbf{1}_q & M_2 & M_3 \end{pmatrix}.$$

Then, H forms a symmetric Hadamard matrix of order $n = 2q + 2$. We transform H to a biregular Hadamard matrix with maximum excess by negating some rows and columns.

Define

$$N_1 = \begin{pmatrix} M_1 \\ M_2 \end{pmatrix} \quad \text{and} \quad N_2 = \begin{pmatrix} M_2 \\ M_3 \end{pmatrix}.$$

We label the rows of the upper half submatrices (resp. the lower half submatrices) of N_1 and N_2 by the elements of $\{0\} \times \mathbb{F}_q$ (resp. $\{1\} \times \mathbb{F}_q$) so that $(0,j)$th rows (resp. $(1,j)$th rows) of N_1 and N_2 are respectively corresponding to jth rows of M_1 and M_2 (resp. M_2 and M_3). Furthermore, we can, and do, label the columns of $N = \begin{pmatrix} N_1 & N_2 \end{pmatrix}$ in the same way with the rows of N since N is symmetric. Define $P = \{0,1\} \times \mathbb{F}_q$,

and let $(P, \mathcal{B}_i)$, $i = 1, 2$, be the block designs with incidence matrices $(N_i + J_{2q,q})/2$, $i = 1, 2$, respectively.

PROPOSITION 5.1. *Let $q = m^2 + (m+1)^2$ be a prime power and $(P, \mathcal{B}_i)$, $i = 1, 2$, be the block designs defined above. Assume that there is a $2m^2 + m$-subset D of P such that $|D \cap (\{0\} \times \mathbb{F}_q)| = m^2$ and $|D \cap (\{1\} \times \mathbb{F}_q)| = m^2 + m$, which is a four-intersection set with parameters $(2m^2 + m; \{m^2, m^2 + 1, m^2 + m, m^2 + m + 1\})$ for $(P, \mathcal{B}_1)$ and with parameters $(2m^2 + m; \{m^2 - 1, m^2, m^2 + m - 1, m^2 + m\})$ for $(P, \mathcal{B}_2)$. Then, there exists a biregular Hadamard matrix H' of order $n = (2m + 1)^2 + 3$ such that $H' \mathbf{1}_n$ has entries in $\{2m - 2, 2m + 2\}$.*

Proof. Let H be the Hadamard matrix defined in (26). Define
$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (m^2, m^2 + 1, m^2 + m, m^2 + m + 1)$$
and
$$(\beta_1, \beta_2, \beta_3, \beta_4) = (m^2 - 1, m^2, m^2 + m - 1, m^2 + m).$$

Let $\mathbf{x}$ (resp. $\mathbf{y}$) be the support vector of $D \cap (\{0\} \times \mathbb{F}_q)$ in $\{0\} \times \mathbb{F}_q$ (resp. $D \cap (\{1\} \times \mathbb{F}_q)$ in $\{1\} \times \mathbb{F}_q$). Furthermore, let A_1 (resp. $A_1^\perp$) be the $q \times q$-diagonal matrix, whose rows and columns are labeled by the elements of $\{0\} \times \mathbb{F}_q$ and diagonal entries are defined by $(A_1)_{i,i} = -1$ if $i \in D \cap (\{0\} \times \mathbb{F}_q)$ and 1 otherwise (resp. $(A_1^\perp)_{i,i} = -1$ if $i \in D_{\alpha_3}^\perp \cup D_{\alpha_4}^\perp$ and 1 otherwise). Similarly, let A_2 (resp. $A_2^\perp$) be the $q \times q$-diagonal matrix, whose rows and columns are labeled by the elements of $\{1\} \times \mathbb{F}_q$ and diagonal entries are defined by $(A_2)_{i,i} = -1$ if $D \cap (\{1\} \times \mathbb{F}_q)$ and 1 otherwise (resp. $(A_2^\perp)_{i,i} = -1$ if $D_{\beta_3}^\perp \cup D_{\beta_4}^\perp$ and 1 otherwise). Define
$$B = \begin{pmatrix} 1 & 0 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ 0 & 1 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ \mathbf{0}_q & \mathbf{0}_q & A_1 & O_q \\ \mathbf{0}_q & \mathbf{0}_q & O_q & A_2 \end{pmatrix}, \quad B^\perp = \begin{pmatrix} 1 & 0 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ 0 & 1 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ \mathbf{0}_q & \mathbf{0}_q & A_1^\perp & O_q \\ \mathbf{0}_q & \mathbf{0}_q & O_q & A_2^\perp \end{pmatrix},$$
where O_q is the $q \times q$ all-zero matrix. Then, $H' = B^\perp H B$ is the desired Hadamard matrix.

We show that $B^\perp H B \mathbf{1}_{2(q+1)}$ has entries in $\{2m - 2, 2m + 2\}$. By the definitions of B, $B^\perp$ and H, we have
$$B^\perp H B \mathbf{1}_{2(q+1)} = \begin{pmatrix} 1 & 0 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ 0 & 1 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ \mathbf{0}_q & \mathbf{0}_q & A_1^\perp & O_q \\ \mathbf{0}_q & \mathbf{0}_q & O_q & A_2^\perp \end{pmatrix} \begin{pmatrix} 1 & -1 & \mathbf{1}_q^\top & \mathbf{1}_q^\top \\ -1 & -1 & \mathbf{1}_q^\top & -\mathbf{1}_q^\top \\ \mathbf{1}_q & \mathbf{1}_q & M_1 & M_2 \\ \mathbf{1}_q & -\mathbf{1}_q & M_2 & M_3 \end{pmatrix} \begin{pmatrix} 1 & 0 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ 0 & 1 & \mathbf{0}_q^\top & \mathbf{0}_q^\top \\ \mathbf{0}_q & \mathbf{0}_q & A_1 & O_q \\ \mathbf{0}_q & \mathbf{0}_q & O_q & A_2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ \mathbf{1}_q \\ \mathbf{1}_q \end{pmatrix}$$
$$= \begin{pmatrix} \mathbf{1}_q^\top A_1 \mathbf{1}_q + \mathbf{1}_q^\top A_2 \mathbf{1}_q \\ -2 + \mathbf{1}_q^\top A_1 \mathbf{1}_q - \mathbf{1}_q^\top A_2 \mathbf{1}_q \\ A_1^\perp (2\mathbf{1}_q + M_1 A_1 \mathbf{1}_q + M_2 A_2 \mathbf{1}_q) \\ A_2^\perp (M_2 A_1 \mathbf{1}_q + M_3 A_2 \mathbf{1}_q) \end{pmatrix}.$$

Since $|D \cap (\{0\} \times \mathbb{F}_q)| = m^2$ and $|D \cap (\{1\} \times \mathbb{F}_q)| = m^2 + m$, we have $\mathbf{1}_q^\top A_1 \mathbf{1}_q + \mathbf{1}_q^\top A_2 \mathbf{1}_q = 2m + 2$ and $-2 + \mathbf{1}_q^\top A_1 \mathbf{1}_q - \mathbf{1}_q^\top A_2 \mathbf{1}_q = 2m - 2$. Furthermore, since D is a four-intersection set with parameters $(2m^2 + m; \{m^2, m^2 + 1, m^2 + m, m^2 + m + 1\})$ for $(P, \mathcal{B}_1)$ and with parameters $(2m^2 + m; \{m^2 - 1, m^2, m^2 + m - 1, m^2 + m\})$ for $(P, \mathcal{B}_2)$, we have
$$\left(\frac{1}{2}((M_1 + J_q)\mathbf{x} + (M_2 + J_q)\mathbf{y}) \right)_i = \begin{cases} m^2, & \text{if } i \in D_{\alpha_1}^\perp, \\ m^2 + 1, & \text{if } i \in D_{\alpha_2}^\perp, \\ m^2 + m, & \text{if } i \in D_{\alpha_3}^\perp, \\ m^2 + m + 1, & \text{if } i \in D_{\alpha_4}^\perp, \end{cases}$$

and

$$\left(\frac{1}{2}((M_2 + J_q)\mathbf{x} + (M_3 + J_q)\mathbf{y}) \right)_i = \begin{cases} m^2 - 1, & \text{if } i \in D_{\beta_1}^\perp, \\ m^2, & \text{if } i \in D_{\beta_2}^\perp, \\ m^2 + m - 1, & \text{if } i \in D_{\beta_3}^\perp, \\ m^2 + m, & \text{if } i \in D_{\beta_4}^\perp. \end{cases}$$

Hence,

$$\left(A_1^\perp (2\mathbf{1}_q + M_1 A_1 \mathbf{1}_q + M_2 A_2 \mathbf{1}_q) \right)_i = \left(A_1^\perp (2\mathbf{1}_q + M_1 \mathbf{1}_q + M_2 \mathbf{1}_q - 2M_1 \mathbf{x} - 2M_2 \mathbf{y}) \right)_i$$
$$= \begin{cases} 2m + 2, & \text{if } i \in D_{\alpha_1}^\perp \cup D_{\alpha_4}^\perp, \\ 2m - 2, & \text{if } i \in D_{\alpha_2}^\perp \cup D_{\alpha_3}^\perp, \end{cases}$$

and

$$\left(A_2^\perp (M_2 A_1 \mathbf{1}_q + M_3 A_2 \mathbf{1}_q) \right)_i = \left(A_2^\perp (M_2 \mathbf{1}_q + M_3 \mathbf{1}_q - 2M_2 \mathbf{x} - 2M_3 \mathbf{y}) \right)_i$$
$$= \begin{cases} 2m + 2, & \text{if } i \in D_{\beta_1}^\perp \cup D_{\beta_4}^\perp, \\ 2m - 2, & \text{if } i \in D_{\beta_2}^\perp \cup D_{\beta_3}^\perp. \end{cases}$$

This completes the proof of the proposition. □

We have the following proposition similar to Proposition 5.1.

PROPOSITION 5.2. *Let $q = m^2 + (m+1)^2$ be a prime power and $(P, \mathcal{B}_i)$, $i = 1, 2$, be the block designs defined as in Proposition* 5.1. *Assume that there is a $2m^2 + m + 1$-subset D of P such that $|D \cap (\{0\} \times \mathbb{F}_q)| = m^2$ and $|D \cap (\{1\} \times \mathbb{F}_q)| = m^2 + m + 1$, which is a four-intersection set with parameters $(2m^2 + m + 1; \{m^2, m^2 + 1, m^2 + m + 1, m^2 + m + 2\})$ for $(P, \mathcal{B}_1)$ and with parameters $(2m^2 + m + 1; \{m^2 - 1, m^2, m^2 + m, m^2 + m + 1\})$ for $(P, \mathcal{B}_2)$. Then, there exists a biregular Hadamard matrix H' of order $n = (2m+1)^2 + 3$ such that $H'\mathbf{1}_n$ has entries in $\{2m, 2m + 4\}$.*

We omit the proof of the proposition above since the proof is similar to that of Proposition 5.1.

5.2. CONSTRUCTION OF FOUR-INTERSECTION SETS SATISFYING THE CONDITIONS OF PROPOSITIONS 5.1 AND 5.2. Let $q = m^2 + (m + 1)^2$ be a prime power. We will use the notations in Section 3 with $e = 4$. Let χ_4 be a multiplicative character of order 4 of $\mathbb{F}_{q^2}$, and η the quadratic character of $\mathbb{F}_q$. It is clear that $\chi_{4|\mathbb{F}_q} = \eta$. We first give the following lemma.

LEMMA 5.3. *With notations as above, there are $\epsilon, \delta \in \{1, -1\}$ such that*

$$G_q(\eta) G_{q^2}(\chi_4)/q = \epsilon m + \delta(m + 1)\zeta_4 \text{ or } \epsilon(m + 1) + \delta m \zeta_4$$

depending on whether m is odd or even.

Proof. Let χ_4' be the multiplicative character of order 4 of $\mathbb{F}_q$ such that $\chi_4'(\omega^{q+1}) = \chi_4(\omega)$. Then, by Theorem 2.4, we have $G_{q^2}(\chi_4) = -G_q(\chi_4')^2$. By (8), we have

$$G_q(\eta) G_{q^2}(\chi_4) = -G_q(\eta) G_q(\chi_4')^2 = -\chi_4'(-1)q \frac{G_q(\eta) G_q(\chi_4')}{G_q(\chi_4'^3)} = -\chi_4'(-1)q J_q(\eta, \chi_4').$$

Finally, by Theorem 2.5, there are $\epsilon, \delta \in \{1, -1\}$ such that $-\chi_4'(-1) J_q(\eta, \chi_4') = \epsilon m + \delta(m + 1)\zeta_4$ or $-\chi_4'(-1) J_q(\eta, \chi_4') = \epsilon(m + 1) + \delta m \zeta_4$ depending on whether m is odd or even. This completes the proof of the lemma. □

Let ℓ be an integer not divisible by $q + 1$. Fix ℓ and $h \in \{0, 1, 2, 3\}$ satisfying the following conditions:

$$(27) \qquad \chi_4(\omega^\ell) = \zeta_4^{3+h}, \quad \chi_4(\omega^{\ell q} - \omega^\ell) = \zeta_4^{\delta(1+2h)}.$$

In the following remark, we show that such a pair $(h, \ell) \in \{0, 1, 2, 3\} \times \{0, 1, \ldots, q^2 - 2\}$ exists.

REMARK 5.4. In this remark, we see that the set

$$\left\{ (h, \ell) : (q + 1) \nmid \ell, \chi_4(\omega^\ell) = \zeta_4^{3+h}, \chi_4(\omega^{\ell q} - \omega^\ell) = \zeta_4^{\delta(1+2h)} \right\}$$

is nonempty. We assume that h is even. This is valid whenever ℓ is odd since $\chi_4(\omega^\ell) = \zeta_4^{3+h}$. Then, the condition $(q + 1) \nmid \ell$ is satisfied. Since $\omega^{\ell q} - \omega^\ell = -\omega^{-\frac{q+1}{2}} \operatorname{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}})$ is a nonsquare in $\mathbb{F}_{q^2}$, the condition $\chi_4(\omega^{\ell q} - \omega^\ell) = \zeta_4^{\delta(1+2h)}$ is reformulated as

$$\eta(-\operatorname{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}})) = \zeta_4^{m^2+m+1+\delta}.$$

Therefore, it is enough to see that each of the sets

$$T_i = \left\{ \omega^\ell \in C_1^{(2,q^2)} \ : \ \operatorname{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}}) \in C_i^{(2,q)} \right\}, \quad i = 0, 1,$$

is nonempty. Similar to Remark 4.2, by Theorem 2.2, we have

$$|T_i| = -\frac{q-1}{2q} \sum_{x \in C_1^{(2,q^2)}} \psi_{\mathbb{F}_{q^2}}(x\omega^{\frac{q+1}{2}}) + \frac{(q-1)(q^2-1)}{4q}$$

$$= -\frac{q-1}{2q} \left(\frac{-1 + G_{q^2}(\eta)}{2} \right) + \frac{(q-1)(q^2-1)}{4q} = \frac{q^2-1}{4} > 0.$$

Hence, each T_i is nonempty.

We first treat the case where m is odd.

THEOREM 5.5. Let $q = m^2 + (m+1)^2$ be a prime power with m odd. Let h and ℓ be integers defined as above. Define $(H_0, H_1) = (\{h, h+1\}, \{h+1, h+2\})$ or $(H_0, H_1) = (\{h+1, h+2\}, \{h, h+1\})$ depending on whether $\epsilon\delta = 1$ or -1. Furthermore, define

$$D_{\ell, H_d} = \left\{ x \in \mathbb{F}_q : 1 + x\omega^\ell \in \bigcup_{j \in H_d} C_j^{(4,q^2)} \right\}, \quad d = 0, 1.$$

Then, it holds that $|D_{\ell, H_0}| = m^2$ and $|D_{\ell, H_1}| = m^2 + m$. Furthermore,

$$\{|D_{\ell, H_0} \cap ((C_0^{(2,q)} \cup \{0\}) + s)| + |D_{\ell, H_1} \cap (C_0^{(2,q)} + s)| : s \in \mathbb{F}_q\} = \{m^2, m^2 + m + 1\}$$

and

$$\{|D_{\ell, H_0} \cap (C_0^{(2,q)} + s)| + |D_{\ell, H_1} \cap ((\mathbb{F}_q^* \smallsetminus C_0^{(2,q)}) + s)| : s \in \mathbb{F}_q\}$$
$$= \{m^2 - 1, m^2, m^2 + m - 1, m^2 + m\}.$$

Proof. We first evaluate the sizes of D_{ℓ, H_d}, $d = 0, 1$. Let $A_{i,d} = \sum_{j \in H_d} \zeta_e^{-ji}$. By Proposition 3.3 and Lemma 5.3, we have

$$(28) \quad |D_{\ell, H_d}| = \frac{q}{2} + \frac{G_q(\eta)}{4q} \sum_{i=0,1} A_{2i+1,d} G_{q^2}(\chi_4^{2i+1}) \chi_4^{-(2i+1)}(\omega^\ell) \chi_4^{2i+1}(\omega^{\ell q} - \omega^\ell)$$

$$= \frac{m^2 + (m+1)^2}{2} + \frac{1}{4} A_{1,d}(\epsilon m + \delta(m+1)\zeta_4) \chi_4^{-1}(\omega^\ell) \chi_4(\omega^{\ell q} - \omega^\ell)$$

$$+ \frac{1}{4} A_{3,d}(\epsilon m - \delta(m+1)\zeta_4) \chi_4(\omega^\ell) \chi_4^{-1}(\omega^{\ell q} - \omega^\ell).$$

Substituting $\chi_4(\omega^\ell) = \zeta_4^{3+h}$ and $\chi_4(\omega^{\ell q} - \omega^\ell) = \zeta_4^{\delta(1+2h)}$ into (28), it is direct to see that $(|D_{\ell,H_0}|, |D_{\ell,H_1}|) = (m^2, m^2 + m)$.

Next, we evaluate the following:

$$M_{1,s} = |D_{\ell,H_0} \cap ((C_0^{(2,q)} \cup \{0\}) + s)| + |D_{\ell,H_1} \cap (C_0^{(2,q)} + s)|,$$

$$M_{2,s} = |D_{\ell,H_0} \cap (C_0^{(2,q)} + s)| + |D_{\ell,H_1} \cap ((\mathbb{F}_q^* \setminus C_0^{(2,q)}) + s)|.$$

By Proposition 3.5 and Lemma 5.3, we have

$$(29) \qquad M_{1,s} = \frac{q-1}{2} + \frac{1}{8} \sum_{i=1,3} (A_{i,0} + A_{i,1}) N_s^{(i)} + \frac{1}{4} \sum_{i=1,3} A_{i,0} \chi_4^i (1 + \omega^\ell s) + \frac{1}{2}$$

and

$$(30) \qquad M_{2,s} = |D_{\ell,H_1}| + \frac{1}{8} \sum_{i=1,3} (A_{i,0} - A_{i,1}) N_s^{(i)} - \frac{1}{4} \sum_{i=1,3} A_{i,1} \chi_4^i (1 + \omega^\ell s) - \frac{1}{2},$$

where

$$N_s^{(i)} = (\epsilon m + \delta(m+1)\zeta_4^i)\chi_4^i(\omega^{\ell q} - \omega^\ell)(\chi_4^{-i}(1 + \omega^\ell s) + \chi_4^{-i}(\omega^\ell))$$
$$- (\chi_4^i(1 + \omega^\ell s) + \chi_4^i(\omega^\ell)).$$

Substituting $\chi_4(\omega^\ell) = \zeta_4^{3+h}$ and $\chi_4(\omega^{\ell q} - \omega^\ell) = \zeta_4^{\delta(1+2h)}$ into (29) and (30), we can evaluate $M_{1,s}$ and $M_{2,s}$ as

$$M_{1,s} = \begin{cases} m^2 + m + 1, & \text{if } \epsilon\delta = 1 \text{ and } \chi_4(1 + \omega^\ell s) \in \{\zeta_4^h, \zeta_4^{h+1}\}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_4(1 + \omega^\ell s) \in \{\zeta_4^{h+1}, \zeta_4^{h+2}\}, \\ m^2, & \text{if } \epsilon\delta = 1 \text{ and } \chi_4(1 + \omega^\ell s) \in \{\zeta_4^{h+2}, \zeta_4^{h+3}\}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_4(1 + \omega^\ell s) \in \{\zeta_4^h, \zeta_4^{h+3}\}, \end{cases}$$

and

$$M_{2,s} = \begin{cases} m^2 - 1, & \text{if } \epsilon\delta = 1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^h, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^{h+2}, \\ m^2 + m - 1, & \text{if } \epsilon\delta = 1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^{h+1}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^{h+1}, \\ m^2 + m, & \text{if } \epsilon\delta = 1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^{h+2}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^h, \\ m^2, & \text{if } \epsilon\delta = 1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^{h+3}, \\ & \quad \text{or } \epsilon\delta = -1 \text{ and } \chi_4(1 + \omega^\ell s) = \zeta_4^{h+3}. \end{cases}$$

This completes the proof of the theorem. □

The theorem above implies that $(\{0\} \times D_{\ell,H_0}) \cup (\{1\} \times D_{\ell,H_1})$ satisfies the condition of Proposition 5.1. Then, the assertion for the case where m is odd in Theorem 1.3 follows.

We next treat the case where m is even.

THEOREM 5.6. *Let $q = m^2 + (m+1)^2$ be a prime power with m even. Let h and ℓ be integers defined in (27). Define $(H_0, H_1) = (\{h, h+1\}, \{h+1, h+2\})$ or $(H_0, H_1) = (\{h+1, h+2\}, \{h, h+1\})$ depending on whether $\epsilon\delta = 1$ or -1. Furthermore, define*

$$D_{\ell,H_d} = \left\{ x \in \mathbb{F}_q : 1 + x\omega^\ell \in \bigcup_{j \in H_d} C_j^{(4,q^2)} \right\}, \quad d = 0, 1.$$

Then, it holds that $|D_{\ell,H_0}| = m^2$ and $|D_{\ell,H_1}| = m^2 + m + 1$. Furthermore,

$$\{|D_{\ell,H_0} \cap ((C_0^{(2,q)} \cup \{0\}) + s)| + |D_{\ell,H_1} \cap (C_0^{(2,q)} + s)| : s \in \mathbb{F}_q\}$$
$$= \{m^2, m^2 + 1, m^2 + m + 1, m^2 + m + 2\}$$

and

$$\{|D_{\ell,H_0} \cap (C_0^{(2,q)} + s)| + |D_{\ell,H_1} \cap ((\mathbb{F}_q^* \smallsetminus C_0^{(2,q)}) + s)| : s \in \mathbb{F}_q\} = \{m^2, m^2 + m\}.$$

We omit the proof of Theorem 5.6 since the proof is similar to that of Theorem 5.5. This theorem implies that $(\{0\} \times D_{\ell,H_0}) \cup (\{1\} \times D_{\ell,H_1})$ is a set satisfying the condition of Proposition 5.2. Then, the assertion for the case where m is even in Theorem 1.3 follows.

6. Construction of regular Hadamard matrices

In this section, we prove Theorem 1.4. We restate the theorem below.

Theorem 6.1. *Let $q = 2m^2 - 1$ be a prime power with m odd. Let $X_0 = \{0\}$, and assume that there are subsets X_i, $i = 1, 2, 3, 4$, of $\mathbb{F}_{q^2}$ partitioning $\mathbb{F}_{q^2}^*$ satisfying the following conditions:*

(1) $X_1 = \omega^{2m^2} X_3$ *and* $X_2 = \omega^{2m^2} X_4$;

(2) *Each X_i, $i = 1, 2, 3, 4$, is a union of cosets of $C_0^{(4m^2, q^2)}$;*

(3) *$(\mathbb{F}_{q^2}, \{R_i\}_{i=0}^4)$ is a four-class association scheme with Table 1 as its first eigenmatrix. Here, for $i = 0, 1, 2, 3, 4$, $(x, y) \in R_i$ if and only if $x - y \in X_i$. Furthermore, the sets Y_i, $i = 0, 1, 2, 3, 4$, are defined by $Y_0 = \{0\}$, $Y_1 = \omega^{-m^2 \tau} X_1^q$, $Y_2 = \omega^{-m^2 \tau} X_2^q$ $Y_3 = \omega^{-m^2 \tau} X_3^q$, $Y_4 = \omega^{-m^2 \tau} X_4^q$, where $\tau = 1$ or -1 and $X_i^q := \{x^q : x \in X_i\}$, $i = 1, 2, 3, 4$.*

Then, there exists a regular Hadamard matrix of order $n = 4m^2$.

Table 1. The first eigenmatrix of $(\mathbb{F}_{q^2}, \{R_i\}_{i=0}^4)$: $\psi_{\mathbb{F}_{q^2}}(aX_i)$, $a \in \mathbb{F}_{q^2}^*$, take four character values depending on whether $a \in Y_i$, $i = 1, 2, 3, 4$.

	X_0	X_1	X_2
$a \in Y_0$	1	$m(m^2-1)(m-1)$	$m(m^2-1)(m+1)$
$a \in Y_1$	1	$\frac{m^2+m-1}{2} - \frac{m}{2}G_q(\eta)$	$\frac{-m^2-m}{2} - \frac{m+1}{2}G_q(\eta)$
$a \in Y_2$	1	$\frac{-m^2+m}{2} - \frac{m-1}{2}G_q(\eta)$	$\frac{m^2-m-1}{2} + \frac{m}{2}G_q(\eta)$
$a \in Y_3$	1	$\frac{m^2+m-1}{2} + \frac{m}{2}G_q(\eta)$	$\frac{-m^2-m}{2} + \frac{m+1}{2}G_q(\eta)$
$a \in Y_4$	1	$\frac{-m^2+m}{2} + \frac{m-1}{2}G_q(\eta)$	$\frac{m^2-m-1}{2} - \frac{m}{2}G_q(\eta)$

	X_3	X_4
$a \in Y_0$	$m(m^2-1)(m-1)$	$m(m^2-1)(m+1)$
$a \in Y_1$	$\frac{m^2+m-1}{2} + \frac{m}{2}G_q(\eta)$	$\frac{-m^2-m}{2} + \frac{m+1}{2}G_q(\eta)$
$a \in Y_2$	$\frac{-m^2+m}{2} + \frac{m-1}{2}G_q(\eta)$	$\frac{m^2-m-1}{2} - \frac{m}{2}G_q(\eta)$
$a \in Y_3$	$\frac{m^2+m-1}{2} - \frac{m}{2}G_q(\eta)$	$\frac{-m^2-m}{2} - \frac{m+1}{2}G_q(\eta)$
$a \in Y_4$	$\frac{-m^2+m}{2} - \frac{m-1}{2}G_q(\eta)$	$\frac{m^2-m-1}{2} + \frac{m}{2}G_q(\eta)$

Remark 6.2. We remark that $W_1 = X_1 \cup X_3$ (resp. $W_2 = X_2 \cup X_4$) is a union of cosets of $\mathbb{F}_q^*$ and it takes exactly two nontrivial character values $m^2 + m - 1$ and $-m^2 + m$ (resp. $m^2 - m - 1$ and $-m^2 - m$). Equivalently, $(\mathbb{F}_{q^2}, \{R_i'\}_{i=0}^2)$ is a two-class

association scheme, where $R_0' := \{(x, x) \; : \; x \in \mathbb{F}_{q^2}\}$ and R_i', $i = 1, 2$, are defined by $(x, y) \in R_i'$ if and only if $x - y \in W_i$. On the other hand, it is known that any union of cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$ takes exactly two nontrivial character values [6, Theorem 2], and there exist such subsets W_1 and W_2. Then, by Proposition 2.1, $(\mathbb{F}_{q^2}, \{R_i\}_{i=0}^4)$ is a fission scheme of a known two-class association scheme.

In Subsection 6.1, we give a construction of regular Hadamard matrices of order $n = 4m^2$ under the assumption of the existence of two-intersection sets. In Subsection 6.2, we construct two-intersection sets with prescribed intersection numbers from the finite field of order $q = 2m^2 - 1$.

6.1. CONSTRUCTION OF REGULAR HADAMARD MATRICES FROM QUADRATIC RESIDUES OF $\mathbb{F}_q$ WITH $q \equiv 1 \pmod 4$. We first modify the construction given in Proposition 5.1. Let M_1, M_2, M_3 be matrices defined as in Subsection 5.1. Define

$$(31) \qquad H = \begin{pmatrix} 1 & 1 & \mathbf{1}_q^\top & \mathbf{1}_q^\top \\ 1 & -1 & -\mathbf{1}_q^\top & \mathbf{1}_q^\top \\ \mathbf{1}_q & -\mathbf{1}_q & M_1 & M_2 \\ \mathbf{1}_q & \mathbf{1}_q & M_2 & M_3 \end{pmatrix},$$

which is the matrix obtained by negating the second row and the second column of the matrix defined in (26). Consider the symmetric submatrix

$$(32) \qquad N' = \begin{pmatrix} -1 & -\mathbf{1}_q^\top & \mathbf{1}_q^\top \\ -\mathbf{1}_q & M_1 & M_2 \\ \mathbf{1}_q & M_2 & M_3 \end{pmatrix}$$

of H. Note that $(N' + J_{2q+1})/2$ is the incidence matrix of a symmetric 2-design $(P, \mathcal{B})$ with parameters $(v, k, \lambda) = (2q + 1, q, (q - 1)/2)$.

PROPOSITION 6.3. *Let $q = 2m^2 - 1$ be a prime power with m odd and $(P, \mathcal{B})$ be the block design defined as above. Assume that there is a $(2m^2 - m)$-subset D of P, which is a two-intersection set with parameters $(2m^2 - m; \{m^2 - m, m^2\})$ for $(P, \mathcal{B})$. Then, there exists a regular Hadamard matrix of order $n = 4m^2$.*

Proof. Let H be the Hadamard matrix defined in (31). Define

$$(\alpha, \beta) = (m^2 - m, m^2).$$

Let $\mathbf{x}$ be the support vector of D in P. Furthermore, let A (resp. $A^\perp$) be the $(2q + 1) \times (2q + 1)$-diagonal matrix, whose entries are defined by $A_{i,i} = -1$ if $i \in D$ and 1 otherwise (resp. $A_{i,i}^\perp = -1$ if $D_\beta^\perp$ and 1 otherwise). Define

$$B = \begin{pmatrix} 1 & \mathbf{0}_q^\top \\ \mathbf{0}_q & A \end{pmatrix}, \quad B^\perp = \begin{pmatrix} 1 & \mathbf{0}_q^\top \\ \mathbf{0}_q & A^\perp \end{pmatrix}.$$

Then, $H' = B^\perp H B$ is the desired Hadamard matrix.

We show that $B^\perp H B \mathbf{1}_{2(q+1)} = 2m \mathbf{1}_{2(q+1)}$. By the definitions of B, $B^\perp$ and H, we have

$$B^\perp H B \mathbf{1}_{2(q+1)} = \begin{pmatrix} 1 & \mathbf{0}_{2q+1}^\top \\ \mathbf{0}_{2+1} & A^\perp \end{pmatrix} \begin{pmatrix} 1 & \mathbf{1}_{2q+1}^\top \\ \mathbf{1}_{2q+1} & N' \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0}_{2q+1}^\top \\ \mathbf{0}_{2q+1} & A \end{pmatrix} \begin{pmatrix} 1 \\ \mathbf{1}_{2q+1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 + \mathbf{1}_{2q+1}^\top A \mathbf{1}_{2q+1} \\ A^\perp (\mathbf{1}_{2q+1} + N' A \mathbf{1}_{2q+1}) \end{pmatrix}.$$

Since $D = |2m^2 - m|$, we have $1 + \mathbf{1}_{2q+1}^\top A \mathbf{1}_{2q+1} = 2m$. Furthermore, since D is a two-intersection set with parameters $(2m^2 - m; \{m^2 - m, m^2\})$ for $(P, \mathcal{B})$, we have

$$\left(\frac{1}{2}(N' + J_{2q+1}) \mathbf{x}\right)_i = \begin{cases} m^2 - m, & \text{if } i \in D_\alpha^\perp, \\ m^2, & \text{if } i \in D_\beta^\perp. \end{cases}$$

Hence,

$$\left(A^\perp(\mathbf{1}_{2q+1} + N'A\mathbf{1}_{2q+1})\right)_i = \left(A^\perp(\mathbf{1}_{2q+1} + N'\mathbf{1}_{2q+1} - 2N'\mathbf{x})\right)_i = 2m.$$

This completes the proof of the proposition. □

6.2. Construction of two-intersection sets satisfying the conditions of Proposition 6.3. We construct two-intersection sets satisfying the conditions of Proposition 6.3 under the assumption of the existence of a four-class association scheme.

With notations as in Theorem 6.1, assume that there is an integer ℓ not divisible by $q + 1$ satisfying the following conditions:

$$(33) \qquad \omega^\ell \in X_2 \cup X_4, \quad \omega^{\ell q} - \omega^\ell \in C_{\tau m^2}^{(4m^2, q^2)}.$$

Then, by the definition of Y_i, we have $\omega^{q\ell}(\omega^{\ell q} - \omega^\ell)^{-1} \in Y_2$ or Y_4 depending on whether $\omega^\ell \in X_2$ or X_4. Furthermore, $(\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s) \in Y_i$ if and only if $1 + \omega^\ell s \in X_i$ for every $i = 1, 2, 3, 4$.

In the following remark, we show that there exists $\ell \in \{0, 1, \ldots, q^2 - 2\}$ satisfying the condition (33).

Remark 6.4. In this remark, we see that the set

$$S = \left\{\ell : (q + 1) \nmid \ell, \omega^\ell \in X_2 \cup X_4, \omega^{\ell q} - \omega^\ell \in C_{\tau m^2}^{(4m^2, q^2)}\right\}$$

is nonempty. Since $|X_2 \cup X_4| > q$, there is $\omega^\ell \in X_2 \cup X_4$ such that $\omega^\ell \notin \mathbb{F}_q$. Furthermore, note that $X_2 \cup X_4$ is a union of cosets of $\mathbb{F}_q^*$. Hence, we evaluate the size of the set

$$T = \left\{\ell : \omega^\ell \in \omega^t \mathbb{F}_q^*, \omega^{\ell q} - \omega^\ell \in C_{\tau m^2}^{(4m^2, q^2)}\right\},$$

where $\omega^t \notin \mathbb{F}_q$. Since $\omega^{\ell q} - \omega^\ell = -\omega^{-\frac{q+1}{2}} \mathrm{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}})$, the condition $\omega^{\ell q} - \omega^\ell \in C_{\tau m^2}^{(4m^2, q^2)}$ is reformulated as

$$\mathrm{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}}) \in C_{(\tau+1)m^2}^{(4m^2, q^2)} = C_{(\tau+1)/2}^{(2, q)}.$$

Hence, we have

$$T = \left\{\ell : \omega^\ell \in \omega^t \mathbb{F}_q^*, \; \mathrm{Tr}_{q^2/q}(\omega^{\ell + \frac{q+1}{2}}) \in C_{(\tau+1)/2}^{(2, q)}\right\}.$$

The size of T is given by

$$|T| = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{x \in \omega^t \mathbb{F}_q^*} \sum_{b \in C_{(\tau+1)/2}^{(2, q)}} \psi_{\mathbb{F}_{q^2}}(ax\omega^{\frac{q+1}{2}}) \psi_{\mathbb{F}_q}(-ab)$$

$$= \frac{1}{q} \sum_{a \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q^*} \sum_{b \in C_{(\tau+1)/2}^{(2, q)}} \psi_{\mathbb{F}_{q^2}}(x\omega^{t + \frac{q+1}{2}}) \psi_{\mathbb{F}_q}(-ab) + \frac{(q-1)^2}{2q}.$$

Since $\mathrm{Tr}_{q^2/q}(\omega^{t + \frac{q+1}{2}}) \neq 0$, we have

$$|T| = \frac{q-1}{2q} \sum_{a \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q^*} \psi_{\mathbb{F}_q}(x \, \mathrm{Tr}_{q^2/q}(\omega^{t + \frac{q+1}{2}})) \psi_{\mathbb{F}_q}(a) + \frac{(q-1)^2}{2q} = \frac{q-1}{2} > 0.$$

Hence, T is nonempty, which also implies that S is nonempty.

THEOREM 6.5. *Let $q = 2m^2 - 1$ be a prime power with m odd. Assume that there are subsets X_i, $i = 1, 2, 3, 4$, satisfying the conditions of Theorem 6.1. Let $(S_0, S_1) = (X_1 \cup X_4, X_1 \cup X_2)$ or $(S_0, S_1) = (X_2 \cup X_3, X_3 \cup X_4)$ depending on whether $\omega^\ell \in X_2$ or $\omega^\ell \in X_4$. Define*

$$D_{\ell, S_d} = \left\{ x \in \mathbb{F}_q : 1 + x\omega^\ell \in S_d \right\}, \quad d = 0, 1.$$

Then, it holds that $|D_{\ell, S_0}| = m^2 - m$ and $|D_{\ell, S_1}| = m^2$. Furthermore,

$$\{|D_{\ell, S_0} \cap ((C_0^{(2,q)} \cup \{0\}) + s)| + |D_{\ell, S_1} \cap (C_0^{(2,q)} + s)| : s \in \mathbb{F}_q\} = \{m^2 - m, m^2\}$$

and

$$\{|D_{\ell, S_0} \cap (C_0^{(2,q)} + s)| + |D_{\ell, S_1} \cap ((\mathbb{F}_q^* \smallsetminus C_0^{(2,q)}) + s)| : s \in \mathbb{F}_q\} = \{m^2 - m, m^2\}.$$

Proof. We consider the case where $\omega^\ell \in X_2$. Let $S_0 = X_1 \cup X_4$ and $S_1 = X_1 \cup X_2$. In this case, $\omega^{q\ell}(\omega^{\ell q} - \omega^\ell)^{-1} \in Y_2$.

We first evaluate the sizes of D_{ℓ, S_d}, $d = 0, 1$. By Proposition 3.4,

$$(34) \qquad |D_{\ell, S_d}| = \frac{2m^2 - 1}{2} + \frac{G_q(\eta)}{2q}(1 + 2\psi_{\mathbb{F}_{q^2}}(\omega^{q\ell}(\omega^{\ell q} - \omega^\ell)^{-1}S_d)).$$

By substituting the character values of S_0 and S_1 listed in Table 1 into (34), we have $(|D_{\ell, S_0}|, |D_{\ell, S_1}|) = (m^2 - m, m^2)$. Here, we used the fact that $G_q(\eta)^2 = q$.

Next, we evaluate the following:

$$M_{1,s} := |D_{\ell, S_0} \cap ((C_0^{(2,q)} \cup \{0\}) + s)| + |D_{\ell, S_1} \cap (C_0^{(2,q)} + s)|,$$

$$M_{2,s} := |D_{\ell, S_0} \cap (C_0^{(2,q)} + s)| + |D_{\ell, S_1} \cap ((\mathbb{F}_q^* \smallsetminus C_0^{(2,q)}) + s)|.$$

By Proposition 3.6, we have

$$(35) \quad M_{1,s} = \frac{G_q(\eta)}{2q}\left(2 + \psi_{\mathbb{F}_{q^2}}((\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s)(S_0 \cup S_1))\right.$$

$$\left. + \psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q} - \omega^\ell)^{-1}\omega^{q\ell}(S_0 \cup S_1))\right) + \frac{q+1}{2} + \frac{\xi_s - \xi_\ell - \xi_s' - \xi_\ell'}{2},$$

where ξ_s, ξ_s', ξ_ℓ, and ξ_ℓ' are defined as

$$\xi_s = \begin{cases} 1, & \text{if } 1 + \omega^\ell s \in S_0, \\ 0, & \text{otherwise}, \end{cases} \qquad \xi_s' = \begin{cases} 1, & \text{if } 1 + \omega^\ell s \in S_1, \\ 0, & \text{otherwise}, \end{cases}$$

$$\xi_\ell = \begin{cases} 1, & \text{if } \omega^\ell \in S_0, \\ 0, & \text{otherwise}, \end{cases} \qquad \xi_\ell' = \begin{cases} 1, & \text{if } \omega^\ell \in S_1, \\ 0, & \text{otherwise}. \end{cases}$$

By Table 1, we have

$$1 + \psi_{\mathbb{F}_{q^2}}((\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s)(S_0 \cup S_1)) = \begin{cases} -mG_q(\eta), & \text{if } 1 + \omega^\ell s \in X_1, \\ -(m-1)G_q(\eta), & \text{if } 1 + \omega^\ell s \in X_2, \\ mG_q(\eta), & \text{if } 1 + \omega^\ell s \in X_3, \\ (m-1)G_q(\eta), & \text{if } 1 + \omega^\ell s \in X_4, \end{cases}$$

and

$$1 + \psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q} - \omega^\ell)^{-1}\omega^{q\ell}(S_0 \cup S_1)) = -(m-1)G_q(\eta).$$

Furthermore,

$$\frac{\xi_s - \xi_\ell - \xi_s' - \xi_\ell'}{2} = \begin{cases} -\frac{1}{2}, & \text{if } 1 + \omega^\ell s \in X_1, \\ -1, & \text{if } 1 + \omega^\ell s \in X_2, \\ -\frac{1}{2}, & \text{if } 1 + \omega^\ell s \in X_3, \\ 0, & \text{if } 1 + \omega^\ell s \in X_4. \end{cases}$$

Hence, we obtain

$$M_{1,s} = \begin{cases} m^2 - m, & \text{if } 1 + \omega^\ell s \in X_1 \cup X_2, \\ m^2, & \text{if } 1 + \omega^\ell s \in X_3 \cup X_4. \end{cases}$$

Next, we evaluate $M_{2,s}$. By Proposition 3.6, we have

$$(36) \quad M_{2,s} = \frac{G_q(\eta)}{2q} \Big(\psi_{\mathbb{F}_{q^2}}((\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s)S_0) - \psi_{\mathbb{F}_{q^2}}((\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s)S_1)$$

$$+ \psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q} - \omega^\ell)^{-1}\omega^{q\ell}S_0) - \psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q} - \omega^\ell)^{-1}\omega^{q\ell}S_1) \Big)$$

$$+ |D_{\ell,S_1}| + \frac{-\xi_s - \xi_\ell - \xi'_s + \xi'_\ell}{2}.$$

By Table 1, we have

$$\psi_{\mathbb{F}_{q^2}}((\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s)S_0) - \psi_{\mathbb{F}_{q^2}}((\omega^{\ell q} - \omega^\ell)^{-1}(1 + \omega^{q\ell}s)S_1)$$

$$= \begin{cases} (m+1)G_q(\eta), & \text{if } 1 + \omega^\ell s \in X_1, \\ -mG_q(\eta), & \text{if } 1 + \omega^\ell s \in X_2, \\ -(m+1)G_q(\eta), & \text{if } 1 + \omega^\ell s \in X_3, \\ mG_q(\eta), & \text{if } 1 + \omega^\ell s \in X_4, \end{cases}$$

and

$$\psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q} - \omega^\ell)^{-1}\omega^{q\ell}S_0) - \psi_{\mathbb{F}_{q^2}}(-(\omega^{\ell q} - \omega^\ell)^{-1}\omega^{q\ell}S_1) = -mG_q(\eta).$$

Furthermore,

$$\frac{-\xi_s - \xi_\ell - \xi'_s + \xi'_\ell}{2} = \begin{cases} -\frac{1}{2}, & \text{if } 1 + \omega^\ell s \in X_1, \\ 0, & \text{if } 1 + \omega^\ell s \in X_2, \\ \frac{1}{2}, & \text{if } 1 + \omega^\ell s \in X_3, \\ 0, & \text{if } 1 + \omega^\ell s \in X_4. \end{cases}$$

Hence, we obtain

$$M_{2,s} = \begin{cases} m^2, & \text{if } 1 + \omega^\ell s \in X_1 \cup X_4, \\ m^2 - m, & \text{if } 1 + \omega^\ell s \in X_2 \cup X_3. \end{cases}$$

This completes the proof of the theorem for the case where $\omega^\ell \in X_2$. The proof for the case where $\omega^\ell \in X_4$ is similar. □

We use the same labels for rows and columns of the matrix

$$N = \begin{pmatrix} M_1 & M_2 \\ M_2 & M_3 \end{pmatrix}$$

with those defined as in Subsection 5.1. The theorem above implies that $(\{0\} \times D_{\ell,S_0}) \cup (\{1\} \times D_{\ell,S_1}) \subset P$ is the desired two-intersection set for the block design $(P, \mathcal{B})$ in Proposition 6.3. (So, we do not negate the second row and column of H.) Then, Theorem 6.1 follows.

EXAMPLE. In the cases where $m = 3, 5$, we can find subsets X_i, $i = 1, 2, 3, 4$, satisfying the conditions of Theorem 6.1. Hence, in these cases, the matrix H defined in (31) can be transformed to a regular Hadamard matrix by negating some rows and columns.

In the case where $m = 3$, define four subsets of $\{0, 1, \ldots, 11\}$:

$$H_1 = \{1, 5\}, \quad H_2 = \{0, 2, 9, 10\},$$
$$H_3 = \{7, 11\}, \quad H_4 = \{3, 4, 6, 8\},$$

and define $X_i = \bigcup_{j \in H_i} C_j^{(12,17^2)}$, $i = 1, 2, 3, 4$. It is clear that $X_1 = \omega^{2m^2} X_3$, $X_2 = \omega^{2m^2} X_4$, and each X_i is a union of cosets of $C_j^{(36,17^2)}$. Furthermore, we checked by computer that X_i, $i = 1, 2, 3, 4$, take the character values listed in Table 1.

In the case where $m = 5$, define four subsets of $\{0, 1, \ldots, 19\}$:

$$H_1 = \{2, 3, 10, 19\}, \quad H_2 = \{1, 7, 14, 15, 16, 18\},$$
$$H_3 = \{0, 9, 12, 13\}, \quad H_4 = \{4, 5, 6, 8, 11, 17\},$$

and define $X_i = \bigcup_{j \in H_i} C_j^{(20,7^4)}$, $i = 1, 2, 3, 4$. It is clear that $X_1 = \omega^{2m^2} X_3$, $X_2 = \omega^{2m^2} X_4$, and each X_i is a union of cosets of $C_j^{(100,7^4)}$. Furthermore, we checked by computer that X_i, $i = 1, 2, 3, 4$, take the character values listed in Table 1.

In the case where $m = 7$, we checked by computer that there is no translation association scheme satisfying the conditions of Theorem 6.1 if each part X_i is a union of cosets of $C_0^{(28,97^2)}$. However, it may be possible if each X_i is a union of cosets of $C_0^{(196,97^2)}$ rather than a union of cosets of $C_0^{(28,97^2)}$. But, in this case, our computer could not work.

7. Concluding remarks

We conclude this paper by listing some problems for future work.

In this paper, we found new constructions of Hadamard matrices with maximum excess. In particular, we proved that if either of $(2m + 1)^2 + 2$ or $m^2 + (m + 1)^2$ is a prime power, then there exists a biregular Hadamard matrix of order $n = (2m+1)^2 + 3$ with maximum excess attaining the bound of Proposition 1.1. The constructions are based on negating some rows and columns of known Hadamard matrices obtained from quadratic residues of finite fields. In a similar way, we tried to find regular Hadamard matrices. In particular, we gave a sufficient condition for the matrix H defined in (31) being transformed to a regular Hadamard matrix of order $2(q + 1)$ under the assumption of the existence of a four-class translation association scheme on $(\mathbb{F}_{q^2}, +)$, where $q = 2m^2 - 1$ with m odd. Furthermore, we found association schemes satisfying the conditions of Theorem 6.1 in the cases where $m = 3$ and 5. Hence, we naturally have the following open question.

QUESTION 7.1. *Let $q = 2m^2 - 1$ be a prime power with m an odd integer. Does there exist a four-class association scheme satisfying the conditions of Theorem* 6.1 *for $m \geqslant 7$?*

More generally, we have the following.

QUESTION 7.2. *Can the matrix H defined in* (31) *be transformed to a regular Hadamard matrix?*

In this paper, we did not care about "symmetry" of Hadamard matrices. Hence, we give the following question.

QUESTION 7.3. *Can the Hadamard matrices obtained in Theorems* 1.2, 1.3 *and* 1.4 *be transformed to symmetric or skew ones by permuting rows and columns?*

References

[1] Eiichi Bannai, *Subschemes of some association schemes*, J. Algebra **144** (1991), no. 1, 167–188.
[2] Eiichi Bannai and Tatsuro Ito, *Algebraic Combinatorics I. Association Schemes*, Mathematics Lecture Note Series, Benjamin/Cumming Publishing Company, 1984.

[3] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley, 1997.

[4] Marc R. Best, *The excess of Hadamard matrix*, Indagationes Math. **80** (1977), 357–361.

[5] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz, *Design Theory, vol. 1, 2*, 2nd ed., Encyclopedia of Mathematics and Its Applications, vol. 69, 78, Cambridge University Press, 1999.

[6] Andries E. Brouwer, Richard M. Wilson, and Qing Xiang, *Cyclotomy and strongly regular graphs*, J. Algebr. Comb. **10** (1999), no. 1, 25–28.

[7] Robert Craigen and Hadi Kharaghani, *Weaving Hadamard matrices with maximum excess and classes with small excess*, J. Combin. Des. **12** (2004), no. 4, 233–255.

[8] Nikos Farmakis and Stratis Kounias, *The excess of Hadamard matrices and optimal designs*, Discrete Math. **67** (1987), 165–176.

[9] Joseph Hammer, Richard Levingston, and Jennifer Seberry, *A remark on the excess of Hadamard matrices and orthogonal designs*, Ars Comb. **5** (1978), 237–254.

[10] Wolfgang H. Holzmann and Hadi Kharaghani, *On the excess of Hadamard matrices*, Congr. Numer. **92** (1993), 257–260.

[11] Wolfgang H. Holzmann, Hadi Kharaghani, and M. T. Lavassani, *The excess problem and some excess inequivalent matrices of order* 32, J. Stat. Plann. Inference **72** (1998), no. 1-2, 381–391.

[12] Hadi Kharaghani, *An infinite class of Hadamard matrices of maximal excess*, Discrete Math. **89** (1991), 307–312.

[13] Christos Koukouvinos and Stratis Kounias, *Construction of some Hadamard matrices with maximum excess*, Discrete Math. **85** (1990), no. 3, 295–300.

[14] Christos Koukouvinos, Stratis Kounias, and Jennifer Seberry, *Supplementary difference sets and optimal designs*, Discrete Math. **88** (1991), no. 1, 49–58.

[15] Christos Koukouvinos and Jennifer Seberry, *Hadamard matrices of order* ≡ 8 (mod 16) *with maximal excess*, Discrete Math. **92** (1991), no. 1-3, 173–176.

[16] Stratis Kounias and Nikos Farmakis, *On the excess of Hadamard matrices*, Discrete Math. **68** (1988), no. 1, 59–69.

[17] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, 1997.

[18] Paul Meijer and Marcel van der Vlugt, *The evaluation of Gauss sums for characters of* 2-*power order*, J. Number Theory **100** (2003), no. 2, 381–395.

[19] Koji Momihara and Sho Suda, *Conference matrices with maximum excess and two-intersection sets*, Integers **17** (2017), A30 (15 pages).

[20] Mikhail E. Muzychuk, *V-rings of permutation groups with invariant metric*, Ph.D. thesis, Kiev State University (Ukraine), 1987.

[21] Jennifer Seberry, *Existence of SBIBD*($4k^2, 2k^2 \pm k, k^2 \pm k$) *and Hadamard matrices with maximal excess*, Australas. J. Comb. **4** (1991), 87–91.

[22] Thomas Storer, *Cyclotomy and Difference Sets*, Markham Publishing Company, 1967.

[23] Tianbing Xia, Mingyuan Xia, and Jennifer Seberry, *Regular Hadamard matrix, maximum excess and SBIBD*, Australas. J. Comb. **27** (2003), 263–275.

Mitsugu Hirasaka, Department of Mathematics, Pusan National University, Busan 609-735, Republic of Korea
E-mail : `hirasaka@pusan.ac.kr`

Koji Momihara, Division of Natural Science, Faculty of Advanced Science and Technology, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan
E-mail : `momihara@educ.kumamoto-u.ac.jp`

Sho Suda, Department of Mathematics Education, Aichi University of Education, 1 Hirosawa, Igaya-cho, Kariya, Aichi 448-8542, Japan
E-mail : `suda@auecc.aichi-edu.ac.jp`