Construction of Baumert-Hall-Welch Arrays and T-matrices

J. Bell*

D.Z. Djokovic
Department of Pure Mathematics
University of Waterloo
Waterloo, ON Canada N2L 3G1
E-mail: dragomir@herod.uwaterloo.ca

Abstract

We show that Menon difference sets and also pairs of periodic complementary binary sequences can be used to construct BHW-arrays. We present a new method for constructing BHW-arrays over finite groups of even order. In particular we show that such arrays exist over all cyclic groups of even order $n \leq 36$.

T-matrices are constructed for infinitely many new orders, all of them even. In particular we obtain T-matrices of size 134, which were not known before. This means that BH-arrays and Hadamard matrices are constructed for infinitely many new orders.

1 Introduction

Baumert-Hall-Welch arrays (BHW-arrays) were originally defined over finite cyclic groups and the definition was extended to matrices over finite Abelian groups (also known as type 1 matrices). For any finite group G, we define the set $BHW(G)$ consisting of ordered quadruples (A_1, A_2, A_3, A_4) of 4 by 4 matrices over the group ring $\mathbf{Z}G$ such that

$$\sum_{i=1}^{4} A_i A_i^* = nI_4,$$

where n is the order of G, $A_iA_j^* + A_jA_i^* = 0$ for $i \neq j$, and satisfying some additional combinatorial conditions (see section 3 for precise definition). In the case when G is

*Supported in part by an NSERC Undergraduate Research Award.

Abelian, by applying the left regular representation φ of $\mathbf{Z}G$ to the matrix entries we obtain the BHW-array

$$\sum_{i=1}^{4} x_i \varphi(A_i),$$

as defined in [6]. BHW-arrays are used together with T-matrices to construct orthogonal designs $OD(4n; n, n, n, n)$, also known as Baumert-Hall arrays (BH-arrays). This construction is explained in section 4.

Apart from the case when G is the trivial group, only two BHW-arrays appear in the literature. The first such array was constructed by L.R. Welch in 1971 over the cyclic group C_5, and the second example was constructed by Ono, Sawade, and Yamamoto in 1984 over the group $C_3 \times C_3$.

Seberry and Yamada [12] have conjectured that BHW-arrays exist for all orders $n \equiv 1 \pmod 4$. In this paper we present a method for constructing $BHW(G)$'s over groups of even order. In particular we show that $BHW(C_n)$ exist for all even integers $n \leq 36$. We show that Menon difference sets and pairs of periodic complementary binary sequences provide new examples of $BHW(G)$'s. We also show that $BHW(C_3)$ is empty.

We construct T-matrices for infinitely many new orders. More precisely, we show that if T-matrices of order n exist, then they also exist in orders $m^k \cdot n$, where k is an arbitrary nonnegative integer and $m \in \{2, 6, 10, 14, 18, 22, 26\}$.

Notations : If A is a matrix, then $A(i,j)$ denotes its (i,j)-th entry. By A^T we denote the transpose of A. By I_n we denote the identity matrix of order n, and by J_n the matrix of order n all of whose entries are 1. A $\{\pm 1\}$-matrix is a matrix all of whose entries are ± 1.

If G is a group and $x, y \in G$, we define $\delta_{x,y}$ to be 1 if $x = y$ and 0 otherwise. By C_n we denote the cyclic group of order n (written multiplicatively).

2 Orthogonal designs

A $\{\pm 1\}$− matrix M of order n is called a *Hadamard matrix* if $MM^T = nI_n$. The existence of such M implies that n is $1, 2$, or a multiple of 4. The famous Hadamard matrix conjecture asserts that Hadamard matrices exist for all orders n which are multiples of 4. In this section we give a brief description of a particular method, invented by L. Baumert and M. Hall Jr., for constructing Hadamard matrices. This method is based on the notion of orthogonal designs which we now introduce.

Definition 1. Let $x_1, x_2, \ldots, x_k$ be independent commuting variables and A a matrix of order n whose entries are of the form $0, \pm x_1, \pm x_2, \ldots, \pm x_k$. If

$$AA^T = \left(\sum_{i=1}^{k} m_i x_i^2 \right) \cdot I_n,$$

where m_i are non-negative integers, we say that A is an *orthogonal design* of type

$$OD(n; m_1, \ldots, m_k).$$

In this paper we are interested exclusively in the orthogonal designs with parameters $OD(4n; n, n, n, n)$, which are also known as *Baumert-Hall arrays* and abbreviated as *BH-arrays*. We shall denote the set of all such arrays by $BH(4n)$.

The first example of such array was constructed by L. Baumert and M. Hall Jr.. Their example was a $BH(12)$ and they used it to construct some new Hadamard matrices (see [3] and [7, p. 221]). In order to describe this construction we introduce the following definition.

Definition 2. *Williamson type* matrices of order m are four $\{\pm1\}$-matrices W_1, W_2, W_3, W_4 of order m such that

(i) $W_i W_j^T = W_j W_i^T$ for all i, j;

(ii) $\sum_{i=1}^{4} W_i W_i^T = 4mI_m$.

Now let $A \in BH(4n)$ and let W_i, $1 \leq i \leq 4$, be Williamson type matrices of order m. Then each entry of A is $\pm x_i$ for some i, and by making the substitutions $x_i \to W_i$ we obtain from A a Hadamard matrix of order $4mn$.

The basic reference for orthogonal designs is the book [6] of Geramita and Seberry.

3 Baumert-Hall-Welch arrays

In this section we describe a special subclass of $OD(4n; n, n, n, n)$ which are known as Baumert-Hall-Welch arrays or Welch-type orthogonal designs.

Let G be a finite group of order n, written multiplicatively, with identity element 1. By $\mathbf{Z}G$ we denote its group ring over the integers $\mathbf{Z}$. The inversion map $x \to x^{-1}$ on G extends to an involutorial authomorphism of $\mathbf{Z}G$ which we denote by *. Thus we have

$$\left(\sum_{x\in G} k_x x\right)^* = \sum_{x\in G} k_x x^{-1}$$

where $k_x \in \mathbf{Z}$. This involution extends to the ring $M_k(\mathbf{Z}G)$ of k by k matrices over $\mathbf{Z}G$. Namely, if $A \in M_k(\mathbf{Z}G)$, then the matrix A^* is obtained from A by transposing A and then applying * to each of the entries. The star operation on $M_k(\mathbf{Z}G)$ is an involutorial anti-automorphism.

We say that an element $x \in \mathbf{Z}G$ is *hermitian* if $x^* = x$ and *skew-hermitian* if $x^* = -x$. A subset $X \subset G$ is called *symmetric* if $X^* = X$.

If $X \subset G$ we shall identify X with the element of $\mathbf{Z}G$ obtained by adding up all the elements of X, i.e.,

$$X = \sum_{x\in X} x \in \mathbf{Z}G.$$

Definition 3. An element $z \in \mathbf{Z}G$ is called a *combinatorial element* if it can be written as $z = X - Y$ where X and Y are disjoint subsets of G. In that case we say that $X \cup Y$ is the *support* of z. If $X \cup Y = G$, we say that z has *full support*. Two combinatorial elements are said to be *disjoint* if their supports are disjoint sets. A matrix $A \in M_k(\mathbf{Z}G)$ is called a *combinatorial matrix* if all its entries are combinatorial elements of $\mathbf{Z}G$. Two combinatorial matrices $A, B \in M_k(\mathbf{Z}G)$ are said to be *disjoint* if the entries $A(i,j)$ and $B(i,j)$ are disjoint for all i, j.

Definition 4. $BHW(G)$ is the set of ordered quadruples (A_1, A_2, A_3, A_4) of 4 by 4 combinatorial matrices over $\mathbf{Z}G$ satisfying the following conditions :

(i) A_i and A_j are disjoint for $i \neq j$;

(ii) $A_i A_i^* = nI_4 \quad , \quad 1 \leq i \leq 4$;

(iii) $A_i A_j^* + A_j A_i^* = 0$ for $i \neq j$.

If $BHW(G)$ is nonempty, we shall express this fact also by saying that $BHW(G)$ *exist*. By φ (or φ_G if that is required by the context) we denote the embedding of $\mathbf{Z}G$ into the ring $M_n(\mathbf{Z})$ of n by n integral matrices which arises from the left regular representation of G. Explicitly, for $x \in G$, $\varphi(x) \in M_n(\mathbf{Z})$ is the matrix of the left multiplication by x with respect to the basis G of $\mathbf{Z}G$, i.e.,

$$\varphi(x)(y,z) = \delta_{xz,y} \ ; \quad y, z \in G;$$

where $\delta_{x,y} = 1$ for $x = y$ and 0 otherwise.

For $x \in G$, $\varphi(x)$ is a permutation matrix and so $\varphi(x^{-1}) = \varphi(x)^T$. Consequently we have

$$\varphi(x^*) = \varphi(x)^T, \quad \forall x \in \mathbf{Z}G.$$

The ring embedding $\varphi : \mathbf{Z}G \to M_n(\mathbf{Z})$ extends naturally to an embedding of the matrix ring $M_k(\mathbf{Z}G)$ into $M_{nk}(\mathbf{Z})$. Explicitly, if $A \in M_k(\mathbf{Z}G)$, then $\varphi(A)$ is obtained from A by replacing each entry $A(i,j) \in \mathbf{Z}G$ by the matrix $\varphi(A(i,j)) \in M_n(\mathbf{Z})$. We also have

$$\varphi(A^*) = \varphi(A)^T, \quad A \in M_k(\mathbf{Z}G).$$

It is easy to verify that, if $(A_1, A_2, A_3, A_4) \in BHW(G)$, then the matrix

$$A = \sum_{i=1}^{4} x_i \varphi(A_i)$$

is an $OD(4n; n, n, n, n)$. The OD's which arise in this manner will be called *Baumert-Hall-Welch arrays*, and in abbreviated form *BHW-arrays* (see [6, 13]).

In the next section we shall need some properties of the matrix $R = R_G$ which is defined by

$$R(x,y) = \delta_{xy,1}; \quad x, y \in G.$$

Clearly R is a symmetric matrix. For $x, z \in G$ we have

$$\sum_{y \in G} R(x,y)R(y,z) = \sum_{y \in G} \delta_{xy,1}\delta_{yz,1} = \delta_{x,z},$$

i.e., $R^2 = I_n$. For $a, x, w \in G$ we have

$$\begin{aligned} \sum_{y,z \in G} R(x,y)\varphi(a)(y,z)R(z,w) &= \sum_{y,z \in G} \delta_{xy,1}\delta_{az,y}\delta_{zw,1} \\ &= \delta_{aw^{-1},x^{-1}} \\ &= \varphi(a)(x^{-1}, w^{-1}). \end{aligned}$$

In the case where G is Abelian, we have

$$\varphi(a)(x^{-1},w^{-1}) = \delta_{aw^{-1},x^{-1}} = \delta_{a^{-1}w,x} = \varphi(a^{-1})(x,w),$$

and so

$$R\varphi(a)R = \varphi(a^{-1}) = \varphi(a)^T.$$

Hence, if G is Abelian, then

$$R\varphi(x)R = \varphi(x)^T \quad , \quad \forall x \in \mathbf{Z}G.$$

4 T-partitions

In this section we explain the known procedure, due to Turyn (see [6, 13, 14]), for constructing new BH's by using BHW's. For that purpose we need another definition.

Definition 5. Let H be a finite group of order m. A *T-partition* of H is an ordered quadruple (b_1, b_2, b_3, b_4) of combinatorial elements of H such that:

(i) the supports of the b_i's form a partition of H;

(ii) $\sum_{i=1}^4 b_i b_i^* = m$.

The set of all T-partitions of H will be denoted by $TP(H)$.

If $(b_1, b_2, b_3, b_4) \in TP(H)$, with H Abelian, then the four matrices $\varphi_H(b_i)$ are known as *T-matrices* (see [6, 13]).

Theorem 1. *Let G and H be finite Abelian groups of order n and m, respectively. If $BHW(G)$ and $TP(H)$ exist, then also $BH(4mn)$ exist.*

Proof. Let $(A_1, A_2, A_3, A_4) \in BHW(G)$ and $(b_1, b_2, b_3, b_4) \in TP(H)$. Define matrices $X_k, 1 \le k \le 4$, of order mn by

$$X_k = \sum_{i,j=1}^{4} x_i \varphi_{G\times H}(A_i(j,k)b_j),$$

where $A_i(j,k)b_j$ is viewed as an element of the integral group ring of the direct product $G \times H$. We claim that

$$\sum_{k=1}^{4} X_k X_k^T = mn\left(\sum_{i=1}^{4} x_i^2\right) \cdot I_{mn}.$$

Indeed we have

$$\begin{aligned}\sum_{k=1}^{4} X_k X_k^T &= \sum_{i,j,k,r,s=1}^{4} x_i x_r \varphi_{G\times H}(A_i(j,k)b_j A_r(s,k)^* b_s^*) \\ &= \sum_{i,j,r,s=1}^{4} x_i x_r \varphi_{G\times H}(b_j b_s^* \sum_{k=1}^{4} A_i(j,k)A_r(s,k)^*).\end{aligned}$$

Since $A_iA_r^* + A_rA_i^* = 0$ for $i \neq r$ and $A_iA_i^* = nI_4$, we obtain

$$\sum_{k=1}^{4} X_kX_k^T = \sum_{i,j,s=1}^{4} x_i^2\varphi_{G\times H}(b_jb_s^* \sum_{k=1}^{4} A_i(j,k)A_i(s,k)^*)$$

$$= \sum_{i,j,s=1}^{4} \delta_{j,s}nx_i^2\varphi_{G\times H}(b_jb_s^*)$$

$$= n\left(\sum_{i=1}^{4} x_i^2\right)\cdot\varphi_{G\times H}\left(\sum_{j=1}^{4} b_jb_j^*\right)$$

$$= mn\left(\sum_{i=1}^{4} x_i^2\right)\cdot I_{mn}.$$

This proves our claim.

Each entry of the matrices X_k is one of $\pm x_1, \pm x_2, \pm x_3, \pm x_4$. We now plug these matrices into the Goethals-Seidel array

$$\begin{pmatrix} X_1 & X_2R & X_3R & X_4R \\ -X_2R & X_1 & -RX_4 & RX_3 \\ -X_3R & RX_4 & X_1 & -RX_2 \\ -X_4R & -RX_3 & RX_2 & X_1 \end{pmatrix}$$

and replace R by the matrix $R_{G\times H}$ defined in the previous section.

The resulting matrix, is a $BH(4mn)$. This follows from the following facts:

$$R^2 = I_{mn}, \quad R^T = R, \quad RX_iR = X_i^T,$$

$$X_iX_j = X_jX_i, \quad X_iX_j^T = X_j^TX_i.$$

■

5 Two examples of BHW-arrays

In this section we describe the two known examples of BHW-arrays. Let us introduce the following four auxiliary matrices:

$$\sigma_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \qquad \sigma_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

We have $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in BHW(G)$ where G is the trivial group.

The first (non-trivial) example of a BHW-array was constructed by L.R. Welch in 1971 (see [6]). In his example $G = C_5$ is a cyclic group of order 5. Let x be a generator of C_5. Define matrices A_i by

$$A_1 = \begin{pmatrix} 0 & 1 & x - x^4 & -x - x^4 \\ 1 & 0 & x + x^4 & x^4 - x \\ x^4 - x & x + x^4 & 0 & 1 \\ -x - x^4 & x - x^4 & 1 & 0 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} x^2 + x^3 & 0 & -1 & x^3 - x^2 \\ 0 & x^2 + x^3 & x^2 - x^3 & 1 \\ -1 & x^3 - x^2 & -x^2 - x^3 & 0 \\ x^2 - x^3 & 1 & 0 & -x^2 - x^3 \end{pmatrix},$$

and

$$A_3 = A_1\sigma_3 \ , \quad A_4 = A_2\sigma_3.$$

Since σ_3 commutes with A_1 and anti-commutes with A_2, it is easy to verify that $(A_1, A_2, A_3, A_4) \in BHW(C_5)$.

The second example of a BHW-array was constructed by Ono, Sawade and Yamamoto in 1984 (see [10, 12, 13]). In their example $G = C_3 \times C_3$ is the direct product of two cyclic groups of order 3 with generators x and y. The matrix

$$A_1 = A_1(x) = \begin{pmatrix} 1 + x + x^2 & x^2 - x & x^2 - x & x^2 - x \\ x - x^2 & 1 + x + x^2 & x^2 - x & x - x^2 \\ x - x^2 & x - x^2 & 1 + x + x^2 & x^2 - x \\ x - x^2 & x^2 - x & x - x^2 & 1 + x + x^2 \end{pmatrix}$$

is hermitian (i.e., $A_1^* = A_1$), satisfies the equation $A_1 A_1^* = 9I_4$, and anti-commutes with σ_2, σ_3, and σ_4. Set

$$A_2 = A_1(y)\sigma_2, \quad A_3 = A_1(xy)\sigma_3, \quad A_4 = A_1(x^2y)\sigma_4.$$

Now it is easy to check that $(A_1, A_2, A_3, A_4) \in BHW(C_3 \times C_3)$.

6 A construction for BHW-arrays

In this section we describe a particular method for constructing BHW-arrays. It is based on the following theorem.

Theorem 2. *Let G be a finite group of order n (not necessarily Abelian). Assume that there exists a combinatorial matrix A_1 whose columns are T-partitions of G and such that $A_1 A_1^* = nI_4$. Then $(A_1, A_2 = \sigma_2 A_1, A_3 = \sigma_3 A_1, A_4 = \sigma_4 A_1)$ is a $BHW(G)$. If such A_1 exists, then $n = 1$ or n is even.*

Proof. Since the columns of A_1 are T-partitions of G, the matrices A_1, A_2, A_3, A_4 are pairwise disjoint. All the other required properties of the A_i's follow immediately from $A_1 A_1^* = nI_4$ and the properties of the matrices σ_i.

Now assume that A_1 exists having the properties mentioned in the theorem. Assume that $n > 1$ is odd. By Feit-Thompson theorem, G is solvable and so $G' \neq G$. Hence G has a nontrivial 1-dimensional complex representation say, χ.

Let (s_1, s_2, s_3, s_4) be the column sums of A_1. We have

$$s_i = G - 2X_i, \quad X_i \subset G.$$

Since $A_1 A_1^* = nI_4$, we have

$$\sum_{j=1}^{4} s_j A_1(1,j)^* = n.$$

By applying χ to this equation, and by using the fact that $\chi(G) = 0$, we obtain

$$\sum_{j=1}^{4} \chi(X_i)\chi(A_1(1,j)^*) = -\frac{n}{2}.$$

As the left hand side of this equality is an algebraic integer, n must be even. ■

Recall that a subset X of cardinality k of a finite group G of order n is called a *difference set* if

$$XX^* = \lambda G + (k - \lambda) \cdot 1,$$

for some integer λ. Note that this equation implies that $k^2 = \lambda n + k - \lambda$.

A difference set is called a *Menon difference set* (or *Hadamard difference set*) if $n = 4(k - \lambda)$. It is well known that the parameters of a Menon difference set have the form

$$n = 4u^2, \quad k = 2u^2 - u, \quad \lambda = u^2 - u$$

for some integer u. It is also known that, for each u of the form $u = 2^a 3^b$ where $a, b \geq 0$ are arbitrary integers, there exists at least one Abelian group of order $n = 4u^2$ having a Menon difference set. For more information about the existence of Menon difference sets see [1, 8].

Corollary 1. *If G is a finite group of order n possessing a Menon difference set X, then $BHW(G)$ exist.*

Proof. Let (n, k, λ) be the parameters of X and recall that $n = 4(k - \lambda)$. The element $a = G - 2X$ is a combinatorial element of $\mathbf{Z}G$ with full support. We have

$$\begin{aligned} aa^* &= (G - 2X)(G - 2X^*) \\ &= (n - 4k)G + 4XX^* \\ &= (n - 4k + 4\lambda)G + 4(k - \lambda) \cdot 1 \\ &= n. \end{aligned}$$

Hence we can apply the theorem to the diagonal matrix $A_1 = aI_4$. ■

Corollary 2. *If G is a finite group having a T-partition $(a,b,0,0)$ such that $ab^* = b^*a$, then $BHW(G)$ exist.*

Proof. It suffices to observe that the matrix

$$A_1 = \begin{pmatrix} a & -b^* & 0 & 0 \\ b & a^* & 0 & 0 \\ 0 & 0 & a & -b^* \\ 0 & 0 & b & a \end{pmatrix}$$

satisfies the conditions of the theorem. ■

If $u = a+b$, $v = a-b$, i.e., $a = (u+v)/2$, $b = (u-v)/2$, then $(a,b,0,0) \in TP(G)$ if and only if u and v are combinatorial elements in $\mathbf{Z}G$ having full support and satisfying the equation

$$uu^* + vv^* = 2n. \tag{1}$$

Now let $G = C_n =< x >$ and write

$$u = \sum_{i=0}^{n-1} u_i x^i, \quad v = \sum_{i=0}^{n-1} v_i x^i$$

where all coefficients u_i and v_i are ± 1. If u and v satisfy (1), we say that the binary sequences

$$U = u_0, u_1, \ldots, u_{n-1} \text{ and } V = v_0, v_1, \ldots, v_{n-1}$$

are *two periodic complementary sequences* (PCS_2^n). This means that

$$\sum_{i=0}^{n-1} (u_i u_{i+j} + v_i v_{i+j}) = 0 \ ; \ j = 1, 2, \ldots, n-1;$$

where $u_{i+n} = u_i$ and $v_{i+n} = v_i$.

If the stronger conditions

$$\sum_{i=0}^{n-j-1} (u_i u_{i+j} + v_i v_{i+j}) = 0 \ ; \quad j = 1, 2, \ldots, n-1 \ ;$$

hold, then we say that U and V are *two aperiodic complementary sequences* (ACS_2^n) or *Golay sequences*.

It is known (see [13]) that ACS_2^n exist for all n of the form

$$n = 2^a 10^b 26^c \tag{2}$$

where a, b, c are arbitrary nonnegative integers. In addition it is known that PCS_2^{34} exist and that PCS_2^n is empty for all other values of $n < 50$ not of the form (2) (see [2, 4, 5]).

Hence $BHW(C_n)$ exist for $n = 34$ and all integers n of the form (2). For $n \leq 40$ these are the following integers:

$$n = 1, 2, 4, 8, 10, 16, 20, 26, 32, 34, 40.$$

Corollary 3. *If G is a finite Abelian group having a T-partition $(a,b,c,0)$ such that a,b, and c have symmetric supports, then $BHW(G)$ exist.*

Proof. The matrix

$$A_1 = \begin{pmatrix} a & 0 & b & c \\ 0 & a & -c^* & b^* \\ -b^* & c & a^* & 0 \\ -c^* & -b & 0 & a^* \end{pmatrix}$$

satisfies the conditions of the theorem. ∎

7 Some new BHW-arrays

In this section we show that $BHW(C_n)$ exist for $n = 6, 12, 14, 18, 22, 24$, and also that $BHW(D_3)$ exist where D_3 is the dihedral group of order 6.

In view of Theorem 2, Corollary 3, it suffices to construct T-partitions (a,b,c,d) of $C_n =< x >$ such that $d = 0$ and each of a,b,c has symmetric support. We have found many such T-partitions, but we give in Table 1 only one for each of the values listed above and also for $n = 10$ and 26.

We give now an example of a $BHW(D_3)$ where $D_3 =< x,y : x^3 = y^2 = (xy)^2 = 1 >$ the dihedral group of order 6. Let $a,b,c \in \mathbf{Z}D_3$ be defined by

$$a = (x+x^2)y,\ b = y,\ c = 1+x-x^2.$$

Then the matrix

$$A_1 = \begin{pmatrix} a & b & c & 0 \\ b & -a & 0 & c \\ c & 0 & -a & -b \\ 0 & c & -b & 0 \end{pmatrix}$$

satisfies the conditions of Theorem 2. Hence

$$(A_1, \sigma_2 A_1, \sigma_3 A_1, \sigma_4 A_1) \in BHW(D_3).$$

8 Multiplication theorems

It is well known that if $X \subset G$ and $Y \subset H$ are Menon difference sets, then

$$(X \times (H \setminus Y)) \cup ((G \setminus X) \times Y)$$

is a Menon difference set in $G \times H$. In this section we prove that several analogous results are valid for T-partitions and BHW's.

Theorem 3. *Let G and H be finite Abelian groups, $(a,b,c,d) \in TP(G)$, and $(\alpha,\beta,\gamma,\delta) \in TP(H)$. If $\alpha,\beta,\gamma,\delta$ have symmetric supports, then*

$$u = a^*\alpha + b\beta + c\gamma + d\delta,$$

Table 1

T-partitions $(a, b, c, 0)$ of C_n with symmetric supports

$n = 6$	$a = 1,\ b = x^3,\ c = x + x^{-1} + x^2 - x^{-2}$;
$n = 10$	$a = 1 + x^4 + x^{-4},\ b = x^5,$ $c = x + x^{-1} + x^2 - x^{-2} - x^3 - x^{-3}$;
$n = 12$	$a = 1 - x + x^{-1} + x^6,$ $b = x^2 + x^{-2} - x^3 + x^{-3},$ $c = -x^4 + x^{-4} + x^5 + x^{-5}$;
$n = 14$	$a = 1 + x^6 + x^{-6},\ b = x^7,$ $c = x + x^{-1} - x^2 + x^{-2} + x^3 + x^{-3} + x^4 - x^{-4} - x^5 - x^{-5}$;
$n = 18$	$a = 1 + x^3 - x^{-3} + x^7 + x^{-7} + x^8 - x^{-8},$ $b = x^5 - x^{-5} + x^6 + x^{-6} + x^9,$ $c = x + x^{-1} + x^2 - x^{-2} - x^4 - x^{-4}$;
$n = 22$	$a = 1 - x + x^{-1} - x^2 + x^{-2} + x^4 + x^{-4},$ $b = -x^7 + x^{-7} + x^8 - x^{-8} + x^9 + x^{-9} + x^{11},$ $c = -x^3 + x^{-3} + x^5 + x^{-5} - x^6 + x^{-6} + x^{10} - x^{-10}$;
$n = 24$	$a = 1 - x + x^{-1} + x^2 + x^{-2} - x^3 + x^{-3} + x^{12},$ $b = x^4 + x^{-4} - x^5 + x^{-5} - x^6 - x^{-6} - x^7 + x^{-7} + x^{10} + x^{-10},$ $c = x^8 + x^{-8} - x^9 + x^{-9} + x^{11} - x^{-11}$;
$n = 26$	$a = 1 - x^9 + x^{-9} + x^{10} + x^{-10} + x^{11} - x^{-11} + x^{12} + x^{-12},$ $b = x^2 - x^{-2} + x^4 - x^{-4} - x^6 + x^{-6} + x^8 - x^{-8} + x^{13},$ $c = x + x^{-1} + x^3 - x^{-3} - x^5 - x^{-5} + x^7 - x^{-7}.$

$$
\begin{aligned}
v &= b^*\alpha - a\beta + d\gamma^* - c\delta^*, \\
w &= c^*\alpha - d\beta^* - a\gamma + b\delta^*, \\
z &= d^*\alpha + c\beta^* - b\gamma^* - a\delta,
\end{aligned}
$$

form a T-partition of $G \times H$.

Proof. Since $\alpha, \beta, \gamma, \delta$ have symmetric supports, the elements u, v, w, z of $\mathbf{Z}(G \times H)$ are combinatorial elements with disjoint supports. A straightforward computation shows that

$$
uu^* + vv^* + ww^* + zz^* = (aa^* + bb^* + cc^* + dd^*) \cdot (\alpha\alpha^* + \beta\beta^* + \gamma\gamma^* + \delta\delta^*).
$$

As $(a, b, c, d) \in TP(G)$ and $(\alpha, \beta, \gamma, \delta) \in TP(H)$, it follows that $(u, v, w, z) \in TP(G \times H)$. ■

According to [12], among integers $n \leq 210$, T-partitions (or equivalently T-matrices) are not known for any group of order n only for the following values of n:

71, 73, 79, 83, 89, 97, 103, 107, 109, 113, 127,
131, 133, 134, 135, 137, 139, 149, 151, 157, 163,
167, 173, 179, 181, 183, 191, 193, 197, 199.

Subsequently, T-sequences of length 71 were constructed in [9]. Recall that T-matrices of order 67 are known (see [11]), while T-sequences of length 67 are still not known. We can use Theorem 3 to construct T-matrices of size 134. Hence the numbers 71 and 134 should be removed from the above list. More generally, we obtain infinitely many new orders for T-matrices, e.g. all orders $6^k \cdot 67$ with $k \geq 1$.

By reducing coefficients modulo 2, it is easy to see that if there exists (b_1, b_2, b_3, b_4) in $TP(G)$ with each b_i having symmetric support, then the order of G must be even.

Theorem 4. *Let G and H be finite groups of order n and m, respectively. Let $A_1 \in M_4(\mathbf{Z}G)$ satisfy the conditions of Theorem 2 and let $(B_1, B_2, B_3, B_4) \in BHW(H)$. Let $C_k = A_1^* B_k$, considered as a matrix over the group ring $\mathbf{Z}(G \times H)$. Then $(C_1, C_2, C_3, C_4) \in BHW(G \times H)$.*

Proof. Since $A_1 A_1^* = nI_4$ and $B_k B_k^* = mI_4$, we have $C_k C_k^* = mnI_4$. For $i \neq j$ we have $B_i B_j^* + B_j B_i^* = 0$, and so $C_i C_j^* + C_j C_i^* = 0$. The (i, j)-th entry of C_k is given by

$$
C_k(i, j) = \sum_{r=1}^{4} A_1(r, i)^* B_k(r, j).
$$

These entries are obviously combinatorial elements of $\mathbf{Z}(G \times H)$. Since the elements $B_k(r, j)$, $k = 1, 2, 3, 4$, have disjoint supports and the elements $A_1(r, i)^*$, $r = 1, 2, 3, 4$, have disjoint supports, it follows that the elements $C_k(i, j)$, $k = 1, 2, 3, 4$, have disjoint supports. ■

Theorem 5. *Let G be a finite group, H a subgroup of G of index 2 and $y \in G \setminus H$. If $(A_1, A_2, A_3, A_4) \in BHW(H)$ and*

$$B = \begin{pmatrix} 1 & y & 0 & 0 \\ -y^{-1} & 1 & 0 & 0 \\ 0 & 0 & 1 & y \\ 0 & 0 & -y^{-1} & 1 \end{pmatrix},$$

then $(A_1B, A_2B, A_3B, A_4B) \in BHW(G)$.

Proof. The verification of this assertion is straightforward. ∎

Corollary 1. *$BHW(C_n)$ exist for all even integers $n \leq 36$.*

Proof. For the cases $n = 2, 4, 8, 10, 16, 20, 26, 32$, and 34 see section 6, and for the cases $n = 6, 12, 14, 18, 22$, and 24 see section 7. The assertion in the cases $n = 28$ and 36 follows from the above theorem. For $n = 30$ we can use Theorem 4. ∎

9 $BHW(C_3)$ is empty

In this section we prove the assertion made in the title. Assume that there exists

$$(A_1, A_2, A_3, A_4) \in BHW(C_3)$$

where $C_3 = \langle x \rangle$. All the entries of the matrices A_i must be either 0 or of the form $\pm x^k$. Furthermore exactly one zero occurs in each row and column. Without any loss of generality we may assume that

$$A_1 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & -1 \\ -1 & -1 & 0 & -1 \\ -1 & 1 & -1 & 0 \end{pmatrix}.$$

This can be achieved by a transformation

$$A_i \to PA_iP^*, \quad 1 \leq i \leq 4, \tag{3}$$

where P is a suitable monomial matrix with nonzero entries of the form $\pm x^k$.

The disjointness of the A_i's implies that one of the matrices A_2, A_3, A_4 has ± 1 as its first entry. We may assume that this matrix is A_2. By replacing A_2 by $-A_2$, if necessary, we may assume that $A_2(1,1) = 1$.

Let us denote by r_1, r_2, r_3, r_4 the rows of A_1 and by s_1, s_2, s_3, s_4 those of A_2. We have $A_1A_2^* + A_2A_1^* = 0$ and hence $r_is_j^* + s_ir_j^* = 0$ for all i and j. For $i = 1$ and $j = 2$ we obtain the equation

$$A_2(2,2)^* + A_2(2,3)^* + A_2(2,4)^* - A_2(1,1) + A_2(1,3) - A_2(1,4) = 0. \tag{4}$$

By disjointness of A_1 and A_2, we know that $A_2(2,j) \neq \pm 1$ for $j \neq 2$. Since $A_2(1,1) = 1$, the above equation implies that $A_2(2,2) = 1$. Similarily, we can show that $A_2(3,3) = A_2(4,4) = 1$.

One of the entries $A_2(1,j)$, $j \neq 1$, is 0. If we perform the transformation (3) where

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

then A_1 remains invariant, the diagonal entries of A_2 remain equal 1, and the entries $A_2(1,j)$, $j \neq 1$, are permuted cyclically. Hence we may assume that $A_2(1,2) = 0$. Since the left hand side of (4) cannot have exactly three nonzero terms, it follows that $A_2(2,1) = 0$. Since each row and column of A_2 has exactly one zero, it follows that $A_2(3,4) = A_2(4,3) = 0$.

Since $A_2 A_2^* = 3I_3$, we have $s_i s_j^* = 3\delta_{ij}$. For i = 1,2 and $j = 3$ we obtain the equations :

$$\begin{aligned} A_2(3,1) &= -A_2(1,3)^*, \quad A_2(3,2) = -A_2(2,3)^*, \\ A_2(4,1) &= -A_2(1,4)^*, \quad A_2(4,2) = -A_2(2,4)^*, \end{aligned}$$

and for $i = 1$, $j = 2$ the equation

$$A_2(1,3)A_2(2,3)^* + A_2(1,4)A_2(2,4)^* = 0. \qquad (5)$$

The equation $r_1 s_3^* + s_1 r_3^* = 0$ implies that $A_2(2,3) = A_2(1,4)$, and $r_1 s_4^* + s_1 r_4^* = 0$ implies that $A_2(2,4) = -A_2(1,3)$.

The equation (5) implies that the element $A_2(1,3)A_2(1,4)^*$ is hermitian and so is ± 1. Thus $A_2(1,4) = \pm A_2(1,3)$. From $r_1 s_1^* + s_1 r_1^* = 0$, we deduce that $A_2(1,3) + A_2(1,4)$ is skew-hermitian, and so we must have $A_2(1,4) = -A_2(1,3)$.

Since $A_2(2,3) = A_2(1,4) = -A_2(1,3)$ and $A_2(2,4) = -A_2(1,3)$, the equation (4) reduces to

$$2(A_2(1,3) - A_2(1,3)^*) = 0.$$

This is impossible since $A_2(1,3)$ is $\pm x$ or $\pm x^2$. Hence we have a contradiction and the proof is completed.

References

[1] K.T. Arasu, J.A. Davis, J. Jedwab, and S.K. Sehgal, New construction of Menon difference sets, *J. Combinatorial Theory,* Series A **64** (1993), 329-336.

[2] K.T. Arasu and Q. Xiang, On the existence of periodic complementary binary sequences, *Designs, Codes and Criptography* **2** (1992), 257-262.

[3] L.D. Baumert and M.Hall, Jr., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* **68** (1962), 237-238.

[4] L. Bömer and M. Antweiler, Periodic complementary binary sequences, *IEEE Trans. Inform. Theory* **36** (1990), 1487-1494.

[5] D. Ž. Đoković , Note on periodic complementary sets of binary sequences (preprint).

[6] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, M. Dekker, New York and Basel, 1979.

[7] M. Hall, Jr., *Combinatorial Theory,* Blaisdell, 1967.

[8] D. Jungnickel, Difference sets, in *Contemporary Design Theory: A Collection of Surveys*, Eds. J.H. Dinitz and D.R. Stinson, J. Wiley, New York, 1992, p. 241-324.

[9] C. Koukouvinos, S. Kounias, J. Seberry, C.H. Yang, and J. Yang, On sequences with zero autocorrelation, *Designs, Codes and Cryptography* **4** (1994), 327-340.

[10] T. Ono and K. Sawade, A construction of Baumert-Hall-Welch array of order 36, *Sugaku* **36** (1984), 172-174.

[11] K. Sawade, A Hadamard matrix of order 268, *Graphs and Combinatorics* **1** (1985), 185-187.

[12] J. Seberry and M. Yamada, On the products of Hadamard matrices, Williamson matrices and other orthogonal matrices using M-structures, *J. Comb. Math. Comb. Comput.* **7** (1990), 97-137.

[13] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, in *Contemporary Design Theory: A Collection of Surveys,* Eds. J.H. Dinitz and D.R. Stinson, J. Wiley, New York, 1992, p. 431-560.

[14] R.J. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combinatorial Theory*, Series A **16** (1974), 313-333.

(Received 7/9/95)