European Journal of Combinatorics 76 (2019) 73–81

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Constructions of skew Hadamard difference families

Koji Momihara [a], Qing Xiang [b]

[a] Division of Natural Science, Faculty of Advanced Science and Technology, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan
[b] Department of Mathematical Sciences, University of Delaware, Newark DE 19716, USA

ARTICLE INFO

Article history:
Received 31 January 2018
Accepted 13 September 2018
Available online xxxx

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 papers of Szekeres, Whiteman, and Wallis–Whiteman, the constructions of skew Hadamard difference families with 2^{u-1} ($u = 2$ or 3) blocks in $(\mathbb{F}_{q^e}, +)$ work only for restricted e;namely $e \equiv 1, 2$, 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 restrictions on e. As a consequence, we obtain new infinite series of skew Hadamard difference families with two or four blocks, and hence 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

E-mail addresses: momihara@educ.kumamoto-u.ac.jp (K. Momihara), qxiang@udel.edu (Q. Xiang).

https://doi.org/10.1016/j.ejc.2018.09.007
0195-6698/

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 $B_i \cup (-B_i) = G \setminus \{0_G\}$. 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

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

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

Proposition 1.1 (*[8, Theorem 4.4]*)**.** *Let $\mathcal{B} = \{B_i \mid i = 1, 2\}$ 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,*

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

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 $\mathcal{B} = \{B_i \mid i = 1, 2, 3, 4\}$ 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,*

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

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