Construction of Proper Higher Dimensional Hadamard Matrices from Perfect Binary Arrays

K. J. Horadam*and Cantian Lin
Department of Mathematics,
Royal Melbourne Institute of Technology,
Melbourne, VIC 3001, Australia.
horadam@rmit.edu.au

1026 McKays Court
Brentwood, TN 37027-2991, U.S.A.

Dedicated to Anne Penfold Street.

Abstract

We describe several techniques for constructing n-dimensional Hadamard matrices from 2-dimensional Hadamard matrices, and note that they may be applied to any perfect binary array (*PBA*), thus optimally improving a result of Yang. We introduce cocyclic perfect binary arrays, whose energy is not restricted to being a perfect square. These include all of Jedwab's generalised perfect binary arrays. There are many more cocyclic *PBA*s than *PBA*s. We resolve a potential ambiguity inherent in the "weak difference set" construction of n-dimensional Hadamard matrices from cocyclic *PBA*s and show it is a relative difference set construction.

1 Introduction

We describe several techniques for constructing proper n-dimensional Hadamard matrices, for arbitrarily large n, from any perfect binary array, generalised perfect binary array, or *cocyclic* perfect binary array. We reconcile

*First author supported by Australian Research Council Large Grants A69230619 and A49701206.

the two possible interpretations of the "weak difference set" construction of [8] and show that this construction derives from a relative difference set.

Much of our attention will be focussed on $\{\pm 1\}$-matrices which are *group developed* over a finite group G; that is, the rows and columns of the matrix are indexed by the elements of G (under some fixed ordering) and there is a map $\phi : G \to \{\pm 1\}$ such that the entry in position (g_1, g_2) is $\phi(g_1 g_2)$. (When columns indexed by g and $g^{-1}, \forall g \in G$ are interchanged, the resulting matrix is referred to as *group invariant*. When G is abelian, group developed matrices are also known as Type 2 matrices.)

A $v \times v$ matrix H with all entries in $\{\pm 1\}$ is called a (2-dimensional) *Hadamard* matrix of order v if $HH^T = vI$, and necessarily v must be 1, 2 or a multiple of 4. If a group developed matrix with entries in $\{\pm 1\}$ is Hadamard then it is regular and, if $v > 2$, it must be a perfect square: $v = 4t^2$. If, in a regular Hadamard matrix, the entries -1 are replaced by 0, it is the incidence matrix of a symmetric $(4t^2, 2t^2 \pm t, t^2 \pm t)$-design, and conversely. For general material on Hadamard matrices, see [18, 9].

Section 2 describes and compares known construction methods for generating higher dimensional Hadamard matrices from 2 dimensional ones. Section 3 notes that the equivalence of perfect binary arrays (*PBA*s) and abelian group developed Hadamard matrices permits construction of n-dimensional Hadamard matrices from *PBA*s (Proposition 3.4) for any $n \geq 2$, optimally improving a result of Yang [20]. In Section 4 a generalisation of group developed Hadamard matrices is used to define "cocyclic" perfect binary arrays, whose energy v is not restricted to being a perfect square. There are many more cocyclic *PBA*s than *PBA*s. In particular, all the generalised perfect binary arrays (*GPBA*s) of Jedwab [13] are included. An effective construction of proper higher dimensional Hadamard matrices from cocyclic *PBA*s is already known, but we show it has two interpretations. We clarify the definition of this construction to resolve any ambiguity. Finally we show that the reconciled construction is a relative difference set construction which generalises the difference set construction for *PBA*s. We suggest this is a profitable new area to search for binary sequences and arrays with ideal correlation properties.

2 Higher Dimensional Designs

Shlichta [16] discovered that there exist higher dimensional $\{\pm 1\}$-arrays which possess a range of orthogonality properties; in particular, he constructed 3-dimensional arrays (A_{ijk}) with the property that any sub-array obtained by fixing one index is a Hadamard matrix. In a later paper [17], he extended some of his constructions to n dimensions, and pointed out that these designs may have security coding and error-correcting coding applications. Subsequently, de Launey [6] showed that the set of proper n-dimensional Hadamard matrices of order 2 is equivalent to a coset of the first-order Reed-Muller code.

A *proper n-dimensional Hadamard matrix of order v*, for $n \geq 2$, is a $\{\pm 1\}$-array $(A(i_1, i_2, \ldots, i_n))$ with $1 \leq i_k \leq v$, $1 \leq k \leq n$, where every *section* (ie. sub-array obtained by fixing all but two indices) is a Hadamard matrix. It follows that a proper n-dimensional Hadamard matrix must have order 1, 2 or a multiple of 4.

That is, an n-dimensional $\{\pm 1\}$-array is a proper n-dimensional Hadamard matrix if, on fixing all but the k^{th} and l^{th} coordinates, letting the k^{th} coordinate take values x and y, and letting the l^{th} coordinate run from 1 to v,

$$\sum_{1 \leq i_l \leq v} A(i_1, \ldots, x, \ldots, i_l, \ldots, i_n) A(i_1, \ldots, y, \ldots, i_l, \ldots, i_n) = v\ \delta_{xy}. \quad (1)$$

A surprisingly simple method for generating a proper n-dimensional Hadamard matrix from a (2-dimensional) Hadamard matrix is due to Yang [19, Theorem 1] and de Launey [4]: if $H = (h(i,j))$ is a Hadamard matrix, then $(A(i_1, i_2, \ldots, i_n))$, where

$$A(i_1, i_2, \ldots, i_n) = \prod_{1 \leq s < t \leq n} h(i_s, i_t), \quad (2)$$

is a proper n-dimensional Hadamard matrix. (Proof follows immediately from the definitions.) We term this the *product construction.*

Hammer and Seberry [10, Theorem 4] used a different technique to construct higher dimensional Hadamard matrices. If a Hadamard matrix $(\phi(g_1 g_2))_{g_i \in G}$ is group developed over an *abelian* group G, they noted that $(A(g_1, g_2, \ldots, g_n))_{g_i \in G}$, where $A(g_1, g_2, \ldots, g_n) = \phi(g_1 g_2 \ldots g_n)$, is a proper n-dimensional Hadamard matrix.

In fact, this construction holds for non-abelian groups: if for any group G and map $\phi : G \to \{\pm 1\}$, $D = (\phi(g_1 g_2))_{g_i \in G}$ is a group developed Hadamard matrix, and

$$H_n(g_1, g_2, \ldots, g_n) = \phi(g_1 g_2 \ldots g_n),\ g_i \in G, \quad (3)$$

then every section of H_n is a Hadamard matrix. The argument is as follows. Fix the entries of H_n in all but coordinates k and l, and put $h_1 = g_1 g_2 \cdots g_{k-1}$, $h_2 = g_{k+1} g_{k+2} \cdots g_{l-1}$ and $h_3 = g_{l+1} g_{l+2} \cdots g_n$. In any section D^* obtained from H_n in this manner, the formal inner product of the two "rows" in coordinate k indexed by group elements a and b is $\sum_{c \in G} \phi(g_1 \ldots a \ldots c \ldots g_n)\ \phi(g_1 \ldots b \ldots c \ldots g_n) = \sum_{c \in G} \phi(h_1 a h_2 \ . \ c h_3)$

$\phi(h_1bh_2 \,.\, ch_3) = \sum_{C\in G}\phi(A.C)\phi(B.C) = v\delta_{AB} = v\delta_{ab}$, so D^* is also Hadamard.

We term this the *difference set construction*, by virtue of the difference set structure of an abelian group developed Hadamard matrix (Corollary 3.3 below).

If G is abelian, each section is itself group developed over G. The mapping $\phi^* : G \to \{\pm 1\}$ given by $\phi^*(a) = \phi(a \,.\, h_1h_2h_3)$, $a \in G$, shows that $D^*(a, c) = \phi(h_1ah_2ch_3) = \phi^*(ac)$. Thus we have derived the following result.

Lemma 2.1 *The difference set construction* (3) *applied to a G-developed Hadamard matrix H determines a proper n-dimensional Hadamard matrix H_n, for any $n \geq 2$. If G is abelian, H_n is proper G-developed.* □

The product and difference set constructions each have advantages and disadvantages: the product construction requires $O(n^2)$ operations to calculate each entry, while the difference set construction requires only $O(n)$ operations. However, the product construction applies to any Hadamard matrix; the difference set construction applies only to group developed Hadamard matrices (but is also applicable to other designs). For abelian group developed Hadamard matrices, the restrictiveness of this property is outlined in the next section.

More recently, de Launey [5] and de Launey and Horadam [8] introduced a variant of the difference set construction which significantly enlarges the set of Hadamard matrices to which the faster technique can be applied. The resultant proper n-dimensional Hadamard matrices have the form $(\Phi(e_1e_2 \,...\, e_n))_{e_i\in R}$, where R is a subset containing $v = |G|$ elements of a group extension E of $\{\pm 1\}$ by G, and $\Phi : E \to \{\pm 1\}$. As a consequence, calculating a single entry of these designs requires $n-1$ multiplications in E and one lookup of a table of length $|E| = 2v$; that is, $O(n)$ operations. In §4, this construction will be reviewed and redefined, and R will be identified as a $(4t, 2, 4t, 2t)$-relative difference set in E.

Although the focus of this paper is on construction of *proper* higher dimensional designs, constructions satisfying a weaker orthogonality condition than (1) are also known. In its most general form, an *n-dimensional Hadamard matrix of order v* is an array $(A(i_1, i_2, \ldots, i_n))$ with $1 \leq i_k \leq v$, $1 \leq k \leq n$ such that when the k^{th} coordinate takes values x and y,

$$\sum_{l\neq k}\sum_{i_l} A(i_1, \ldots, x, \ldots, i_l, \ldots, i_n)A(i_1, \ldots, y, \ldots, i_l, \ldots, i_n) = v^{n-1}\delta_{xy}. \tag{4}$$

For example, the Kronecker product construction can be used to create higher dimensional Hadamard matrices. If $H_1, \ldots, H_n$ are all Hadamard matrices of order v, then $H_1 \otimes \cdots \otimes H_n$ is a 2-dimensional Hadamard matrix H of order v^n, with entries $H((i_1, i_2, \ldots, i_n), (j_1, j_2, \ldots, j_n)) = H_1(i_1, j_1)H_2(i_2, j_2)\ldots H_n(i_n, j_n)$. In particular, if H_i is group developed over G_i, $1 \leq i \leq n$, then H is group developed over $G_1 \times \cdots \times G_n$.

Shlichta [17] points out that by orienting the factors of the Kronecker product in appropriate directions, it is an n-dimensional Hadamard matrix of order v^2. Equally, it can be thought of as an $2n$-dimensional Hadamard matrix of order v, on setting

$$A(i_1, j_1, i_2, j_2, \ldots, i_n, j_n) = H_1(i_1, j_1)H_2(i_2, j_2)\ldots H_n(i_n, j_n). \quad (5)$$

3 Perfect Binary Arrays

A $v \times v$ matrix $C = (c(i,j))$ is *circulant* if $c(i,j) = c(0, j-i)$, where the indices are reduced mod v. Each circulant matrix determines a back circulant matrix by column (or row) permutation. Clearly, "back circulant" means the matrix is group developed over the cyclic group $\mathbf{Z}_v$. The only known back circulant Hadamard matrices are of order 4, and it is conjectured that there is no (back) circulant Hadamard matrix of order greater than 4. For general material on circulant Hadamard matrices, Barker sequences and related topics, see [14].

Evidently, the next question to ask is if there are group developed Hadamard matrices over any other abelian groups. The answer is that an abelian group developed Hadamard matrix exists if and only if there is a corresponding perfect binary array.

Definition 3.1 An m-dimensional array $(a(i_0, \ldots, i_{m-1}))$ with $a(i_0, \ldots, i_{m-1}) = \pm 1$ for $0 \leq i_k \leq s_k - 1, 0 \leq k \leq m-1$ is called an $s_0 \times s_1 \times \ldots \times s_{m-1}$ *perfect binary array* and denoted by $PBA(s_0, \ldots, s_{m-1})$ if

$$\sum_{i_0=0}^{s_0-1} \cdots \sum_{i_{m-1}=0}^{s_{m-1}-1} a(i_0, \ldots, i_{m-1})a(i_0 + j_0, \ldots, i_{m-1} + j_{m-1})$$
$$= \prod_{i=0}^{m-1} s_i, \text{ if } j_0 = j_1 = \ldots = j_{m-1} = 0; \text{ and } = 0, \text{ otherwise} \quad (6)$$

for all $j_0, \ldots, j_{m-1}$, where the index $i_k + j_k$ is reduced mod s_k. (We assume that $\exists\ i : s_i \neq 1$.) The *energy* of the $PBA(s_0, \ldots, s_{m-1})$ is its volume $\prod_{i=0}^{m-1} s_i$.

For general material on perfect binary arrays, see [2, 13]. The energy of the $PBA(s_0, \ldots, s_{m-1})$ is $4t^2$ for some $t \geq 1$. It is well known that Menon-Hadamard difference sets over abelian groups of order $4t^2$ and nontrivial $PBAs$ are equivalent [13, Theorem 3.1].

The equivalence with abelian group developed Hadamard matrices is also apparent, since if M is group developed over $G = \mathbf{Z}_{s_0} \times \ldots \times \mathbf{Z}_{s_{m-1}}$ by the mapping $\phi : G \to \{\pm 1\}$, and its rows and columns are indexed by the lexicographically ordered elements $(i_0, \ldots, i_{m-1})$ of G, the entry in the $(i_0, \ldots, i_{m-1})^{th}$ row and $(j_0, \ldots, j_{m-1})^{th}$ column is $\phi(i_0 + j_0, \ldots, i_{m-1} + j_{m-1})$. So the inner product of the $(k_0, \ldots, k_{m-1})^{th}$ row and the $(k_0 + j_0, \ldots, k_{m-1} + j_{m-1})^{th}$ row is

$\sum_{i_0=0}^{s_0-1} \cdots \sum_{i_{m-1}=0}^{s_{m-1}-1} \phi(i_0, \ldots, i_{m-1})\ \phi(i_0 + j_0, \ldots, i_{m-1} + j_{m-1})$.

We have:

Remark 3.2 *The top row of a Hadamard matrix which is group developed over $\mathbf{Z}_{s_0} \times \ldots \times \mathbf{Z}_{s_{m-1}}$ is a $PBA(s_0, \ldots, s_{m-1})$, and vice versa.* □

For example, the top row of the $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_4$-developed Hadamard matrix of order 36:

$$++++\ +---\ +---\ ++--\ +-+-\ +--+\ -+--\ ---+\ --+-$$

where the elements are ordered lexicographically, is a $PBA(3,3,4)$.

Corollary 3.3 (This translates [13, Theorem 3.1].) *Let G be an abelian group. A G-developed $\{\pm 1\}$-matrix $(\phi(g_1 g_2))_{g_i \in G}$ is Hadamard if and only if the set $\{g \in G : \phi(g) = -1\}$ is a Menon-Hadamard $(4t^2, 2t^2 \pm t, t^2 \pm t)$-difference set in G.* □

Over the past few years, substantial effort has been made by many researchers, to find and characterise perfect binary arrays, because of their engineering applications in digital communications. Until very recently there was a paucity of positive results: there were constructions for $t = 2^a 3^b$, but many nonexistence results outside this condition. Then Xia found sufficient conditions for many more constructions having $t = 2^a 3^b w^2$, where w is the product of not necessarily distinct primes $\equiv 3 \pmod 4$, and subsequently, examples with primes $\equiv 1 \pmod 4$ have been found. See [3] for a good coverage of recent results.

In [20], Yang gives a method to construct a $(m+1)$-dimensional Hadamard matrix of order r from an m-dimensional perfect binary array $PBA(r, \ldots, r)$ of energy r^m. However, only construction in a single higher dimension will result. Furthermore, the higher dimensional Hadamard matrix so constructed will not be proper. Finally, the requirement that $r^m = 4t^2$, significantly restricts the perfect binary arrays to which his method applies.

The observations above improve Yang's result optimally. By Remark 3.2, any construction of a higher dimensional Hadamard matrix from an abelian group developed Hadamard matrix applies to the corresponding perfect binary array. This includes the Shlichta and Kronecker power (5) constructions (with factors all equal), product (2) and difference set (3) constructions. The latter two constructions determine proper n-dimensional Hadamard matrices and of these, the second is faster, and hence is preferable.

Proposition 3.4 *For any* PBA *and any $n \geq 2$, there exists an n-dimensional Hadamard matrix. In particular, by the difference set construction, if the elements of the* PBA $(s_0, \ldots, s_{m-1})$ *are $a(\vec{i})$, $\vec{i} \in \mathbf{Z}_{s_0} \times \ldots \times \mathbf{Z}_{s_{m-1}}$ with lexicographical order, then for any $n \geq 2$ a proper n-dimensional Hadamard matrix of order $4t^2 = \prod_{i=0}^{m-1} s_i$, group developed over $\mathbf{Z}_{s_0} \times \ldots \times \mathbf{Z}_{s_{m-1}}$, is given by* $A(\vec{i}, \vec{j}, \ldots, \vec{l}) = a(\vec{i} + \vec{j} + \ldots + \vec{l})$. □

Addition in $\mathbf{Z}_{s_0} \times \ldots \times \mathbf{Z}_{s_{m-1}}$ is fast to implement since it involves $n-1$ additions mod s_k in coordinate k, for each of the m coordinates.

To illustrate, consider calculation of a proper 3-dimensional Hadamard matrix from the *PBA* (3,3,4) given above. The entry $A((0,1,0),(1,0,2),(2,1,3))$, using the product construction, is $a((1,1,2))a((2,2,3))a((0,1,1)) = 1.-1.-1 = 1$; while, using the difference set construction, it is $a((0,2,1)) = -1$. So the constructions determine different 3-dimensional Hadamard matrices.

4 The Cocycle Construction

In this section we briefly describe the construction of de Launey and Horadam and clarify and update its use in extending the results for *PBAs*. First we generalise the notion of group development of designs. In [8, 11] the concept of cocyclic development of designs is introduced, in which a binary *cocyclic* matrix over a finite group G is defined to be a $\{\pm 1\}$ matrix with rows and columns indexed by the elements of G, such that the entry in position (g_1, g_2) is $\psi(g_1, g_2)\phi(g_1 g_2)$. Here $\phi : G \to \{\pm 1\}$ is a set map and $\psi : G \times G \to \{\pm 1\}$ is a (2-dimensional) *cocycle*; that is, it satisfies

$$\psi(g_1, g_2)\psi(g_1 g_2, g_3) = \psi(g_2, g_3)\psi(g_1, g_2 g_3), \quad \forall g_1, g_2, g_3 \in G. \qquad (7)$$

Note $\psi(1, g) = \psi(g, 1) = \psi(1, 1), \forall g \in G$. Any cocycle ψ determines a group extension E_ψ of $\mathbf{Z}_2 \cong \{\pm 1\}$ by G consisting of the set $E_\psi = \{(1, g),\ (-1, g) : g \in G\}$ with multiplication $(x, g)(y, h) = (\psi(g, h)xy,\ gh)$. If $\psi \equiv 1$, $E_\psi = \mathbf{Z}_2 \times G$.

Proposition 4.1 (Weak Difference Set Construction) [8, Theorem 2.7]

If a cocyclic matrix $(\psi(g_1, g_2)\phi(g_1g_2))_{g_i \in G}$ *is Hadamard, there is a proper n-dimensional Hadamard matrix* $(A(g_1, g_2, \ldots, g_n))_{g_i \in G}$ *, for any* $n \geq 2$*, where*

$$A(g_1, g_2, \ldots, g_n) = \prod_{i=2}^{n} \psi(\prod_{j=1}^{i-1} g_j, g_i)\phi(g_1g_2 \cdots g_n). \quad \square \tag{8}$$

Given ψ, any set mapping $\phi : G \to \{\pm 1\}$ determines a set mapping $\Phi_{\psi,\phi} : E_\psi \to \{\pm 1\}$, given by $\Phi_{\psi,\phi}(x, g) = x\phi(g)$. In E_ψ, $\prod_{i=1}^{n}(1, g_i) = \left(\prod_{i=2}^{n} \psi(\prod_{j=1}^{i-1} g_j, g_i),\ g_1g_2 \cdots g_n\right)$ so the right hand term in (8) is the image under $\Phi_{\psi,\phi}$ of this product of elements from the v-element subset $R = \{(1, g) : g \in G\} \subset E_\psi$. It was this derivation in terms of the set R which prompted the "weak difference set" terminology. However, as we shall see, this construction can be interpreted as a generalisation of the difference set construction in either of two ways.

Cocyclic matrices clearly specialise to group developed matrices when ψ is the trivial cocycle which always maps to 1. However group developed matrices also arise intrinsically as cocyclic matrices: the group developed matrix $(\varphi(g_1g_2))_{g_i \in G}$ is Hadamard equivalent to the normalised matrix $(\partial\varphi(g_1, g_2) = \varphi(g_1)^{-1}\varphi(g_2)^{-1}\varphi(g_1g_2))_{g_i \in G}$, and this particular type of cocycle $\partial\varphi$ is known as a *coboundary.*

Therefore, application of the weak difference set construction to a group developed Hadamard matrix determines two distinct n-dimensional Hadamard matrices.

Corollary 4.2 *Let* $H = (\varphi(g_1g_2))_{g_i \in G}$ *be a group developed Hadamard matrix over a (not necessarily abelian) group G. Then*
$(A_j(g_1, g_2, \ldots, g_n))_{g_i \in G}$, $j = 1, 2$,
is a proper n-dimensional Hadamard matrix, for any $n \geq 2$*, where*
(i) $A_1(g_1, g_2, \ldots, g_n) = \varphi(g_1g_2 \cdots g_n)$*, and*
(ii) $A_2(g_1, g_2, \ldots, g_n) = \prod_{i=2}^{n} \partial\varphi(\prod_{j=1}^{i-1} g_j, g_i)$.

Proof. (i) Set $\psi \equiv 1$ in Proposition 4.1. (ii) H is Hadamard equivalent to the coboundary matrix $(\partial\varphi(g_1, g_2))_{g_i \in G}$ which is therefore Hadamard. Set $\phi \equiv 1$ in Proposition 4.1. $\square$

The first construction, (A_1), is precisely the difference set construction (3) for an arbitrary group G. The relationship of (A_2) to this difference set construction is easily explained.

Lemma 4.3 *Let* $H = (\varphi(g_1g_2))_{g_i \in G}$ *be a group developed Hadamard matrix. Then*

$$A_2(g_1, g_2, \ldots, g_n) = (\prod_{i=1}^n \varphi(g_i)^{-1}) A_1(g_1, g_2, \ldots, g_n).$$

Proof. By definition,

$$\begin{aligned} & \prod_{i=2}^n \partial\varphi(\prod_{j=1}^{i-1} g_j, g_i) \\ = \; & \prod_{i=2}^n [\varphi(\prod_{j=1}^{i-1} g_j)^{-1} \varphi(g_i)^{-1} \varphi(\prod_{j=1}^{i} g_j)] \\ = \; & (\prod_{i=1}^n \varphi(g_i)^{-1}) \varphi(\prod_{i=1}^n g_i). \end{aligned}$$

Alternatively, there is an isomorphism $\alpha : E_{\partial\varphi} \to \mathbf{Z}_2 \times G$ given by $\alpha(x, g) = (x\varphi(g)^{-1}, g)$, so that $\Phi_{1,\varphi}(\alpha(\prod_{i=1}^n (1, g_i))) = \Phi_{\partial\varphi,1}(\prod_{i=1}^n (1, g_i))$. □

Thus, (A_2) can be thought of as a *normalised* version of (A_1), just as $(\partial\varphi)$ is the normalised version of (φ).

Similarly, alternative constructions can be applied for any cocyclic Hadamard matrix $(\psi(g_1, g_2)\varphi(g_1 g_2))_{g_i \in G}$, since it will be Hadamard equivalent to the normalised cocyclic Hadamard matrix $((\psi \cdot \partial\varphi)(g_1, g_2))_{g_i \in G}$. In order to prevent any confusion arising in application of Proposition 4.1, it is preferable to establish equivalent but simpler definitions of cocyclic matrices and the corresponding construction of higher dimensional matrices.

Definition 4.4 A binary *cocyclic* matrix over a finite group G is a $\{\pm 1\}$-matrix with rows and columns indexed by the elements of G, such that the entry in position (g_1, g_2) is $\psi(g_1, g_2)$, where $\psi : G \times G \to \{\pm 1\}$ is a cocycle (7). □

(This definition of cocyclic matrices is now in more general use.) We see that in a cocyclic matrix, the inner product of the rows indexed by elements a and b of G is $\sum_{g \in G} \psi(a, g)\psi(b, g)$. The cocyclic matrix is Hadamard if and only if

$$\sum_{g \in G} \psi(a, g)\psi(b, g) = v\, \delta_{ab}, \quad \forall a,\ b \in G. \tag{9}$$

For convenience, we assume in what follows that $|G| = 4t$, though the results below also go through analogously when $|G| = 2$.

In this situation, R is a *relative difference set* in E_ψ and Corollary 3.3 generalises. For general material on relative difference sets, see [15]. A version of the next result was known to de Launey [7] at least as early as 1993; the proof below is new.

Theorem 4.5 [de Launey] *Let G be a group of order $v = 4t$ and $\psi : G \times G \to \{\pm 1\}$ be a cocycle. The cocyclic matrix $(\psi(g_1, g_2))_{g_1, g_2 \in G}$ is Hadamard if and only if $R = \{(1, g) : g \in G\}$ is a $(4t, 2, 4t, 2t)$-relative difference set in E_ψ, relative to $\{(\pm 1, 1)\} \cong \mathbf{Z}_2$.*

Proof. By [15, pp.10-11], $R = \{(1,g) : g \in G\}$ is a $(4t, 2, 4t, 2t)$-relative difference set in E_ψ relative to $\{(\pm 1, 1)\} \cong \mathbf{Z}_2$ if and only if, in the integral group ring $\mathbf{Z}E_\psi$,

$$\begin{aligned} & \textstyle\sum_{g\in G}\sum_{h\in G}(1,g)(1,h)^{-1} \\ = \;& 4t(1,1) + 2t\textstyle\sum_{1\neq g\in G}(1,g) + 2t\sum_{1\neq g\in G}(-1,g). \end{aligned}$$

But $(1,h)^{-1} = (\psi(h,h^{-1}), h^{-1})$ in E_ψ and $\psi(h,h^{-1}) = \psi(h^{-1},h)$, so

$$\begin{aligned} & \textstyle\sum_{g\in G}\sum_{h\in G}(1,g)(1,h)^{-1} \\ = \;& \textstyle\sum_{g\in G}\sum_{h\in G}(\psi(g,h^{-1})\psi(h,h^{-1})^{-1}, gh^{-1}) \\ = \;& \textstyle\sum_{g\in G}\sum_{h\in G}(\psi(gh^{-1},h)^{-1}\psi(g,h^{-1}h), gh^{-1}) \\ = \;& \textstyle\sum_{k\in G}\sum_{h\in G}(\pm\psi(k,h)^{-1}, k) \\ = \;& 4t(1,1) + \textstyle\sum_{1\neq g\in G}(\sum_{h\in G}(\pm\psi(g,h)^{-1}, g)). \end{aligned}$$

Then the result follows since for $1 \neq g$, $\psi(g,h)^{-1}$ takes the values ± 1 equally often as h runs through G if and only if for $1 \neq g$, $\sum_{h\in G}\psi(g,h) = 0$, if and only if (by [1, Lemma 2.6]) $(\psi(g_1,g_2))_{g_1,g_2\in G}$ is Hadamard. □

In the terminology of this section, existence of a coboundary Hadamard matrix over $\mathbf{Z}_{s_0} \times \ldots \times \mathbf{Z}_{s_{m-1}}$ and existence of a $PBA(s_0,\ldots,s_{m-1})$ are equivalent. Therefore, existence of a cocyclic Hadamard matrix over a (not necessarily abelian) group G corresponds to existence of a generalised form of perfect binary array, which we will term a *cocyclic PBA*. Equation (9) is the requisite generalisation of (6). A cocyclic matrix always has a constant top row, so it is not feasible to generalise the equivalence of a *PBA* with a coboundary Hadamard matrix by using a row-based definition of a cocyclic *PBA*.

Definition 4.6 **(i)** Let G be a finite group. A *G-cocyclic perfect binary array* (*G-CPBA*) is a $\{\pm 1\}$-array $(\psi(g_1,g_2))_{g_1,g_2\in G}$ such that $\psi : G \times G \to \{\pm 1\}$ is a cocycle which also satisfies Equation (9). The *energy* of a *G-CPBA* is $|G|$.
(ii) For any $n \geq 2$, the *relative difference set construction* of a proper n-dimensional Hadamard matrix $(A(g_1,g_2,\ldots,g_n))_{g_i\in G}$ from a *G-CPBA* (ψ) is

$$A(g_1,g_2,\ldots,g_n) = \prod_{i=2}^{n}\psi(\prod_{j=1}^{i-1} g_j, g_i). \tag{10}$$

We can now state the appropriate generalisation of Proposition 3.4.

Theorem 4.7 *For any G-*CPBA *and any $n \geq 2$, there exists an n-dimensional Hadamard matrix. In particular, by the relative difference set construction, if the G-*CPBA *is (ψ), then for any $n \geq 2$ a proper n-dimensional Hadamard matrix of order 4t is given by* $A(g_1,g_2,\ldots,g_n) = \prod_{i=2}^{n}\psi(\prod_{j=1}^{i-1} g_j, g_i)$. □

G-$CPBA$s are far more numerous than PBAs. For example, there is no $PBA(9,2,2)$ but there are 3240 $\mathbf{Z}_9 \times \mathbf{Z}_2^2$-$CPBA$s with energy 36. There can be no $PBA(5,2,2)$ since 20 is not a perfect square, but there are 120 $\mathbf{Z}_5 \times \mathbf{Z}_2^2$-$CPBA$s with energy 20. Over the *non-abelian* dihedral group of the same order, $CPBA$s are even more numerous: there are 2380 D_{20}-$CPBA$s with energy 20.

Since Jedwab's generalised perfect binary arrays ($GPBA$s) are equivalent to certain abelian $(4t, 2, 4t, 2t)$-relative difference sets [13, Theorem 3.2, Result 4.9], we see that every $GPBA$ corresponds to a $CPBA$ and hence determines higher dimensional Hadamard matrices. Hughes [12] has identified this correspondence precisely. But the $GPBA$s do not account for all $CPBA$s: none of the $CPBA$s mentioned above can be $GPBA$s because the corresponding relative difference sets are not abelian.

This leads us to suggest that this is a profitable area to search for binary sequences and arrays with ideal correlation properties. Furthermore, the proper higher dimensional Hadamard matrices which arise by the relative difference set construction (10) have a hierarchy of orthogonalities which, as well as applications to security and error-correction coding, should be suitable for more general targetting problems, such as in fault-tolerant computing.

References

[1] A. Baliga and K. J. Horadam, Cocyclic matrices over $\mathbf{Z}_t \times \mathbf{Z}_2^2$, *Australas. J. Combin.*, 11 (1995), 123–134.

[2] Y.K. Chan, M.K. Siu and P. Tong, Two-dimensional binary arrays with good autocorrelation, *Inform. & Control*, 42 (1979), 125-130.

[3] J. A. Davis and J. Jedwab, A survey of Hadamard difference sets, in *Groups, Difference Sets and the Monster*, K. T. Arasu et al., eds, de Gruyter, Berlin 1996, 145–156.

[4] W. de Launey, *$(0, G)$-Designs and Applications*, Ph. D. Thesis, University of Sydney, 1987.

[5] W. de Launey, On the construction of n-dimensional designs from 2-dimensional designs, *Australas. J. Combin.*, 1 (1990), 67-81.

[6] W. de Launey, A note on N-dimensional Hadamard matrices of order 2^t and Reed-Muller codes, *IEEE Trans-IT*, 37 (1991), 664–667.

[7] W. de Launey, unpublished talk, Hadamard Centenary Conference, U. Wollongong, 1993.

[8] W. de Launey and K.J. Horadam, A weak difference set construction for higher dimensional designs, *Designs, Codes and Cryptography*, 3 (1993), 75-87.

[9] J. H. Dinitz and D. R. Stinson, Eds, *Contemporary Design Theory: A Collection of Surveys*, John Wiley & Sons, 1992.

[10] J. Hammer and J. Seberry, Higher dimensional orthogonal designs and Hadamard matrices II, *Congr. Numer.*, 27 (1979), 23-29.

[11] K. J. Horadam and W. de Launey, Cocyclic development of designs, *J. Algebraic Combinatorics* 2 (1993), 267-290.

[12] G. Hughes, Cocyclic theory of generalised perfect binary arrays, RMIT Mathematics Department Research Report No. 6, May 1998.

[13] J. Jedwab, Generalized perfect arrays and Menon difference sets, *Designs, Codes and Cryptography*, 2 (1992), 19-68.

[14] C. Lin and W. D. Wallis, Barker sequences and circulant Hadamard matrices, *Journal of Combin., Inform. & Sys. Sci.* 18 (1993), 19-25.

[15] A. Pott, *Finite Geometry and Character Theory*, LNM 1601, Springer, Berlin, 1995.

[16] P. J. Shlichta, Three and four-dimensional Hadamard matrices, *Bull. Amer. Phys. Soc.*, ser. 11, vol. 16, pp. 825-826, 1971.

[17] P.J. Shlichta, Higher dimensional Hadamard matrices, *IEEE Trans. Inform. Theory*, IT-25 (1979), 566-572.

[18] W.D. Wallis, A.P. Street and J.S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, LNM 292, Springer-Verlag, Berlin, 1972.

[19] Yang, Yi Xian, The proofs of some conjectures on higher dimensional Hadamard matrices, *Kexue Tongbao* (English translation), 31 (1986), 1662-1667.

[20] Yang, Yi Xian, Existence of one-dimensional perfect binary arrays, *Electron. Lett.*, 23 (1987), 1277-1278.