Skew Hadamard difference families and skew Hadamard matrices

Koji Momihara and Qing Xiang

Abstract. In this paper, we generalize classical constructions of skew Hadamard difference families with two or four blocks in the additive groups of finite fields given by Szekeres (1969, 1971), Whiteman (1971) and Wallis-Whiteman (1972). In particular, we show that there exists a skew Hadamard difference family with 2^{u-1} blocks in the additive group of the finite field of order q^e for any prime power $q \equiv 2^u + 1 \pmod{2^{u+1}}$ with $u \geqslant 2$ and any positive integer e. In the aforementioned work of Szekeres, Whiteman, and Wallis-Whiteman, the constructions of skew Hadamard difference families with 2^{u-1} ($u = 2$ or 3) blocks in $(\mathbb{F}_{q^e}, +)$ depend on the exponent e, with $e \equiv 1, 2$, or $3 \pmod 4$ when $u = 2$, and $e \equiv 1 \pmod 2$ when $u = 3$, respectively. Our more general construction, in particular, removes the dependence on e. As a consequence, we obtain new infinite families of skew Hadamard matrices.

1. Introduction

A Hadamard matrix of order n is an $n \times n$ matrix H with entries ± 1 such that $HH^\top = nI_n$, where I_n is the identity matrix of order n. It is well known that if H is a Hadamard matrix of order n then $n = 1, 2$ or $n \equiv 0 \pmod 4$. One of the most famous conjectures in combinatorics states that a Hadamard matrix of order n exists for every positive integer n divisible by 4. This conjecture is far from being resolved despite extensive research on the problem. The smallest n for which the existence of a Hadamard matrix of order n is unknown is currently 668 (see [3]). In this paper, we are interested in Hadamard matrices which are "skew". A Hadamard matrix is called *skew* if $H = A + I_n$ and $A^\top = -A$. See [4] for a short survey of known constructions of skew Hadamard matrices. One of the most effective methods for constructing (skew) Hadamard matrices is by using difference families. Let $(G, +)$ be an additively written abelian group of order v. A *difference family* with parameters (v, k, λ) in G is a family $\mathcal{B} = \{B_i \mid i = 1, 2, \ldots, \ell\}$ of k-subsets of G such that the list of differences "$x - y, x, y \in B_i, x \neq y, i = 1, 2, \ldots, \ell$" represents every nonzero element of G exactly λ times. Each subset B_i is called a *block* of the difference family. A block B_i is called *skew* if it has the property that $B_i \cap -B_i = \emptyset$ and $B_i \cup -B_i = G \backslash \{0_G\}$. If all blocks of a difference family are skew, then the difference family is called *skew Hadamard*.

We review two known constructions of skew Hadamard matrices based on difference families. Let X be a subset of a finite abelian group $(G, +)$. Fixing an ordering for the elements of G, we define matrices $M = (m_{i,j})$ and $N = (n_{i,j})$ by

$$m_{i,j} = \begin{cases} 1, & \text{if } j - i \in X, \\ -1, & \text{if } j - i \notin X, \end{cases} \quad \text{and} \quad n_{i,j} = \begin{cases} 1, & \text{if } j + i \in X, \\ -1, & \text{if } j + i \notin X. \end{cases}$$

The matrices M and N are called *type-1* and *type-2* matrices of X, respectively.

Key words and phrases. Difference family; Skew Hadamard difference family; Skew Hadamard matrix; Gauss sum.

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, and a JSPS invitational fellowship for research in Japan S17114.

PROPOSITION 1.1. ([8, Theorem 4.4]) *Let $\mathcal{B} = \{B_i \,|\, i = 1, 2\}$ be a difference family with parameters $(v, k, \lambda) = (2m + 1, m, m - 1)$ such that B_1 is skew. Furthermore, let M_1 be the type-1 matrix of B_1 and M_2 be the type-2 matrix of B_2. Then,*

$$H = \begin{pmatrix} 1 & 1 & \mathbf{1}_v^{\mathrm{T}} & \mathbf{1}_v^{\mathrm{T}} \\ -1 & 1 & \mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} \\ -\mathbf{1}_v & -\mathbf{1}_v & -M_1 & -M_2 \\ -\mathbf{1}_v & \mathbf{1}_v & M_2 & -M_1 \end{pmatrix} \tag{1.1}$$

is a skew Hadamard matrix of order $4(m + 1)$.

Szekeres [6, 7] and Whiteman [10] found two series of skew Hadamard difference families with two blocks in $(\mathbb{F}_q, +)$, the additive group of the finite field $\mathbb{F}_q$ of order q.

PROPOSITION 1.2. *There exists a skew Hadamard difference family with two blocks in $(\mathbb{F}_q, +)$ if*

(i) ([6]) $q \equiv 5 \pmod 8$*; or*
(ii) ([7, 10]) $q = p^e$ *with* $p \equiv 5 \pmod 8$ *a prime and* $e \equiv 2 \pmod 4$.

The proofs of the results above are based on cyclotomic numbers of order four and eight, respectively. Szekeres [7] claimed that his proof for Part (ii) of Proposition 1.2 works well also for the case where $e \equiv 0 \pmod 4$. However, in the case where $e \equiv 0 \pmod 4$, the two subsets demonstrated in Theorem 1 of [7] are not skew. This inconsistency was pointed out in [8, p. 324], and also in the MathSciNet mathematical review of [7] written by B. M. Stewart.

PROPOSITION 1.3. ([9]) *Let $\mathcal{B} = \{B_i \,|\, i = 1, 2, 3, 4\}$ be a difference family with parameters $(v, k, \lambda) = (2m+1, m, 2(m-1))$ such that B_1 is skew. Furthermore, let M_1, M_2, M_4 be the type-1 matrices of B_1, B_2, B_4, respectively, and M_3 be the type-2 matrix of B_3. Then,*

$$H = \begin{pmatrix} 1 & -1 & -1 & -1 & -\mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} \\ 1 & 1 & 1 & -1 & \mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} & \mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} \\ 1 & -1 & 1 & 1 & \mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} & \mathbf{1}_v^{\mathrm{T}} \\ 1 & 1 & -1 & 1 & \mathbf{1}_v^{\mathrm{T}} & \mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} & -\mathbf{1}_v^{\mathrm{T}} \\ \mathbf{1}_v & -\mathbf{1}_v & -\mathbf{1}_v & -\mathbf{1}_v & -M_1 & -M_2 & -M_3 & -M_4 \\ \mathbf{1}_v & \mathbf{1}_v & \mathbf{1}_v & -\mathbf{1}_v & M_2^T & -M_1^{\mathrm{T}} & M_4 & -M_3 \\ \mathbf{1}_v & -\mathbf{1}_v & \mathbf{1}_v & \mathbf{1}_v & M_3 & -M_4^{\mathrm{T}} & -M_1 & M_2^{\mathrm{T}} \\ \mathbf{1}_v & \mathbf{1}_v & -\mathbf{1}_v & \mathbf{1}_v & M_4^{\mathrm{T}} & M_3 & -M_2 & -M_1^{\mathrm{T}} \end{pmatrix} \tag{1.2}$$

is a skew Hadamard matrix of order $8(m + 1)$.

Wallis and Whiteman [9] found one series of skew Hadamard difference families with four blocks in $(\mathbb{F}_q, +)$ based on cyclotomic numbers of order eight.

PROPOSITION 1.4. *There exists a skew Hadamard difference family with four blocks in $(\mathbb{F}_q, +)$ if $q \equiv 9 \pmod{16}$.*

In this paper, we generalize the results in Propositions 1.2 and 1.4 using cyclotomic classes of order a power of 2. In general, it is quite difficult to find explicit formulas for cyclotomic numbers of high order. In this paper, we overcome this difficulty by evaluating Gauss sums with respect to a multiplicative character of order a power of 2 by a recursive technique.

THEOREM 1.5. *Let $u \geqslant 2$ be an integer and q be a prime power such that $q \equiv 2^u + 1 \pmod{2^{u+1}}$. Then, there exists a skew Hadamard difference family with 2^{u-1} blocks in $(\mathbb{F}_{q^e}, +)$ for any positive integer e.*

We emphasize that the exponent $e \geq 1$ can be taken arbitrarily in Theorem 1.5. In contrast, Propositions 1.2 and 1.4 depend on e. In the case of Proposition 1.2, the exponent e is limited to $e \equiv 1, 2$, or $3 \pmod 4$, and in the case of Proposition 1.4, the exponent e is limited to $e \equiv 1 \pmod 2$.

By applying Propositions 1.1 and 1.3 to the skew Hadamard difference families arising from Theorem 1.5 with $u = 2$ and $u = 3$, respectively, we have the following corollaries.

COROLLARY 1.6. *Let q be a prime power such that $q \equiv 5 \pmod 8$ and e be an arbitrary positive integer. Then, there exists a skew Hadamard matrix of order $2(q^e+1)$.*

COROLLARY 1.7. *Let q be a prime power such that $q \equiv 9 \pmod{16}$ and e be an arbitrary positive integer. Then, there exists a skew Hadamard matrix of order $4(q^e+1)$.*

2. Evaluation of Gauss sums

Let $\mathbb{F}_q$ be the finite field of order $q = p^r$ with p a prime and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$. Let γ be a primitive element of $\mathbb{F}_q$. For a positive integer N dividing $q-1$, define

$$C_i^{(N,q)} = \gamma^i\langle\gamma^N\rangle, \quad i = 0, 1, \ldots, N-1,$$

which are called *cyclotomic classes* of order N. We will need to compute additive character values of a union of some cyclotomic classes of order N. So we introduce additive characters of finite fields below.

For a positive integer k, let ζ_k be a complex primitive kth root of unity. Define $\psi_{\mathbb{F}_q}\colon \mathbb{F}_q \to \mathbb{C}^*$ by

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

where $\mathrm{Tr}_{q/p}(x)$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. The map $\psi_{\mathbb{F}_q}$ is a character of the additive group of $\mathbb{F}_q$, and it is called the *canonical* additive character of $\mathbb{F}_q$.

DEFINITION 2.1. For a multiplicative character χ and the canonical additive character $\psi_{\mathbb{F}_q}$ of $\mathbb{F}_q$, the *Gauss sum* $G_q(\chi)$ of $\mathbb{F}_q$ is defined by

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

For a multiplicative character χ of order N of $\mathbb{F}_q$ and $x \in \mathbb{F}_q^*$, by the orthogonality of characters [**5**, p. 195, (5.17)], the character value of $C_i^{(N,q)}$ can be expressed in terms of Gauss sums as follows:

$$\psi_{\mathbb{F}_q}(C_i^{(N,q)}) = \frac{1}{N}\sum_{j=0}^{N-1} G_q(\chi^j)\chi^{-j}(\gamma^i),\ 0 \leqslant i \leqslant N-1. \tag{2.1}$$

We list some basic properties of Gauss sums below, which will be used in Section 3.

LEMMA 2.1. *The Gauss sums $G_q(\chi)$ satisfy the following:*

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;*
4. $G_q(\chi^p) = G_q(\chi)$.

We will need the *Davenport-Hasse lifting formula*, which is stated below.

THEOREM 2.2. ([**1**, Theorem 11.5.2]) *Let χ' be a nontrivial multiplicative character of $\mathbb{F}_q$ and let χ be the lift of χ' to $\mathbb{F}_{q^f}$, i.e., $\chi(x) = \chi'(x^{\frac{q^f-1}{q-1}})$ for $x \in \mathbb{F}_{q^f}$, where $f \geq 2$ is an integer. Then*

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

The following theorem is often referred to as the *Davenport-Hasse product formula*.

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

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

In the rest of this paper, we always assume that q is a prime power such that $q \equiv 2^u + 1 \pmod{2^{u+1}}$ with $u \geqslant 2$. Fix $N = 2^t$ with $t \geqslant u+1$ and put $f := 2^{t-u}$. Then q has order f modulo N; that is, $q^f \equiv 1 \pmod{N}$, and $q^{2^{t-u-1}} \not\equiv 1 \pmod{N}$.

The following is our main theorem in this section.

THEOREM 2.4. *Let χ_N be a multiplicative character of order N of $\mathbb{F}_{q^f}$ and ω be a primitive element of $\mathbb{F}_{q^f}$. Furthermore, let χ'_{2^u} be a multiplicative character of order 2^u of $\mathbb{F}_q$ such that $\chi_N^{2^{t-u}}$ is the lift of χ'_{2^u}, i.e., $\chi_N^{2^{t-u}}(\omega) = \chi'_{2^u}(\omega^{\frac{q^f-1}{q-1}})$, and let η' be the quadratic character of $\mathbb{F}_q$. Then, there exists $\epsilon \in \langle \zeta_{2^u} \rangle$ such that*

$$G_{q^f}(\chi_N) = \epsilon q^{f/2-1} G_q(\chi'_{2^u}) G_q(\eta').$$

PROOF. By the Davenport-Hasse product formula (Theorem 2.3), we have

$$G_{q^f}(\chi_N) = \frac{G_{q^f}(\chi_N^f)}{\chi_N^f(f)} \prod_{i=1}^{f-1} \frac{G_{q^f}(\chi_f^i)}{G_{q^f}(\chi_N \chi_f^i)}, \tag{2.2}$$

where χ_f is a fixed multiplicative character of order $f = 2^{t-u}$ of $\mathbb{F}_{q^f}$. We can write $\chi_f = \chi_N^{2^u \ell}$ for some odd ℓ. Then $\chi_N \chi_f = \chi_N^{2^u \ell + 1}$. We claim that for any ℓ, $0 \leq \ell \leq 2^{t-u} - 1$, $2^u \ell + 1 \in \langle q \rangle \pmod{N}$. This can be seen as follows. Noting that q has order $f = 2^{t-u}$ modulo N, and $q^i \equiv 1 \pmod{2^u}$ for any i, we see that $2^u \ell + 1 \in \langle q \rangle \pmod{N}$ for all $\ell = 0, 1, \ldots, 2^{t-u} - 1$. Now from Property (4) of Lemma 2.1, it follows that

$$G_{q^f}(\chi_N) = G_{q^f}(\chi_N \chi_f) = \cdots = G_{q^f}(\chi_N \chi_f^{f-1}).$$

Also from Properties (1) and (2) of Lemma 2.1, we have $G_{q^f}(\chi_f^i) G_{q^f}(\chi_f^{f-i}) = q^f$ for $i = 1, 2, \ldots, f/2 - 1$. Substituting these into (2.2), we obtain

$$G_{q^f}(\chi_N)^f = \chi_N^{-f}(f) q^{f(f/2-1)} G_{q^f}(\chi_N^f) G_{q^f}(\eta), \tag{2.3}$$

where η is the quadratic character of $\mathbb{F}_{q^f}$. Next applying the Davenport-Hasse lifting formula (Theorem 2.2) to the right hand side of (2.3), we have

$$G_{q^f}(\chi_N)^f = \chi_N^{-f}(f) q^{f(f/2-1)} G_q(\chi'_{2^u})^f G_q(\eta')^f.$$

Hence, there exists $\epsilon \in \langle \zeta_N \rangle$ such that

$$G_{q^f}(\chi_N) = \epsilon q^{f/2-1} G_q(\chi'_{2^u}) G_q(\eta'). \tag{2.4}$$

Define $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_N)/\mathbb{Q}(\zeta_p))$ by $\tau(\zeta_{pN}) = \zeta_{pN}^{N\ell+q}$, where ℓ is the inverse of N modulo p. Note that $N\ell + q \equiv q \pmod{N}$ and $N\ell + q \equiv 1 \pmod{p}$. Applying τ to $G_{q^f}(\chi_N)/G_q(\chi'_{2^u}) G_q(\eta')$, we have

$$\begin{aligned}
\tau\left(\frac{G_{q^f}(\chi_N)}{G_q(\chi'_{2^u}) G_q(\eta')}\right) &= \tau\left(\frac{\sum_{x \in \mathbb{F}_{q^f}} \psi_{\mathbb{F}_{q^f}}(x) \chi_N(x)}{\left(\sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(x) \chi'_{2^u}(x)\right)\left(\sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(x) \eta'(x)\right)}\right) \\
&= \frac{\sum_{x \in \mathbb{F}_{q^f}} \psi_{\mathbb{F}_{q^f}}(x) \chi_N^q(x)}{\left(\sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(x) \chi'^q_{2^u}(x)\right)\left(\sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}((x) \eta'^q(x)\right)} \\
&= \frac{G_{q^f}(\chi_N^q)}{G_q(\chi'^q_{2^u}) G_q(\eta'^q)} = \frac{G_{q^f}(\chi_N)}{G_q(\chi'_{2^u}) G_q(\eta')}.
\end{aligned}$$

This shows that ϵ is invariant under the action of τ. It follows that $\epsilon \in \langle \zeta_{2^u} \rangle$. The proof of the proposition is now complete. □

REMARK 2.5. Put $\gamma := \omega^{\frac{q^f-1}{q-1}}$, which is a primitive element of $\mathbb{F}_q$. In the proposition above, ϵ has the form $\epsilon = \chi'_{2^u}(\gamma^{-b})$ for some $b \in \{0, 1, \ldots, 2^u - 1\}$.

3. Skew Hadamard difference families in finite fields

We retain the same assumptions on q, u, N and f as specified in Section 2. Define subsets in $\mathbb{F}_q$ and $\mathbb{F}_{q^f}$, respectively, by

$$B_h := \bigcup_{j=0}^{2^{u-1}-1} C_{h+j}^{(2^u,q)} \subset \mathbb{F}_q, \quad h = 0, 1, \ldots, 2^u - 1, \tag{3.1}$$

and

$$D_h := \bigcup_{j=0}^{N/2-1} C_{h+j}^{(N,q^f)} \subset \mathbb{F}_{q^f}, \quad h = 0, 1, \ldots, N-1. \tag{3.2}$$

We list some important properties of B_h and D_h below:

(i) $-B_h = B_{h+2^{u-1}}$, $B_h \cap -B_h = \emptyset$, $|B_h| = (q-1)/2$, and $B_h \cup -B_h = \mathbb{F}_q^*$;
(ii) $-D_h = D_{h+2^{t-1}}$, $D_h \cap -D_h = \emptyset$, $|D_h| = (q^f-1)/2$, and $D_h \cup -D_h = \mathbb{F}_{q^f}^*$.

Hence, both B_h and D_h are skew.

3.1. Character values of D_h. We express the (additive) character values of D_h in terms of those of B_h.

Proposition 3.1. *For $a = 0, 1, \ldots, N-1$ and $h = 0, 1, \ldots, N-1$, we have*

$$\psi_{\mathbb{F}_{q^f}}(\omega^a D_h) = \frac{-1 + q^{f/2-1} G_q(\eta')}{2} + q^{f/2-1} G_q(\eta') \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0),$$

where $j_{a,h}$ is uniquely determined as $j_{a,h} = (a+h+j)/2^{t-u}$ for some $j \in \{0, 1, \ldots, 2^{t-u}-1\}$ such that $2^{t-u} \mid (a+h+j)$, and b is given in Remark 2.5.

Proof. By (2.1), we have

$$\psi_{\mathbb{F}_{q^f}}(\omega^a D_h) = \frac{1}{N} \sum_{j=0}^{N/2-1} \sum_{i=0}^{N-1} G_{q^f}(\chi_N^i) \chi_N^{-i}(\omega^{a+h+j}). \tag{3.3}$$

Since $\sum_{j=0}^{N/2-1} \chi_N^{-i}(\omega^{a+h+j}) = 0$ if i, $0 \le i \le N-1$, is a nonzero even integer, continuing from (3.3), we have

$$\psi_{\mathbb{F}_{q^f}}(\omega^a D_h) = -\frac{1}{2} + \frac{1}{N} \sum_{j=0}^{N/2-1} \sum_{i:\text{odd}} G_{q^f}(\chi_N^i) \chi_N^{-i}(\omega^{a+h+j}). \tag{3.4}$$

For each odd i, $0 \le i \le N-1$, write $i = 2^u i_1 + i_2$ with $i_1 \in \{0, 1, \ldots, 2^{t-u}-1\}$ and $i_2 \in \{1, 3, \ldots, 2^u - 1\}$. Note that since $2^u \ell + 1 \in \langle q \rangle \pmod N$, we have $G_{q^f}(\chi_N^{2^u i_1 + i_2}) = G_{q^f}(\chi_N^{2^u i_1' + i_2})$ for any $i_1, i_1' = 0, 1, \ldots, 2^{t-u}-1$. It follows that

$$\sum_{j=0}^{N/2-1} \sum_{i:\text{odd}} G_{q^f}(\chi_N^i) \chi_N^{-i}(\omega^{a+h+j}) = \sum_{i_2:\text{odd}} G_{q^f}(\chi_N^{i_2}) \sum_{j=0}^{N/2-1} \sum_{i_1=0}^{2^{t-u}-1} \chi_N^{-2^u i_1 - i_2}(\omega^{a+h+j}). \tag{3.5}$$

Let $J := \{a+h+j \mid a+h+j \equiv 0 \pmod{2^{t-u}}, j = 0, 1, \ldots, N/2-1\}$. There is a unique $j \in \{0, 1, \ldots, 2^{t-u}-1\}$ such that $a+h+j \equiv 0 \pmod{2^{t-u}}$; for such a j, write $a+h+j = 2^{t-u} j_{a,h}$. Then, we have $J = \{2^{t-u}(j_{a,h} + j') \mid j' = 0, 1, \ldots, 2^{u-1}-1\}$. Hence,

$$\begin{aligned}\sum_{j=0}^{N/2-1} \sum_{i_1=0}^{2^{t-u}-1} \chi_N^{-2^u i_1 - i_2}(\omega^{a+h+j}) &= \sum_{j=0}^{N/2-1} \chi_N^{-i_2}(\omega^{a+h+j}) \sum_{i_1=0}^{2^{t-u}-1} \chi_N^{-2^u i_1}(\omega^{a+h+j}) \\ &= 2^{t-u} \sum_{j'=0}^{2^{u-1}-1} \chi_N^{-i_2}(\omega^{2^{t-u}(j_{a,h}+j')}) = 2^{t-u} \sum_{j'=0}^{2^{u-1}-1} \chi'^{-i_2}_{2^u}(\gamma^{j_{a,h}+j'}).\end{aligned}$$

Applying Theorem 2.4 and Remark 2.5, continuing from (3.5), we have

$$\begin{aligned}
&\sum_{i_2:\text{odd}} G_{q^f}(\chi_N^{i_2}) \sum_{j=0}^{N/2-1} \sum_{i_1=0}^{2^{t-u}-1} \chi_N^{-2^u i_1 - i_2}(\omega^{a+h+j}) \\
&= q^{f/2-1} G_q(\eta') \sum_{i_2:\text{odd}} G_q(\chi'^{i_2}_{2^u}) \sum_{j=0}^{N/2-1} \sum_{i_1=0}^{2^{t-u}-1} \chi_N^{-2^u i_1 - i_2}(\omega^{a+h+j}) \chi'^{-i_2}_{2^u}(\gamma^b) \\
&= 2^{t-u} q^{f/2-1} G_q(\eta') \sum_{j'=0}^{2^{u-1}-1} \sum_{i_2:\text{odd}} G_q(\chi'^{i_2}_{2^u}) \chi'^{-i_2}_{2^u}(\gamma^{b+j_{a,h}+j'}). \qquad (3.6)
\end{aligned}$$

Since $\sum_{j'=0}^{2^{u-1}-1} \chi'^{-i}_{2^u}(\gamma^{b+j_{a,h}+j'}) = 0$ for any nonzero even i, we have

$$\sum_{j'=0}^{2^{u-1}-1} \sum_{i_2:\text{odd}} G_q(\chi'^{i_2}_{2^u}) \chi'^{-i_2}_{2^u}(\gamma^{b+j_{a,h}+j'}) = 2^{u-1} + 2^u \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0). \qquad (3.7)$$

Thus, by combining (3.4), (3.5), (3.6) and (3.7), we obtain

$$\psi_{\mathbb{F}_{q^f}}(\omega^a D_h) = \frac{-1 + q^{f/2-1} G_q(\eta')}{2} + q^{f/2-1} G_q(\eta') \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0).$$

This completes the proof of the proposition. □

Remark 3.2. For $j_{a,h}$ defined in Proposition 3.1, we have $j_{a,h+2^{t-u}\ell} = j_{a,h} + \ell$ for any $\ell \in \mathbb{Z}$.

Corollary 3.3. *For $a = 0, 1, \ldots, N-1$ and $h = 0, 1, \ldots, N-1$, we have*

$$\psi_{\mathbb{F}_{q^f}}(\omega^a D_h) \overline{\psi_{\mathbb{F}_{q^f}}(\omega^a D_h)} = \frac{1 - q^{f-1}}{4} + q^{f-1} \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0) \overline{\psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0)}.$$

Proof. By Proposition 3.1, we have

$$\begin{aligned}
\psi_{\mathbb{F}_{q^f}}(\omega^a D_h) \overline{\psi_{\mathbb{F}_{q^f}}(\omega^a D_h)} = &\left(\frac{-1 + q^{f/2-1} G_q(\eta')}{2} + q^{f/2-1} G_q(\eta') \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0) \right) \\
&\times \left(\overline{\frac{-1 + q^{f/2-1} G_q(\eta')}{2} + q^{f/2-1} G_q(\eta') \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0)} \right). \qquad (3.8)
\end{aligned}$$

Here, $G_q(\eta') \in \mathbb{R}$ since $q \equiv 1 \pmod 4$. Furthermore, note that

$$\psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0) + \overline{\psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0)} = \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0) + \psi_{\mathbb{F}_q}(-\gamma^{b+j_{a,h}} B_0) = -1.$$

Now, continuing from (3.8), we have

$$\psi_{\mathbb{F}_{q^f}}(\omega^a D_h) \overline{\psi_{\mathbb{F}_{q^f}}(\omega^a D_h)} = \frac{1 - q^{f-2} G_q(\eta')^2}{4} + q^{f-2} G_q(\eta')^2 \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0) \overline{\psi_{\mathbb{F}_q}(\gamma^{b+j_{a,h}} B_0)}.$$

Finally, by using $G_q(\eta')^2 = q$, we obtain the assertion of the corollary. □

3.2. Construction of skew Hadamard difference families. We begin by stating the following lemma which is well known in the theory of difference families. We refer the reader to [2] for a proof of the lemma.

Lemma 3.4. *Let $(G, +)$ be a finite abelian group, and E_i, $1 \le i \le \ell$, be k-subsets of G. Then, the following are equivalent:*

1. *The family $\{E_i \mid i = 1, 2, \ldots, \ell\}$ is a difference family in G;*
2. *For any $a \in G \setminus \{0_G\}$, $\sum_{i=1}^{\ell} |E_i \cap (E_i + a)|$ is a constant not depending on a;*
3. *For any nontrivial character ψ of G, $\sum_{i=1}^{\ell} \psi(E_i) \overline{\psi(E_i)} = k\ell - \lambda$ for some $\lambda \in \mathbb{N}$.*

Now we define two families of subsets of $\mathbb{F}_q$ and $\mathbb{F}_{q^f}$, respectively, by

$$\mathcal{B} := \{B_i \mid i = 0, 1, \ldots, 2^{u-1} - 1\} \tag{3.9}$$

and

$$\mathcal{D} := \{D_{2^{t-u}\ell} \mid \ell = 0, 1, \ldots, 2^{u-1} - 1\}. \tag{3.10}$$

LEMMA 3.5. *The family $\mathcal{B}$ is a skew Hadamard difference family in $(\mathbb{F}_q, +)$.*

PROOF. We show that $\sum_{i=0}^{2^{u-1}-1} |B_i \cap (B_i + a)|$ is a constant not depending on $a \in \mathbb{F}_q^*$. Then, by Lemma 3.4 (2), $\mathcal{B}$ is a skew Hadamard difference family in $(\mathbb{F}_q, +)$. Since $-B_i = B_{i+2^{u-1}}$, we have $|B_i \cap (B_i + a)| = |B_{i+2^{u-1}} \cap (B_{i+2^{u-1}} + a)|$. It follows that

$$\begin{aligned}\sum_{i=0}^{2^{u-1}-1} |B_i \cap (B_i + a)| &= \frac{1}{2} \sum_{i=0}^{2^u-1} |B_i \cap (B_i + a)| \\ &= \frac{1}{2} \sum_{j=0}^{2^{u-1}-1} \sum_{h=0}^{2^{u-1}-1} \sum_{i=0}^{2^u-1} \left| C_{i+j}^{(2^u,q)} \cap \left(C_{i+h}^{(2^u,q)} + a \right) \right|.\end{aligned} \tag{3.11}$$

Since the equation $\gamma^{i+j}x = \gamma^{i+h}y + a$ can be rewritten as $\gamma^{j-h}xy^{-1} = a\gamma^{-i-h}y^{-1} + 1$ with $x, y \in C_0^{(2^u,q)}$, the right-hand side of the second equality in (3.11) is equal to

$$\frac{1}{2} \sum_{j=0}^{2^{u-1}-1} \sum_{h=0}^{2^{u-1}-1} \sum_{i=0}^{2^u-1} \left| C_{j-h}^{(2^u,q)} \cap \left(a \cdot C_{-i-h}^{(2^u,q)} + 1 \right) \right| = \frac{1}{2} \sum_{j=0}^{2^{u-1}-1} \sum_{h=0}^{2^{u-1}-1} \left| C_{j-h}^{(2^u,q)} \cap \left(\mathbb{F}_q^* + 1 \right) \right|,$$

which is a constant not depending on $a \in \mathbb{F}_q^*$. □

THEOREM 3.6. *The family $\mathcal{D}$ is a skew Hadamard difference family in $(\mathbb{F}_{q^f}, +)$.*

PROOF. By Proposition 3.3, we have

$$\begin{aligned}&\sum_{\ell=0}^{2^{u-1}-1} \psi_{\mathbb{F}_{q^f}}(\omega^a D_{2^{t-u}\ell}) \overline{\psi_{\mathbb{F}_{q^f}}(\omega^a D_{2^{t-u}\ell})} \\ &= \frac{2^{u-1}(1 - q^{f-1})}{4} + q^{f-1} \sum_{\ell=0}^{2^{u-1}-1} \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,2^{t-u}\ell}} B_0) \overline{\psi_{\mathbb{F}_q}(\gamma^{b+j_{a,2^{t-u}\ell}} B_0)}.\end{aligned} \tag{3.12}$$

By Remark 3.2, the right-hand side of (3.12) can be rewritten as

$$\frac{2^{u-1}(1 - q^{f-1})}{4} + q^{f-1} \sum_{\ell=0}^{2^{u-1}-1} \psi_{\mathbb{F}_q}(\gamma^{b+j_{a,0}} B_\ell) \overline{\psi_{\mathbb{F}_q}(\gamma^{b+j_{a,0}} B_\ell)}.$$

By Part (3) of Lemma 3.4, $\mathcal{D}$ is a skew Hadamard difference family in $(\mathbb{F}_{q^f}, +)$ if and only if $\mathcal{B}$ is a skew Hadamard difference family in $(\mathbb{F}_q, +)$. Now the conclusion of the theorem follows from Lemma 3.5. □

Noting that $q \equiv 2^u + 1 \pmod{2^{u+1}}$ if and only if $q^s \equiv 2^u + 1 \pmod{2^{u+1}}$ for any odd positive integer s, we see that Theorem 1.5 follows from Theorem 3.6.

References

[1] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*. Vol. II. Second edition. Encyclopedia of Mathematics and its Applications, 78. Cambridge University Press, Cambridge, 1999.
[3] H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428, *J. Combin. Des.* **13** (2005), 435–440.
[4] C. Koukouvinos, S. Stylianou, On skew-Hadamard matrices, *Discrete Math.* **308** (2008), 2723–2731.
[5] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
[6] G. Szekeres, Tournaments and Hadamard matrices, *Enseignement Math.* **15** (1969), 269–278.
[7] G. Szekeres, Cyclotomy and complementary difference sets, *Acta Arith.* **18** (1971), 349–353.

[8] W. D. Wallis, A. P. Street, J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics, **292**, Springer, New York, 1972.
[9] J. Wallis, A. L. Whiteman, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.* **7** (1972), 233–249.
[10] A. L. Whiteman, An infinite family of skew Hadamard matrices, *Pacific J. Math.* **38** (1971), 817–822.

Department of Mathematics, 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: qxiang@udel.edu