Journal of Algebraic Combinatorics **14** (2001), 103–117

Hadamard and Conference Matrices

K.T. ARASU
Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435, USA

YU QING CHEN
Department of Mathematics, RMIT-City Campus, GPO Box 2476V, Melbourne, Victoria 3001, Australia

ALEXANDER POTT
Institute for Algebra and Geometry, Otto-von-Guericke-University Magdeburg, 39016 Magdeburg, Germany

Received October 11, 2000; Revised April 12, 2001

Abstract. We discuss new constructions of Hadamard and conference matrices using relative difference sets. We present the first example of a relative $(n, 2, n-1, \frac{n-2}{2})$-difference set where $n-1$ is not a prime power.

Keywords: difference sets, relative difference sets, Hadamard matrices

1. Introduction

One of the most interesting problems in combinatorics is the question whether Hadamard matrices exist for all orders n divisible by 4. A **Hadamard matrix** H of order n is a ± 1-matrix which satisfies $HH^t = nI_n$. They exist for

$$n = 1, \quad n = 2 \left(\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right), \quad n = 4 \left(\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix} \right)$$

and many more values of n. It is not difficult to see that a Hadamard matrix of order n satisfies $n = 1$, $n = 2$ or n is divisible by 4. The smallest case n where it is presently not known whether a Hadamard matrix exists is $n = 428$.

Many recursive or clever "ad hoc" constructions of Hadamard matrices are known; we refer the reader to [3, 5] and [23], for instance. We also refer the reader to [3] for background from design theory. But we define and explain all terms from scratch, hence it is not necessary to consult the encyclopaedian books [3] and [4].

It has been conjectured by de Launey and Horadam [7] that the Hadamard matrix conjecture can be solved using relative difference sets. More precisely, they conjecture that for all $n \equiv 0 \bmod 4$ there exists a (not necessarily abelian) relative difference set with parameters $(n, 2, n, \frac{n}{2})$. It turns out that these relative difference sets are equivalent to cocyclic Hadamard matrices. We refer to [9] and [6] for recent results on cocyclic Hadamard matrices and, more generally, to [14] for cocyclic development of designs.

A more concrete suggestion on how to prove the Hadamard matrix conjecture is contained in Ito [16]. He suggests that certain relative difference sets in a special class of non-abelian groups of order $8t$ should be used to construct Hadamard matrices of order $4t$. Flannery shows [12] that Ito's relative difference sets are indeed equivalent to cocyclic Hadamard matrices. At present, no value t is known for which an argument exists that shows the nonexistence of such a relative difference set. Therefore it is conceivable that Ito's difference set construction can settle the Hadamard matrix conjecture! We emphasize that Ito's suggestion does not imply that the Hadamard design corresponding to the matrix has a difference set description!

Another class of matrices are the so called conference matrices. A **conference matrix** of size n is a $(0, \pm 1)$-matrix which satisfies $CC^t = (n-1)I_n$. It can be easily seen that the size n of a conference matrix is 1 or n is even. It is conjectured that they exist whenever $n \equiv 0 \bmod 4$ or if $n \equiv 2 \bmod 4$ and $n - 1$ is the sum of two squares; it is known that these restrictions on n are necessary. The conjecture that the necessary conditions are also sufficient is true for $n \leq 62$ if $n \equiv 2 \bmod 4$ and $n \leq 184$ if $n \equiv 0 \bmod 4$, see [5].

There is a construction of conference matrices of order n using projections of affine difference sets, see [19] and Section 5 of this paper. It has been conjectured that this construction works only if $n - 1$ is an odd prime power. In this paper we present the first series of relative difference sets in groups of size $2n$ (giving conference matrices of size n) where $n - 1$ is not a prime power. Similar to the Hadamard matrix case, this construction may work for more values of n, not only the cases covered by Theorem 5.7. Therefore, our new construction may help to solve the conference matrix conjecture.

Finally, let us mention some connections between conference and Hadamard matrices of order n. Obviously, not all conference matrices can give rise to Hadamard matrices since conference matrices of size $n \equiv 2 \bmod 4$ exist. A Hadamard matrix H is called **skew** if its entries on the main diagonal are $+1$ and

$$C := H - I_n$$

is skew symmetric. Obviously, C is a skew-symmetric conference matrix if and only if H is skew.

It is conjectured that skew Hadamard matrices exist for $n = 1$, $n = 2$ and all n divisible by 4. The conference matrices constructed in Theorem 5.7 are skew symmetric.

This paper is organized as follows: In Section 2, we introduce the notion of difference sets and group rings. Section 3 deals with the connection between difference sets and Hadamard matrices. In Section 4, we present a new recursive construction of relative difference sets in certain non-abelian groups using Golay complementary pairs. This generalizes a construction of Schmidt. Finally (Section 5), a new construction of certain relative difference sets in groups of order $2n$ (which yield skew symmetric conference matrices of size n and thus skew Hadamard matrices) is presented. This gives the first examples of such relative difference sets where $n - 1$ is not a prime power.

2. Preliminaries

A **divisible design** $\mathcal{D}$ with parameters (n, m, k, λ) is an incidence structure with the following properties:

(D1) The number of points is mn and there is a partition of the points into n point classes of size m, each.
(D2) Given two points p and q in different point classes, there are precisely λ blocks containing p and q.
(D3) Points in the same point class are not joined by a block.
(D4) Each block contains exactly k points.

The **incidence matrix** of a design $\mathcal{D}$ is a $(0, 1)$-matrix where the rows are labelled with the points and the columns with the blocks. The (p, B)-entry is 1 if p is a point on the block B, otherwise it is 0.

A divisible design is called **class regular** if there is an automorphism group H acting regularly on the points of each point class (acting regularly means that for any two points p and q there is a unique group element $g \in H$ such that $p^g = q$).

A divisible design with $m = 2$ is class regular if and only if exchanging the points in each point class induces an automorphism of the design.

For the convenience of the reader we include a short proof of the following well known result:

Theorem 2.1 *The existence of a Hadamard matrix, resp. conference matrix, of size n is equivalent to the existence of a class regular* $(n, 2, n, \frac{n}{2})$, *resp.* $(n, 2, n-1, \frac{n-2}{2})$ *divisible design.*

Proof (only conference matrix case)**:** Take the conference matrix C and replace an entry 0 by $\left(\begin{smallmatrix}0 & 0\\ 0 & 0\end{smallmatrix}\right)$, an entry $+1$ by $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and -1 by $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. The $2n \times 2n$ matrix constructed in this way is the incidence matrix of an $(n, 2, n-1, \frac{n-2}{2})$ divisible design.

Conversely, let τ be the automorphism of order 2 fixing all point classes. We label the rows of the incidence matrix such that rows corresponding to points in the same point class are adjacent. The columns are labeled such that blocks B and $\tau(B)$ correspond to adjacent columns. Then the incidence matrix consists of pieces

$$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, \quad \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Replacing these matrices by 0, 1 and -1 yields the desired conference matrix. □

In this paper, we consider only divisible designs with parameters

$$\left(n, 2, n, \frac{n}{2}\right) \tag{1}$$

and

$$\left(n, 2, n-1, \frac{n-2}{2}\right). \tag{2}$$

The class regular designs which we are going to describe in this paper admit actually a much larger automorphism group. More precisely, we consider so called **relative difference sets**. Let G be a group of order mn containing a normal subgroup H of order m. A k-subset $D \subseteq G$ is called an (n, m, k, λ)-difference set relative to H if the list

$$(dd'^{-1} : d, d' \in D, d \neq d')$$

contains each element in $G \backslash H$ exactly λ times and no element in H. Relative difference sets with $|H| = 1$ are the well known and well studied **difference sets**, see [3]. For obvious reasons, the subgroup H is called the forbidden subgroup. As an example, $\{0, 1, 3\}$ in $\mathbb{Z}_8$ is a $(4, 2, 3, 1)$-difference set (additively written) relative to $\{0, 4\}$.

We define a design corresponding to D as follows: The points are the group elements, the blocks are the "translates" $Dg := \{dg : d \in D\}$ of D. It is fairly easy to see that this design is a divisible (n, m, k, λ) design. The construction also works if H is not a normal subgroup. However, if H is normal then H acts class regularly on the design. More generally, the group of mappings

$$\begin{aligned} \pi_g : G &\to G \\ x &\mapsto xg \end{aligned}$$

acts regularly on the design:

$$\begin{aligned} x, y \in Dh &\Leftrightarrow x = dh \text{ and } y = d'h \text{ for some } d, d' \in D \\ &\Leftrightarrow xy^{-1} = dd'^{-1} \text{ and } x = dh \\ &\Leftrightarrow xg, yg \in Dhg. \end{aligned}$$

Two points $x, y, x \neq y$, are in the same point class if and only if xy^{-1} cannot be represented as a quotient dd'^{-1}, $d, d' \in D$, hence $x \in Hy$. Therefore, point classes are right cosets of H. If $g \in H$, then $\pi_g[Hy] = Hyg = ygH = yH = Hy$ provided H is a normal subgroup of G. If H is not normal then π_g does not fix the point classes.

As an example (which is contained in [8]) for this situation, take $D = \{1, a, a^3, b\} \subset G$ where

$$G = \langle a, b : a^4 = b^2 = 1, bab^{-1} = a^{-1} \rangle$$

is the dihedral group of order 8. The set D is a $(4, 2, 4, 2)$-difference set relative to $H = \{1, a^2b\}$. The involution π_{a^2b} does not fix the point classes since $(Ha)a^2b = Ha^3 \neq Ha$. It should be noted that the design corresponding to this difference set is class regular, hence it gives rise to a Hadamard matrix of size 4. But the involution acting regularly on the points within the point classes is not the involution π_{a^2b}.

We mention this example since Ito [15] claims that H has to be a normal subgroup if there is an $(n, 2, n, \frac{n}{2})$-difference set relative to H. His claim is correct since he additionally assumes in his paper that each block Dg intersects each left coset of H in precisely one point. This assumption (which is always satisfied if H is normal) is not satisfied in our example above: In this case $|Da \cap aH| = 2$.

Many constructions of abelian (relative) difference sets are known, see [19], for instance. It seems that the non-abelian case has not attracted that much attention. But recently, very interesting observations have been published regarding non-abelian $(n, 2, n, \frac{n}{2})$-difference sets. Our focus is on a paper by Ito [16]. He conjectured that for all n divisible by 4, the so called **dicyclic group**

$$\langle a,\ b : a^n = b^4 = 1,\ a^{n/2} = b^2,\ b^{-1}ab = a^{-1}\rangle$$

contains a divisible difference set with parameters $(n, 2, n, \frac{n}{2})$. Up to now, no counterexample to Ito's conjecture is known.

In this paper, we extend a recursive construction of these dicyclic difference sets due to Schmidt [22] to a more general class of non-abelian groups. Moreover, we present new direct constructions of skew Hadamard matrices. These constructions yield new non-abelian difference sets with parameters (2) including the first series where $n-1$ is not a prime power.

In order to study difference sets it is quite handy to use group rings. In this paper we do not really use the algebraic structure of group rings and group algebras. We just use the group ring $\mathbb{Z}[G]$ as a tool which simplifies notation.

We identify a subset A of G with the element $A = \sum_{g \in A} g$ in the group ring $\mathbb{Z}[G]$. If $A = \sum_{g \in G} a_g g$ is an element in $\mathbb{Z}[G]$, we define $A^{(t)} := \sum_{g \in G} a_g g^t$. Note that this is not the t-th power of A. Using this notation, a subset D of G is an (n, m, k, λ)-difference set relative to H (where $|G| = mn$ and $|H| = m$) if and only if

$$D \cdot D^{(-1)} = k + \lambda(G - H). \tag{3}$$

If $G = \langle a : a^n = 1\rangle$ is a cyclic group of order n then $\mathbb{Z}[G] \cong \mathbb{Z}[x]/(x^n - 1)$, the ring of polynomials modulo $x^n - 1$. The canonical isomorphism is simply defined by $\psi : a^i \mapsto x^i$. If $\psi(A) = f(x)$ then $\psi(A^{(-1)})$ is just $f(x^{-1})$. This is an easy observation but it has some interesting consequences in the recursive construction of Theorem 4.1.

3. Relative difference sets and Hadamard matrices

Let G be a group of order $8t$, $K < G$ with $|K| = 4t$. Moreover, let $H = \{1, \tau\}$ be a normal subgroup of G contained in K. Let γ be an arbitrary element in $G \backslash K$. Assume that D is a $(4t, 2, 4t, 2t)$-difference set in G relative to H. We write $D = D_1 + D_2\gamma$ where $D_1 = D \cap K$ and $D_2 = D\gamma^{-1} \cap K$. The fundamental equation (3) for difference sets shows

$$(D_1 + D_2\gamma) \cdot \left(D_1^{(-1)} + \gamma^{-1} D_2^{(-1)}\right) = 4t + 2t(G - H).$$

This is equivalent to

$$D_1D_1^{(-1)} + D_2D_2^{(-1)} = 4t + 2t(K - H), \tag{4}$$

$$\text{and } D_1\big(\gamma^{-1}D_2^{(-1)}\gamma\big)\gamma^{-1} + D_2\big(\gamma D_1^{(-1)}\gamma^{-1}\big)\gamma = 2t(G - K). \tag{5}$$

The latter equation is quite complicated. Therefore we consider only a rather special type of group: We assume that K is abelian and

$$G = gr(K, \tau) := \langle K, \gamma \ : \ \gamma^2 = \tau, \ \gamma^{-1}k\gamma = k^{-1} \quad \text{for all } \ k \in K\rangle. \tag{6}$$

In this case, (5) reduces to

$$D_1D_2\gamma(1 + \tau) = 2t(G - K)$$

which is the same as

$$D_1D_2H = 2tK.$$

However, this follows already from (4): D_1 and D_2 are subsets of K of order $2t$ meeting each coset of H precisely once (otherwise the coefficient of τ on the righthand side of (4) would be $\neq 0$).

We can summarize this in the following Theorem:

Theorem 3.1 *Let K be an abelian group of order $4t$. Let $H = \{1, \tau\}$ be a subgroup of K. If K contains two subsets D_1 and D_2 which satisfy* (*4*) *then the group* $\mathrm{gr}(K, \tau)$ *defined in* (*6*) *contains a* $(4t, 2, 4t, 2t)$*-difference set $D := D_1 \cup D_2\gamma$ relative to H* (*which is a normal subgroup of* $\mathrm{gr}(K, \tau)$).

Conversely, let G be a group containing an abelian subgroup K of index 2. *If G contains a* $(4t, 2, 4t, 2t)$*-difference set D relative to H* (*$H < K$*), *then the subsets $D_1 = D \cap K$ and $D_2 = D\gamma^{-1} \cap K$ in K satisfy* (4).

A pair of subsets D_1 and D_2 defined as above is called a **pair of complementary relative difference sets**. These have been referred to as relative difference families in [1]. One may also think of these objects as a generalization of abelian $(4t, 2, 4t, 2t)$-difference sets.

Theorem 3.1 shows that the existence of a difference set in any group containing an abelian subgroup K of index 2 gives rise to a pair of complementary relative difference sets and thus a non-abelian difference set in $gr(K, \tau)$. In [22], this transformation has been carried out from the group $G \times Q_8$ into a semidirect product $G(Q_8)$ (definition below) of G with Q_8: Here

$$Q_8 = \langle x, \ y : x^4 = y^4 = 1, \ x^2 = y^2, y^{-1}xy = x^{-1}\rangle$$

is the quaternion group, G is an abelian group of order t, the forbidden subgroup is $H = \{1\} \times \langle x^2\rangle$ and $K = G \times \langle x\rangle$ is an abelian group of order $4t$. The semidirect product $G(Q_8)$ is

$$G(Q_8) := \langle K, \ y : y^2 = x^2, y^{-1}ky = k^{-1} \quad \text{for all } \ k \in K\rangle = gr(K, \ x^2).$$

It should be mentioned that difference sets in $G \times Q_8$ are equivalent to Williamson matrices with G-invariant matrices A, B, C and D, see [2] and [12]: A **Williamson matrix** is a special type of Hadamard matrix of the form

$$\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

where A, B, C and D are ± 1-matrices of size $t \times t$. Moreover, a matrix $M = (m_{(x,y)})$ is called **G-invariant** if the rows and columns are labeled by elements from G and $m_{(x,y)} = m_{(xh,yh)}$ for all $x, y, h \in G$. If G is cyclic these are the well known **circulant** matrices.

If t is odd the group $\mathbb{Z}_t(Q_8)$ is dicyclic, therefore Williamson matrices with circulant pieces of odd size can be used to verify Ito's conjecture for Hadamard matrices of size $4t$, t odd. In view of Theorem 4.2 below which generalizes Theorem 3.2 in [22] it suffices to construct relative difference sets in dicyclic groups of order $8t$ with t odd in order to check Ito's conjecture: It is always possible to multiply t by a power of 2. It is worth noting (see [15, 22]) that dicyclic relative difference sets exist which do not follow from Williamson matrices: The existence of Williamson matrices with circulant submatrices implies the existence of dicyclic difference sets. There is no construction (known) to construct Williamson matrices from dicyclic difference sets.

Using Theorem 3.1, we may rephrase Ito's conjecture as follows:

Conjecture 1 Let K be a cyclic group of order $4t$. Then K contains a pair D_1 and D_2 of complementary relative difference sets.

Note that any abelian group of order $4t$ with a pair of complementary relative difference sets gives rise to a Hadamard matrix. Therefore we may weaken Ito's conjecture:

Conjecture 2 For all integers $4t$ there exists an abelian group K of order $4t$ containing a pair of complementary relative difference sets.

We do not know whether this conjecture is easier to prove than the original one; but it also suffices to settle the long-standing Hadamard matrix conjecture.

4. Constructions of complementary relative difference sets

Solutions for (4) can be constructed from Golay complementary pairs. A **Golay complementary pair** of degree $2t-1$ is a pair of polynomials $f,\ g \in \mathbb{Z}[x]$ of degree $2t-1$. The length of the corresponding pair of sequences is $2t$. The coefficients of f and g are ± 1 and they satisfy

$$f(x)f(x^{-1}) + g(x)g(x^{-1}) = 4t \quad \text{in}\, \mathbb{Z}[x, x^{-1}].$$

Let $K = \langle a : a^{4t} = 1\rangle$ be the cyclic group of order $4t$. We define 4 subsets of K:

$$\begin{aligned}
F_+ &:= \{a^i : 0 \le i \le 2t-1,\ \text{coefficient of } x^i \text{ in } f \text{ is } +1\}\\
F_- &:= \{a^i : 0 \le i \le 2t-1,\ \text{coefficient of } x^i \text{ in } f \text{ is } -1\}\\
G_+ &:= \{a^i : 0 \le i \le 2t-1,\ \text{coefficient of } x^i \text{ in } g \text{ is } +1\}\\
G_- &:= \{a^i : 0 \le i \le 2t-1,\ \text{coefficient of } x^i \text{ in } g \text{ is } -1\}.
\end{aligned}$$

Moreover, we put

$$\begin{aligned}
F &:= F_+ + a^{2t}F_-\\
\text{and}\quad G &:= G_+ + a^{2t}G_-
\end{aligned}$$

in $\mathbb{Z}[K]$. We claim that

$$FF^{(-1)} + GG^{(-1)} = 4t + 2t(K - \langle a^{2t}\rangle), \tag{7}$$

therefore F, G is a pair of complementary relative difference sets which gives rise to a relative $(4t, 2, 4t, 2t)$-difference sets in $gr(K, a^{2t})$. Equation (7) can be easily seen using characters, see [22]. Since it is not necessary for the purpose of this paper to introduce characters, we give a more elementary though less elegant argument:

Using the definition of Golay complementary pairs and the isomorphism $\mathbb{Z}[K] \cong \mathbb{Z}[x]/(x^{4t}-1)$ we obtain

$$(F_+ - F_-)(F_+ - F_-)^{(-1)} + (G_+ - G_-)(G_+ - G_-)^{(-1)} = 4t \quad \text{in } \mathbb{Z}[K]$$

hence

$$\begin{aligned}
F_+F_+^{(-1)} + F_-F_-^{(-1)} + G_+G_+^{(-1)} + G_-G_-^{(-1)} &= 4t + F_+F_-^{(-1)}\\
+ F_-F_+^{(-1)} + G_+G_-^{(-1)} + G_-G_+^{(-1)} &=: 4t + A.
\end{aligned}$$

This shows

$$\begin{aligned}
&(F_+ + a^{2t}F_-)(F_+ + a^{2t}F_-)^{(-1)} + (G_+ + a^{2t}G_-)(G_+ + a^{2t}G_-)^{(-1)}\\
&\qquad = 4t + A + a^{2t}A.
\end{aligned}$$

Moreover,

$$\begin{aligned}
4t + 2A &= (F_+ + F_-)(F_+ + F_-)^{(-1)} + (G_+ + G_-)(G_+ + G_-)^{(-1)}\\
&= 4t + 2((2t-1)a + (2t-2)a^2 + \cdots + a^{2t-1}\\
&\quad + a^{2t+1} + 2a^{2t+2} + \cdots + (2t-1)a^{4t-1})
\end{aligned} \tag{8}$$

since

$$F_+ + F_- = G_+ + G_- = \sum_{i=0}^{2t-1} a^i.$$

Eq. (8) shows

$$A + a^{2t} A = 2t(K - \langle a^{2t} \rangle)$$

and the proof of (7) is complete.

The same argument actually proves slightly more which we summarize in the next Theorem:

Theorem 4.1 *Let K be an abelian group of order $4t$, let H be a subgroup of K with $|H| = 2$. Moreover, let T be a complete set of coset representatives of H in K, i.e., $|T| = 2t$. If there are elements*

$$F := \sum_{t \in T} f_t t$$
$$G := \sum_{t \in T} g_t t$$

in $\mathbb{Z}[K]$ with coefficients $f_t, g_t \in \{\pm 1\}$ such that

$$FF^{(-1)} + GG^{(-1)} = 4t \quad \text{in } \mathbb{Z}[K]$$

then there exists a pair of complementary relative difference sets in K.

Golay complementary pairs of degree $2t - 1$ exist whenever

$$t = 2^r \cdot 10^s \cdot 26^u$$

and it is often conjectured that pairs of other length cannot exist, see [11].

There is a nice recursive construction of relative difference sets in dicyclic groups using Golay complementary pairs ([22], Theorem 6). Actually, the construction yields complementary relative difference sets in cyclic groups. We show that this construction can be generalized to non-cyclic groups as well.

Theorem 4.2 *Let M be an abelian group of order $8tt'$. Let K be a subgroup of order $4t$ such that M/K is cyclic of order $2t'$. If there is a Golay complementary pair of degree $2t' - 1$ and if K contains complementary relative difference sets then M contains complementary relative difference sets, too.*

Proof: Let F and G denote the pair of complementary relative difference sets in K relative to $H = \{1, \tau\}$. Instead of F and G we consider $F^* = 2F - K$ and $G^* = 2G - K$:

$$F^*F^{*(-1)} + G^*G^{*(-1)} = 16t + 8t(K - H) - 8tK = 8t(1 - \tau).$$

Conversely, a pair of elements F^*, G^* in $\mathbb{Z}[K]$ with coefficients ±1 which satisfies

$$F^*F^{*(-1)} + G^*G^{*(-1)} = 8t(1 - \tau) \tag{9}$$

gives rise to a pair of complementary relative difference sets (replace -1 by 0).

Now let h be an element in M such that hK has order $2t'$ in M/K. If $f = \sum f_i x^i$ and $g = \sum g_i x^i$ is the Golay complementary pair, we put $F' := \sum f_i h^i$ and $G' := \sum g_i h^i$ in $\mathbb{Z}[M]$. We define

$$S^* := \frac{1}{2}\big[F^*(F' + G') + G^{*(-1)}(F' - G')\big],$$
$$T^* := \frac{1}{2}\big[G^*(F' + G') + F^{*(-1)}(-F' + G')\big]$$

in $\mathbb{Z}[M]$. It is not difficult to see that S^* and T^* both have coefficients ±1. We compute

$$\begin{aligned} 4\big[S^*S^{*(-1)} + T^*T^{*(-1)}\big] &= \big(F^*F^{*(-1)} + \big(G^*G^{*(-1)}\big)\big((F' + G')(F' + G')^{(-1)}\big) \\ &\quad + (F' - G')(F' - G')^{(-1)}\big) \\ &= 8t(1 - \tau)8m' \\ &= 4 \cdot (16tt'(1 - \tau)). \end{aligned}$$

This shows that S^* and T^* is a pair of complementary relative difference sets in M (when -1 is replaced by 0). □

The bad news about this recursive construction is that it gives Hadamard matrices of order $8tt'$ using a matrix of size $4t$ and a Golay pair (which itself gives rise to a Hadamard matrix of size $4t'$). It would be much nicer to have a construction of Hadamard matrices of size $4tt'$ using matrices of size $4t$ and $4t'$.

5. Skew relative difference sets and conference matrices

We now come to the investigation of conference matrices and the corresponding difference sets with parameters (2). The following proposition is obvious and contained in [22]:

Proposition 5.1 *Let K be an abelian group of order $4t$ and $H = \{1, \tau\}$ a subgroup of order 2. If D is a $(2t, 2, 2t - 1, t - 1)$-difference set relative to H and if $D \cap H = \emptyset$ (which we may assume without loss of generality, see [21]) then $D_1 = D \cup \{1\}$ and $D_2 = D \cup \{\tau\}$ is a pair of complementary relative difference sets in K.*

This proposition shows that $D \cup \{1\}$ and $D \cup \{\tau\}$ can be used to construct Hadamard matrices via Theorem 3.1, therefore the two pieces can be used to construct a $(4t, 2, 4t, 2t)$-difference set in $gr(K, \tau)$. The question arises whether it is also possible to construct a $(2t, 2, 2t, t)$-difference set directly. A candidate for such a difference set is the set $D \cup \{1\}$. We cannot expect that $D \cup \{1\}$ always is a difference set:

$$\begin{aligned}(D+1)(D+1)^{(-1)} &= DD^{(-1)} + D + D^{(-1)} + 1\\ &= 2t + (t-1)(K-H) + D + D^{(-1)}.\end{aligned}$$

This proves

Proposition 5.2 *Let D be a $(2t, 2, 2t-1, t-1)$-difference set in a not necessarily abelian group K relative to a normal subgroup H and $D \cap H = \emptyset$. Then $D \cup \{1\}$ is a $(2t, 2, 2t, t)$-difference set in K relative to H if and only if*

$$D + D^{(-1)} = K - H. \tag{10}$$

Difference sets (not necessarily with the parameters (2)) satisfying (10) are called **skew relative difference sets**.

Proposition 5.3 *If G contains a skew difference set D relative to H then $|H| \leq 2$.*

Proof: Since D intersects each coset $\neq H$ of H in G at most once, we have

$$\frac{|G|-|H|}{2} = |D| \leq \frac{|G|}{|H|} - 1 = \frac{|G|-|H|}{|H|}.$$

This shows $|H| \leq 2$. □

When $|H| = 1$, these are classical skew Hadamard difference sets and have been studied in [17, 18] and [23]. However, when $|H| = 2$, these are a new type of relative difference sets with parameters $(2t, 2, 2t-1, t-1)$. If H is normal in G then $D \cup \{1\}$ gives rise to a class regular $(2t, 2, 2t, t)$-design, hence a Hadamard matrix of size $2t$, which shows that $t = 1$ or t is even. We call these **skew Hadamard relative difference sets**.

The following theorem and its corollary are contained in [15]. It seems that this non-abelian version of Theorem 4.1.1 in [19] is not well known. Therefore we sketch the proof of Ito.

Theorem 5.4 *Let D be a relative $(2t, 2, 2t, t)$-difference set in G relative to a normal subgroup H of order 2. If t is even, the Sylow 2-subgroup S of G cannot be cyclic.*

Proof: Write $|G| = 2^k \cdot m$ where m is odd and $k \geq 3$. Assume that the Sylow 2-subgroup of G is cyclic, and let α be a generator of S. We have $H = \{\alpha^{2^{k-1}}, 1\}$. Let T be a transversal of the cosets of S in G. Then $G = \bigcup_{\beta \in T} \beta S$. We define

$$D(\beta) := \beta S \cap D$$

and we define $\gamma(i) \in H$ to be the element in N such that $\beta\alpha^i\gamma(i) \in D$. Note that $\gamma(i)$ is well defined since D meets each coset of H precisely once. We have

$$D(\beta) = \{\beta\alpha^i\gamma(i) : i = 0, \ldots, 2^{k-1} - 1\}.$$

We claim that $|D(\beta) \cap D\alpha|$ is odd which shows that $|D \cap D\alpha|$ is odd, a contradiction to t being even. Note that

$$D(\beta) \cap D\alpha = \beta S \cap D \cap D\alpha = (\beta S \cap D) \cap (\beta S \cap D\alpha) = D(\beta) \cap D(\beta)\alpha$$

which shows that we have to prove $|D(\beta) \cap D(\beta)\alpha|$ is odd. We assume

$$\gamma(0) = \gamma(2^{k-1} - 1), \tag{11}$$

the case of inequality is similar. For $i = 0, \ldots, 2^{k-1} - 2$, we have

$$\beta\alpha^j\gamma(j)\alpha \in D(\beta) \cap D(\beta)\alpha \iff \gamma(j+1) = \gamma(j)$$

which occurs for an odd number of j's, $j = 0, \ldots 2^{k-1} - 2$ in view of (11). Moreover,

$$\beta\alpha^{2^{k-1}-1}\gamma(2^{k-1} - 1)\alpha \neq \beta\alpha^{2^k}\gamma(0),$$

hence

$$\beta\alpha^{2^{k-1}-1}\gamma(2^{k-1} - 1)\alpha \notin D(\beta) \cap D(\beta)\alpha. \qquad \square$$

We note that this theorem is also contained in [13].

The following corollary shows where we have to look for skew relative difference sets.

Corollary 5.5 *If a group G contains a skew relative difference set relative to a normal subgroup H of order* 2, *then H is the unique subgroup of order* 2 *in G and the Sylow* 2*-subgroup of G is a generalized quaternion group.*

Proof: Since the relative difference set is skew symmetric, G has no element of order 2 outside H, see (10). Since the Sylow 2-subgroup cannot be cyclic, it has to be a generalized quaternion group. □

In order to use the results of the last section to search for skew relative difference sets, we have to look for $(4t, 2, 4t, 2t)$-difference sets in $gr(K, \tau)$ (see (6) for the definition of this group) where K is abelian with a cyclic Sylow 2-subgroup and τ is the unique involution in K.

Assume that D is a skew Hadamard relative difference set in $gr(K, \tau)$ where K has a cyclic Sylow 2-subgroup. We write $D = D_1 + D_2\gamma$ where γ is an element in $gr(K, \tau)$

outside K with $\gamma^2 = \tau$. Then it can be seen as before that D is a skew relative difference set in $gr(K, \tau)$ if and only if there are two subsets $D_1, D_2 \subset K$ which satisfy

$$\begin{aligned} |D_1| = 2t - 1, \quad |D_2| &= 2t, \\ D_1 + D_1^{(-1)} &= K - \langle\tau\rangle, \\ D_1 D_1^{(-1)} + D_2 D_2^{(-1)} &= 4t - 1 + (2t - 1)(K - \langle\tau\rangle). \end{aligned} \tag{12}$$

Moreover, if D_1 and D_2 satisfy the conditions above, then $D_1 + D_2\gamma$ is the skew relative difference set in $gr(K, \tau)$. We have the following analogue of Theorem 3.1:

Theorem 5.6 *Let K be an abelian group of order $4t$ with cyclic Sylow 2-subgroup. Let $H = \{1, \tau\}$ be the unique subgroup of K of order 2. If K contains two subsets D_1 and D_2 which satisfy the three conditions* (12) *then the group* $\mathrm{gr}(K, \tau)$ *contains both a skew Hadamard relative $(4t, 2, 4t - 1, 2t - 1)$-difference set $D := D_1 \cup D_2\gamma$ relative to H and a relative $(4t, 2, 4t, 2t)$-difference set $D \cup \{1\}$.*

Conversely, if $\mathrm{gr}(K, \tau)$ *contains a skew Hadamard relative $(4t, 2, 4t - 1, 2t - 1)$-difference set D relative to $H = \{1, \tau\}$, then the subsets $D_1 = D \cap K$ and $D_2 = D\gamma^{-1} \cap K$ in K satisfy* (12).

We note that the skew Hadamard relative difference sets in Theorem 5.6 immediately gives rise to a pair of complementary relative difference sets in K and therefore to Hadamard matrices.

The next theorem shows that we can construct such skew relative difference sets from arbitrary abelian $(4t, 2, 4t - 1, 2t - 1)$-difference sets in G where G is an abelian group of size $8t$ with cyclic Sylow 2-subgroup. Before we state this theorem some comments on the existence of relative $(n, 2, n - 1, \frac{n-2}{2})$-difference sets are in order.

The set of elements $\alpha \neq 0$ in $\mathbb{F}_{q^2}$ with $\alpha + \alpha^q = 1$ forms a relative $(q + 1, q - 1, q, 1)$-difference set R in the multiplicative group $\mathbb{F}_{q^2}^*$ of $\mathbb{F}_{q^2}$, i.e. in the cyclic group $\mathbb{Z}_{q^2-1}$ of order $q^2 - 1$. These difference sets are called **affine**. If q is odd, the forbidden subgroup H of order $q - 1$ has a subgroup N of order $(q - 1)/2$. It is not difficult to see that the image of R under the projection epimorphism $\mathbb{F}_{q^2}^* \to \mathbb{F}_{q^2}^*/N \cong \mathbb{Z}_{2(q+1)}$ is a cyclic relative $(q + 1, 2, q, \frac{q-1}{2})$-difference set, see [20]. These are the only cyclic examples of relative difference sets with parameters (2) and it is sometimes conjectured that no other examples exist. The corresponding conference matrices are “negacyclic”. A systematic investigation of negacyclic conference matrices is [10].

A weaker conjecture says that cyclic relative $(n, 2, n - 1, \frac{n-2}{2})$-difference sets exist only if $n - 1$ is an odd prime power. A stronger conjecture states that for any difference set with parameters (2), $n - 1$ must be a prime power. It is this conjecture which we disprove in the next Theorem.

Theorem 5.7 *Let G be an abelian group whose Sylow-2 subgroup is cyclic. Let K be the unique subgroup of G of index 2. If G contains a $(4t, 2, 4t - 1, 2t - 1)$-relative difference set, then the group* $\mathrm{gr}(K, \tau)$ *of order $8t$ and the group* $\mathrm{gr}(G, \tau)$ *of order $16t$ contain skew Hadamard relative difference sets.*

Proof: Suppose D is a $(4t, 2, 4t-1, 2t-1)$-relative difference set in G relative to the unique subgroup $H = \langle\tau\rangle$ of order 2 in G. By a multiplier theorem in [21], we may assume that D satisfies $D^{(4t-1)} = \tau D$ (this does not hold for relative $(2t, 2, 2t-1, t-1)$-difference sets). Then obviously, $D \cap H = \emptyset$. Let γ be a generator of the Sylow-2 subgroup of G. Then $G = K + \gamma K$. Similarly $D = D_1 + \gamma D_2$, where $D_1 = D \cap K$ and $D_2 = \gamma^{-1} D \cap K$. Since $|K| = 4t$ and $D^{(4t-1)} = \tau D$, we have $D_1^{(-1)} = \tau D_1$ and $D_2^{(-1)} = \tau\gamma^{2-4t} D_2$. The fact that D is a $(4t, 2, 4t-1, 2t-1)$-relative difference set implies that

$$D_1 D_1^{(-1)} + D_2 D_2^{(-1)} = (4t-1) + (2t-1)(K-H).$$

Also $D_1^{(-1)} = \tau D_1$ implies that $D_1 + D_1^{(-1)} = HD_1 = K - H$. Thus by (12) there is a skew Hadamard relative difference set in $gr(K, \tau)$.

If we set $D_1' = D_1 + \gamma^{1-2t} D_2$ and $D_2' = 1 + D_1 + \tau\gamma^{1-2t} D_2$, then D_1' and D_2' are subsets of G and it is easy to verify that $D_1'^{(-1)} + D_1' = G - H$ and $D_1' D_1'^{(-1)} + D_2' D_2'^{(-1)} = (8t-1) + (4t-1)(G-H)$. So again by (12) there is a skew Hadamard relative difference set in $gr(G, \tau)$. □

Corollary 5.8 *Difference sets with parameters* $(n,\ 2,\ n-1,\ \frac{n-2}{2})$ *exist whenever* $n-1$ *is a prime power or* $\frac{n}{2} - 1$ *is a prime power* $\equiv 3 \mod 4$.

Unfortunately, we do not know a recursive construction for the skew Hadamard relative difference sets constructed above.

We close this paper with the following question:

Question 5.9 Does every generalized quaternion group contain a skew Hadamard relative difference set?

Acknowledgments

The authors thank Prof. K. Horadam and Dr. W. de Launey for helpful suggestions. The first author's research is partially supported by NSA grant 904-01-1-0041 and NSF grant CCR-9814106. He also thanks the Alexander von Humboldt-Stiftung and the Institute for Algebra and Geometry at the Otto-von-Guericke-University Magdeburg for financial support and hospitality.

References

1. K.T. Arasu and S. Harris, "New constructions of group divisible designs," *J. Statist. Plann. Inference* **52** (1996), 241–253.
2. A. Baliga and K.J. Horadam, "Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$, *Australas. J. Comb.* **11** (1995), 67–81.
3. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Vol. 1, 2nd edition, Cambridge University Press, Cambridge, 1999.
4. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Vol. 2, 2nd edition, Cambridge University Press, Cambridge, 1999.

5. C.J. Colbourn and J.H. Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996.
6. W. de Launey, D.L. Flannery, and K.J. Horadam, "Cocyclic Hadamard matrices and difference sets," *Discrete Appl. Math.* **102** (2000), 47–61.
7. W. de Launey and K.J. Horadam, "A weak difference set construction for higher-dimensional designs," *Des. Codes Cryptogr.* **3** (1993), 75–87.
8. W. de Launey and M.J. Smith, "Cocyclic orthogonal designs and the asymptotic existence of cocyclic Hadamard matrices and maximal size relative difference sets with forbidden subgroup of size 2," *J. Comb. Theory Ser. A* **93** (2001), 37–92.
9. W. de Launey and R.M. Stafford, "On cocyclic weighing matrices and the regular group actions of certain Paley matrices," *Discrete Appl. Math.* **102** (2000), 63–101.
10. P. Delsarte, J. Goethals, and J. Seidel, "Orthogonal matrices with zero diagonal. II," *Canad. J. Math.* **23** (1971), 816–832.
11. S. Eliahou, M. Kervaire, and B. Saffari, "On Golay polynomial pairs," *Adv. Applied Math.* **12** (1991), 235–292.
12. D.L. Flannery, "Cocyclic Hadamard matrices and Hadamard groups are equivalent," *J. Algebra* **192** (1997), 749–779.
13. J.C. Galati, "On the structure of groups containing central semiregular relative difference sets," Research Report 1, Royal Melbourne Institute of Technology, 2001.
14. K.J. Horadam and W. de Launey, "Cocyclic development of designs," *J. Alg. Combin.* **2** (1993), 267–290.
15. N. Ito, "On Hadamard groups," *J. Algebra* **168** (1994), 981–987.
16. N. Ito, "On Hadamard groups III," *Kyushu J. Math.* **51** (1997), 369–379.
17. E. Johnsen, "Skew-Hadamard abelian group difference sets," *J. Algebra* **4** (1966), 388–402.
18. D. Jungnickel, "On λ-ovals and difference sets," in *Contemporary Methods in Graph Theory*, R. Bodendieck (Ed.), Bibliographisches Institut, Mannheim, 1990, pp. 429–448.
19. A. Pott, *Finite Geometry and Character Theory*, Vol. 1601 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, Heidelberg, 1995.
20. A. Pott, "A survey on relative difference sets," in *Groups, Difference Sets, and the Monster. Proceedings of a Special Research Quarter at the Ohio State University*, Spring 1993, K.T. Arasu, J. Dillon, K. Harada, S. Sehgal, and R. Solomon (Eds.), Berlin, Walter de Gruyter 1996, pp. 195–232.
21. A. Pott, D. Reuschling, and B. Schmidt, "A multiplier theorem for projections of affine difference sets," *J. Stat. Plann. Inf.* **62** (1997), 63–67.
22. B. Schmidt, "Williamson matrices and a conjecture of Ito's," *Des., Codes, Cryptogr.* **17** (1999), 61–68.
23. J. Seberry and M. Yamada, "Hadamard matrices, sequences, and block designs," in *Contemporary Design Theory*, Wiley, New York, 1992, pp. 431–560.