Europ. J. Combinatorics (2000) **21**, 323–331
Article No. 10.1006/eujc.1999.0349
Available online at http://www.idealibrary.com on IDEAL

Non-splitting Abelian $(4t, 2, 4t, 2t)$ Relative Difference Sets and Hadamard Cycles

G. HUGHES

Using cohomology we show that in studying the existence of an abelian non-splitting $(4t, 2, 4t, 2t)$ relative difference set, D, we can assume the groups in question have a certain simple form. We obtain an explicit constructive equivalence between generalized perfect binary arrays and cocycles that define Hadamard matrices and thereby show directly that the existence of D corresponds to that of a symmetric Hadamard matrix of a certain form. This extends the well-known equivalence in the case of splitting relative difference sets.

1. INTRODUCTION

The work of several authors has been concerned with linking cocycles with various objects of combinatorial interest such as difference sets, auto-correlated arrays and Hadamard matrices (see, for example, [1, 2, 7]). The case of a splitting $(4t, 2, 4t, 2t)$ relative difference set (RDS) in an abelian group, M, relative to an order 2 subgroup, N, is well understood. Such an RDS corresponds to a perfect binary array (PBA), an orthogonal coboundary cocycle and a group invariant Hadamard matrix. We wish to examine this correspondence in the case of non-splitting RDSs, D, with the same parameters in M relative to N. In Section 2 we introduce the necessary notation from cohomology theory and, in Section 3, define a cocycle corresponding to a particular abelian extension of an abelian group by a group of order 2. In Section 4 we review the concepts of generalized PBA (GPBA), relative difference set and Hadamard group and show that we may as well assume M and N are of a certain simple form. In particular, we may take N to be a Cartesian subgroup (that is, a subgroup of a direct factor of M). In Section 5 we present an explicit constructive equivalence between GPBAs and cocycles that determine symmetric Hadamard matrices. This equivalence allows us to show that D exists if and only if a symmetric Hadamard matrix of a particular form exists. The form is that of a group invariant matrix multiplied (elementwise) by certain 'extended' back nega-cyclic matrices.

We introduce some notation that will hold throughout this paper. If $\mathbf{u}$ is a vector we will use u_i to denote the ith component and the *weight* of the vector $\mathbf{u}$ will be the number of non-zero components of $\mathbf{u}$. Let $\mathcal{A} = \{\pm 1\}$ be a multiplicative group of order 2. If W is any group and a sequence $\{a_w : w \in W\}$ of elements of $\mathcal{A}$ has an equal number of $+1$s and -1s we write $\sum_{w \in W} a_w = 0$. Finally, any empty product is assumed to take the value 1.

2. SOME COHOMOLOGY

We summarize the results we need on cocycles with trivial action (for proofs see [6, Chapter 2]).

For groups W and V, with V abelian, we call the map $\alpha : W \times W \to V$ a *cocycle* if $\alpha(1, 1) = 1$ and $\forall x, y, z \in W$ it satisfies the equation $\alpha(x, y)\alpha(xy, z) = \alpha(y, z)\alpha(x, yz)$. A consequence of this equation is that $\forall x \in W$ we have $\alpha(x, 1) = \alpha(1, x) = 1$. The abelian group of all such cocycles under the multiplication $(\alpha\alpha')(x, y) = \alpha(x, y)\alpha'(x, y)$ is denoted $Z^2(W, V)$. If $\beta \in Z^2(W, V)$ is of the form $\beta(x, y) = \tau(x)\tau(y)(\tau(xy))^{-1} \forall x, y \in W$ for some $\tau : W \to V$ with $\tau(1) = 1$, then β is called a *coboundary* and we write $\beta = \partial\tau$.

If $\alpha, \alpha' \in Z^2(W, V)$ and $\alpha = \alpha'\partial\tau$ for some τ we say α and α' are *cohomologous* and write $\alpha \sim \alpha'$. This is an equivalence relation and the group of equivalence (cohomology) classes $\overline{\alpha}$ is denoted $H^2(W, V)$. We will call $\alpha \in Z^2(W, V)$ *symmetric* if $\forall x, y \in W$ we have $\alpha(x, y) = \alpha(y, x)$. If W and V are abelian, all coboundaries are symmetric, and the set $\text{Ext}(W, V) = \{\overline{\alpha} \in H^2(W, V) : \alpha \text{ symmetric}\}$ is a subgroup of $H^2(W, V)$.

Let $\mathbf{s} = (s_1, \dots, s_r)$ be a vector of integers greater than one and let $\mathcal{G} = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$, where $\mathbb{Z}_n$ denotes the cyclic group of integers $\{0, 1, \dots, n-1\}$ under addition mod n. Define $\gamma_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathcal{A}$ by

$$\gamma_n(l, m) = \begin{cases} 1 & \text{if } l + m < n \\ -1 & \text{if } l + m \geq n. \end{cases}$$

In this definition the addition, $l + m$, is ordinary integer addition. So, when indexed in the obvious way, γ_n gives a matrix with 1 on and above the diagonal, and -1 below the diagonal (we term this a *back nega-cyclic matrix*). We have the following facts:

(i) any non-identity cocycle $\psi \in Z^2(\mathcal{G}, \mathcal{A})$ is of order 2;
(ii) γ_n is a symmetric cocycle and is a coboundary if and only if n is odd. When n is odd, $\gamma_n = \partial v_n$ where $v_n : \mathbb{Z}_n \to \mathcal{A}$ is given by $v_n(l) = (-1)^l$;
(iii) $\text{Ext}(\mathcal{G}, \mathcal{A}) \cong \text{Ext}(\mathbb{Z}_{s_1}, \mathcal{A}) \times \cdots \times \text{Ext}(\mathbb{Z}_{s_r}, \mathcal{A})$;
(iv) if n is odd, $\text{Ext}(\mathbb{Z}_n, \mathcal{A}) = \{\overline{1}\}$, while if n is even, $\text{Ext}(\mathbb{Z}_n, \mathcal{A}) = \{\overline{1}, \overline{\gamma_n}\}$.

So we see $|\ \text{Ext}(\mathcal{G}, \mathcal{A})\ | = 2^{|E|}$ where $E = \{i : s_i \text{ even}\}$. In fact, because of the above, it is easy to describe all the representatives for the cohomology classes in $\text{Ext}(\mathcal{G}, \mathcal{A})$.

LEMMA 2.1. *Let $E = \{i : s_i$ even$\}$. The $2^{|E|}$ cocycles $\alpha_U : \mathcal{G} \times \mathcal{G} \to \mathcal{A}$ for $U \subseteq E$ defined by*

$$\alpha_U(\mathbf{x}, \mathbf{y}) = \prod_{i \in U} \gamma_{s_i}(x_i, y_i)$$

are representatives for the cohomology classes in $\text{Ext}(\mathcal{G}, \mathcal{A})$.

PROOF. α_U is certainly a symmetric cocycle so we show no two such cocycles can be cohomologous.

Let $U, U' \subseteq E$ with $U \neq U'$. Without loss of generality let $k \in U$ and $k \notin U'$. Let $\mathbf{x} = (0, \dots, 0, x_k, 0, \dots, 0)$ and $\mathbf{y} = (0, \dots, 0, y_k, 0, \dots, 0)$. Now suppose $\alpha_U = \alpha_{U'}\partial\tau$ for some $\tau : \mathcal{G} \to \mathcal{A}$. Using $\gamma_n(0, 0) = 1$ for all n we obtain $\gamma_{s_k}(x_k, y_k) = (\partial\tau_k)(x_k, y_k)$, where $\tau_k(c_k) = \tau(0, \dots, 0, c_k, 0, \dots, 0)$. However, γ_{s_k} cannot be a coboundary because s_k is even. □

Finally, we extend the definition of γ_{s_k} to $\mathcal{G} \times \mathcal{G}$ by $\gamma_{s_k}(\mathbf{x}, \mathbf{y}) = \gamma_{s_k}(x_k, y_k)$ for $\mathbf{x}, \mathbf{y} \in \mathcal{G}$. This extended function is a symmetric cocycle and will be a coboundary precisely when $\gamma_{s_k}(x_k, y_k)$ is. We will call the matrix $[\gamma_{s_k}(\mathbf{x}, \mathbf{y})]$ indexed by elements of $\mathcal{G}$ (in some fixed order) an *extended* back nega-cyclic matrix.

3. JEDWAB GROUPS AND COCYCLES

The notation introduced in this section will be used in the rest of this paper. The groups described here were used by Jedwab (see [5]) to connect generalized perfect binary arrays and relative difference sets. We will examine this connection in Section 4.

Let $\mathbf{z} = (z_1, \ldots, z_r)$ where $z_i = 0$ or 1. We call $\mathbf{z}$ a *type vector*. Let

$$G = \mathbb{Z}_{(z_1+1)s_1} \times \cdots \times \mathbb{Z}_{(z_r+1)s_r}.$$

Thus, the arithmetic in the ith coordinate of G is $\bmod 2s_i$ or $\bmod s_i$ according to whether $z_i = 1$ or $z_i = 0$. Further define the following subgroups of G,

$$\begin{aligned} H &= \{\mathbf{h} \in G : h_i = 0 \text{ if } z_i = 0;\ h_i = 0 \text{ or } s_i \text{ if } z_i = 1\}, \\ K &= \{\mathbf{k} \in H : \mathbf{k} \text{ has even weight}\}. \end{aligned}$$

We may write any $\mathbf{g} \in G$ uniquely in the form $\mathbf{g} = \boldsymbol{\ell} + \mathbf{h}$ where $\boldsymbol{\ell} \in \mathcal{G}$ and $\mathbf{h} \in H$ by taking $\boldsymbol{\ell} = \mathbf{g} \bmod \mathbf{s} = (g_1 \bmod s_1, \ldots, g_r \bmod s_r)$ and $\mathbf{h} = \mathbf{g} - \boldsymbol{\ell}$. Here, $g_i \bmod s_i$ refers to the unique residue in the range $0, \ldots, s_i - 1$.

Take $\mathbf{z} \neq \mathbf{0}$ for the moment. So $H/K = \{K, \boldsymbol{\ell}^* + K\}$, where $\boldsymbol{\ell}^*$ is any fixed vector in H of odd weight (for example $\boldsymbol{\ell}^* = (0, \ldots, 0, s_i, 0, \ldots, 0)$ where $z_i = 1$). Consider the map $\beta : G/K \to \mathcal{G}$ defined by $\beta(\mathbf{g} + K) = \mathbf{g} \bmod \mathbf{s}$. This is a well defined onto homomorphism with kernel H/K.

We now consider the following short exact sequence:

$$1 \to \mathcal{A} \xrightarrow{\iota} G/K \xrightarrow{\beta} \mathcal{G} \to 0, \tag{1}$$

where ι is the homomorphism $\iota(-1) = \boldsymbol{\ell}^* + K$ (so $\iota(\mathcal{A}) = H/K$) and β is the homomorphism above. The function $\lambda : \mathcal{G} \to G/K$ defined by $\lambda(\boldsymbol{\ell}) = \boldsymbol{\ell} + K$ is a set theoretic section of β (that is $\beta(\lambda(\boldsymbol{\ell})) = \boldsymbol{\ell}$ and $\lambda(\mathbf{0}) = K$ or, equivalently, $\lambda(\mathcal{G})$ is a complete transversal for the cosets of $\iota(\mathcal{A}) = H/K$ in G/K). We now use the section λ to define a cocycle $f_J : \mathcal{G} \times \mathcal{G} \to \mathcal{A}$ (see [6, Chapter 2]). We call this the *Jedwab cocycle corresponding to* $\mathbf{s}$ *and* $\mathbf{z}$. Let

$$\begin{aligned} \iota(f_J(\boldsymbol{\ell}, \mathbf{m})) &= \lambda(\boldsymbol{\ell}) + \lambda(\mathbf{m}) - \lambda(\boldsymbol{\ell} + \mathbf{m}) \\ &= (\boldsymbol{\ell} + \mathbf{m} - (\boldsymbol{\ell} + \mathbf{m}) \bmod \mathbf{s}) + K. \end{aligned} \tag{2}$$

So we see $f_J(\boldsymbol{\ell}, \mathbf{m}) = 1$ or -1 according to whether $\Delta = \boldsymbol{\ell} + \mathbf{m} - (\boldsymbol{\ell} + \mathbf{m}) \bmod \mathbf{s} \in K$ or $\notin K$.

Now we will write f_J in terms of the cocycles γ_{s_i} from Section 2. If $z_i = 0$, then $\Delta_i = 0$, and when $z_i = 1$ we have $\Delta_i = 0$ or s_i according to whether $l_i + m_i < s_i$ or $\geq s_i$. So, recalling the definition of γ_{s_i}, we see Δ has even weight if and only if an even number of $z_i = 1$ have $\gamma_{s_i}(l_i, m_i) = -1$, or equivalently, if and only if $\prod_{z_i=1} \gamma_{s_i}(l_i, m_i) = 1$. Therefore,

$$f_J(\boldsymbol{\ell}, \mathbf{m}) = \prod_{z_i=1} \gamma_{s_i}(l_i, m_i). \tag{3}$$

Sometimes we do not wish to distinguish between the cases $\mathbf{z} = \mathbf{0}$ and $\mathbf{z} \neq \mathbf{0}$. We will call a short exact sequence

$$1 \to \mathcal{A} \xrightarrow{\iota} \mathcal{F} \xrightarrow{\beta} \mathcal{G} \to 0, \tag{4}$$

a *Jedwab sequence* under the following circumstances:

(i) if $\mathbf{z} \neq \mathbf{0}$, sequence (4) will denote sequence (1) above;

(ii) if $\mathbf{z} = \mathbf{0}$, sequence (4) will denote the split sequence $1 \to \mathcal{A} \xrightarrow{\iota} \mathcal{G} \times \mathcal{A} \xrightarrow{\beta} \mathcal{G} \to 0$, where $\iota(a) = (\mathbf{0}, a)$ and $\beta(\boldsymbol{\ell}, a) = \boldsymbol{\ell}$.

The extension group $\mathcal{F}$, in (4), we will call the *Jedwab group corresponding to* **s** *and* **z**. The subgroup $\iota(\mathcal{A})$ we will call the corresponding *Jedwab subgroup*. In the split sequence in (ii) we use the section $\lambda(\boldsymbol{\ell}) = (\boldsymbol{\ell}, 1)$ to determine the identity cocycle $1(\boldsymbol{\ell}, \mathbf{m}) = 1$, which we may call, consistently with (3), a Jedwab cocycle.

In the following lemma, the first assertion summarizes the discussion above, and the second follows easily from Lemma 2.1.

LEMMA 3.1. *For given* **s** *and type vector* **z***:*

(i) *the Jedwab cocycle* $f_J \in Z^2(\mathcal{G}, \mathcal{A})$ *corresponding to* **s** *and* **z** *is*

$$f_J(\boldsymbol{\ell}, \mathbf{m}) = \prod_{z_i=1} \gamma_{s_i}(l_i, m_i),$$

where the product is taken to be 1 *when* $\mathbf{z} = \mathbf{0}$*;*

(ii) f_J *is symmetric,*

$$f_J \sim \prod_{z_i=1, s_i \text{ even}} \gamma_{s_i},$$

and, consequently, f_J *is a coboundary if and only if there are no* i*'s with* $z_i = 1$ *and* s_i *even.*

The form of the Jedwab cocycle means that any cohomology class in $\mathrm{Ext}(\mathcal{G}, \mathcal{A})$ can be represented by a Jedwab cocycle and, consequently, any abelian group is a Jedwab group by an isomorphism preserving the relevant order 2 subgroups. This is proved in the following results.

THEOREM 3.2. *Given* **s**, *let* $\psi \in Z^2(\mathcal{G}, \mathcal{A})$ *be a symmetric cocycle. There exists a type vector* **z** *such that* ψ *is cohomologous to* f_J, *the Jedwab cocycle corresponding to* **s** *and* **z**. *For this* **z**, *if* s_i *is odd, then* $z_i = 0$, *and* $\mathbf{z} = \mathbf{0}$ *if and only if* ψ *is a coboundary.*

PROOF. Lemma 2.1 gives $\psi \sim \prod_{i \in U} \gamma_{s_i}$ for a unique $U \subseteq \{i : s_i \text{ even}\}$. Now define **z** by $z_i = 1$ or 0 according to whether $i \in U$ or $i \notin U$. Then $f_J = \prod_{i \in U} \gamma_{s_i}$. □

The following corollary will be used in the study of relative difference sets (see Section 4).

COROLLARY 3.3. *Let* M *be an abelian group with a subgroup* $N = \langle n^* \rangle$ *of order* 2 *and write, for some* $s_i > 1$, $M/N \cong \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} = \mathcal{G}$. *Then there exists a type vector,* **z**, *such that* M *is isomorphic to the Jedwab group corresponding to* **s** *and* **z** *by an isomorphism taking* N *to the corresponding Jedwab subgroup.*

PROOF. Let $\mu : M/N \to \mathcal{G}$ be an isomorphism and consider the short exact sequence $1 \to \mathcal{A} \stackrel{\iota'}{\to} M \stackrel{\pi}{\to} \mathcal{G} \to 0$, where $\iota'(-1) = n^*$ and $\pi(m) = \mu(m + N)$. This will define a symmetric cocycle $\psi \in Z^2(\mathcal{G}, \mathcal{A})$ which, by Theorem 3.2, will be cohomologous to a Jedwab cocycle, $f_J = \prod_{z_i=1} \gamma_{s_i}$, for some **z**. Therefore, by [6, Chapter 2], the sequence above will be equivalent to the corresponding Jedwab sequence (4). So, there is an isomorphism $\Gamma : M \to \mathcal{F}$ which makes the following diagram commute:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{A} & \xrightarrow{\iota'} & M & \xrightarrow{\pi} & \mathcal{G} & \longrightarrow & 0 \\
 & & {\scriptstyle 1_{\mathcal{A}}}\big\downarrow & & {\scriptstyle \Gamma}\big\downarrow & & {\scriptstyle 1_{\mathcal{G}}}\big\downarrow & & \\
1 & \longrightarrow & \mathcal{A} & \xrightarrow{\iota} & \mathcal{F} & \xrightarrow{\beta} & \mathcal{G} & \longrightarrow & 0.
\end{array}$$

Consequently, $\Gamma(N) = \Gamma(\iota'(\mathcal{A})) = \iota(\mathcal{A})$, which is the corresponding Jedwab subgroup of $\mathcal{F}$. □

4. GPBAs and Non-splitting RDSs

In this section we review the equivalence of various combinatorial objects: generalized perfect binary arrays (GPBAs), relative difference sets (RDSs) and Hadamard groups. We show that in establishing the existence of an $(e, 2, e, e/2)$-RDS in an abelian group of order $2e$, where e is even, we can assume that the group and forbidden subgroup have a certain form.

Let M be an additively written abelian group, $N = \{0, n^*\}$ a subgroup of order 2, and e an even integer. A subset T of M is called an $(e, 2, e, e/2)$ *relative difference set* (RDS) in M relative to N if $|M| = 2e$, $|T| = e$ and for $m \in M,\ u, u' \in T$, the equation $u - u' = m$ has no solutions if $m = n^*$ and $e/2$ solutions if $m \notin N$. Such a T is a complete transversal for the cosets of N in M and N is called the *forbidden* subgroup. If such a T exists, Ito [4] calls M a *Hadamard group* with *Hadamard subset* T and shows in [4, Proposition 2] that $e = 2$ or $e = 4t$ for integral t. This can also be proved by using T to construct a Hadamard matrix of side e (see [8, p. 204]). We will look at these constructions from a cocyclic perspective in the next section. T is called a *splitting* RDS in M relative to N if M is a split extension of N (that is $M \cong N \times P$ for some subgroup P of M).

We use the following fundamental property of such an RDS, T, so often it is worth mentioning it explicitly. The proof is clear.

LEMMA 4.1. *For $m \in M$ we have $m \in T$ if and only if $m + n^* \notin T$.*

In [5, p. 24] Jedwab introduces generalized perfect binary arrays (GPBAs). We proceed to define these in terms of the groups G, H and K of Section 3.

Let $a : \mathcal{G} \to \mathcal{A}$ be any set function. As we saw in Section 3, any $\mathbf{g} \in G$ can be written as $\mathbf{g} = \boldsymbol{\ell} + \mathbf{h}$ for $\boldsymbol{\ell} = \mathbf{g} \bmod \mathbf{s} \in \mathcal{G}$ and $\mathbf{h} \in H$. The *expansion of a with respect to* $\mathbf{z}$ (which Jedwab denotes $\epsilon(a; \mathbf{z})$) is the function $a' : G \to \mathcal{A}$ defined by

$$a'(\mathbf{g}) = \begin{cases} a(\boldsymbol{\ell}) & \text{if } \mathbf{h} \in K \\ -a(\boldsymbol{\ell}) & \text{if } \mathbf{h} \notin K. \end{cases} \tag{5}$$

We call a a *GPBA*$(\mathbf{s})$ *of type* $\mathbf{z}$ if $\mathbf{g} \in G - H$ implies

$$\sum_{\mathbf{j} \in G} a'(\mathbf{j}) a'(\mathbf{g} + \mathbf{j}) = 0.$$

If $\mathbf{z} = \mathbf{0}$ the above definition reduces to: $\mathbf{0} \neq \boldsymbol{\ell} \in \mathcal{G}$ implies

$$\sum_{\mathbf{j} \in \mathcal{G}} a(\mathbf{j}) a(\boldsymbol{\ell} + \mathbf{j}) = 0. \tag{6}$$

An a with this property is called a *perfect binary array*, and is denoted by PBA$(\mathbf{s})$.

Jedwab gives the following connection between an abelian relative difference set and a GPBA.

THEOREM 4.2 ([5, THEOREM 3.2]). *Take $\mathbf{z} \neq \mathbf{0}$ and $|\mathcal{G}| = e$, an even integer. For given $a : \mathcal{G} \to \mathcal{A}$ let $D = \{\mathbf{g} + K : a'(\mathbf{g}) = 1\}$. Then, a is a GPBA$(\mathbf{s})$ of type $\mathbf{z}$ if and only if D is an $(e, 2, e, e/2)$-RDS in G/K relative to H/K.*

We should note that in fact Jedwab has $D = \{\mathbf{g} + K : a'(\mathbf{g}) = -1\}$ but this is irrelevant since a is a GPBA if and only if $-a$ is a GPBA. In view of this theorem and the remarks at the start of the section, a GPBA of non-zero type can exist only when $|\mathcal{G}| = 2$ or $4t$ for some t (see also [5, Theorem 8.1(i)]). Further, a PBA can only exist when $|\mathcal{G}| = 4t^2$ for some t (see

[5, Theorem 3.1]). Also note that D in the previous theorem is defined in terms of a given $a : \mathcal{G} \to \mathcal{A}$ but that this is not necessary. If D is any $(e, 2, e, e/2)$-RDS in G/K relative to H/K, then we can define a GPBA($\mathbf{s}$) of type $\mathbf{z}$ by $a(\boldsymbol{\ell}) = 1$ if and only if $\boldsymbol{\ell} + K \in D$.

We now use the equivalence in the above theorem and our cohomological results to show that existence questions for non-splitting $(e, 2, e, e/2)$-RDSs in abelian groups may be answered by assuming the groups in question have a 'canonical' form. In particular we may assume the forbidden subgroup is cartesian (that is, a subgroup of a direct factor).

THEOREM 4.3. *Let M be an abelian group of order $8t$, let N be a subgroup of order 2 and write, for some $s_i > 1$, $M/N \cong \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} = \mathcal{G}$. Put $s_i = 2^{a_i} t_i$ for t_i odd and let $\mathbf{z}$ be the type vector given by Corollary 3.3. Suppose M has no $\mathbb{Z}_2$ factor in its primary invariant decomposition. Then, there exists a non-splitting $(4t, 2, 4t, 2t)$-RDS in M relative to N if and only if there exists a $(4t, 2, 4t, 2t)$-RDS in $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_{i^*-1}} \times \mathbb{Z}_{2s_{i^*}} \times \mathbb{Z}_{s_{i^*+1}} \times \cdots \times \mathbb{Z}_{s_r}$ relative to $0 \times \cdots \times 0 \times < s_{i^*} > \times 0 \times \cdots \times 0$, where i^* is such that $z_{i^*} = 1$ and $a_{i^*} \geq a_i \geq 1$ for all $z_i = 1$.*

PROOF. We have $\mathbf{z} \neq \mathbf{0}$ since M is not a split extension of N. So, using Corollary 3.3, there is an isomorphism, Γ, such that $\Gamma(M)$ and $\Gamma(N)$ are the Jedwab group, G/K, and subgroup, H/K, corresponding to $\mathbf{s}$ and $\mathbf{z}$. By Theorem 4.2 the existence of a $(4t, 2, 4t, 2t)$-RDS in M relative to N is equivalent to that of a GPBA($\mathbf{s}$) of type $\mathbf{z}$. Using [5, Corollary 7.2] this, is in turn, equivalent to the existence of a GPBA($\mathbf{s}$) of type $(0^{(i^*-1)}, 1, 0, \ldots, 0)$. The result follows from another application of Theorem 4.2. □

Instead of using the equivalence of GPBAs, the result above may also be proved by observing that there is an isomorphism between G/K and $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_{i^*-1}} \times \mathbb{Z}_{2s_{i^*}} \times \mathbb{Z}_{s_{i^*+1}} \times \cdots \times \mathbb{Z}_{s_r}$ which maps H/K to the specified subgroup (this technique is used in [9] to prove the case $r = 2$). We should contrast the situation in the above theorem with that where the forbidden subgroup, N, has order larger than 2. Here it may be impossible to map N to a selected Cartesian subgroup, and the existence question cannot be simplified as shown here. Finally we note that, by taking $\mathcal{G}$ in primary invariant form, we can assume that s_{i^*} is a power of 2 in the above theorem.

5. GPBAs AND HADAMARD COCYCLES

In this section we show that a GPBA (of any type) is equivalent to a Hadamard matrix of a certain form.

If W is any finite group, a cocycle $\psi \in Z^2(W, \mathcal{A})$ is called *orthogonal* by Baliga and Horadam in [1] if the matrix $[\psi(w, w')]$, indexed by the elements of W in some fixed order, is a Hadamard matrix (so for such a cocycle to exist we need $\mid W \mid= 2$ or $4t$). Because of the defining equation of a cocycle, orthogonality amounts to the matrix having an equal number of $+1$s and -1s in each row and column not indexed by the identity of W. That is, the following result holds.

LEMMA 5.1 ([1, LEMMA 2.6]). *A cocycle $\psi \in Z^2(W, \mathcal{A})$ is orthogonal if and only if:*

(i) *for each $1 \neq v \in W$ we have $\sum_{u \in W} \psi(u, v) = 0$, or equivalently;*
(ii) *for each $1 \neq u \in W$ we have $\sum_{v \in W} \psi(u, v) = 0$.*

We will call an orthogonal cocycle a *Hadamard* cocycle to emphasize that it defines a Hadamard matrix. Specializing to $W = \mathcal{G}$ we obtain our first connection between cocycles and binary arrays. This is an explicit version of an equivalence first discussed in [3] (see also [7]).

LEMMA 5.2. *Let $\tau : \mathcal{G} \to \mathcal{A}$ be any set function. Then, $\partial\tau$ is a Hadamard cocycle if and only if τ is a PBA*($\mathbf{s}$).

PROOF. Let $\mathbf{0} \neq \boldsymbol{\ell} \in \mathcal{G}$. We have

$$\sum_{\mathbf{j}\in\mathcal{G}} \partial\tau(\mathbf{j}, \boldsymbol{\ell}) = \sum_{\mathbf{j}\in\mathcal{G}} \tau(\mathbf{j})\tau(\boldsymbol{\ell})(\tau(\boldsymbol{\ell}+\mathbf{j}))^{-1} = \tau(\boldsymbol{\ell}) \sum_{\mathbf{j}\in\mathcal{G}} \tau(\mathbf{j})\tau(\boldsymbol{\ell}+\mathbf{j}).$$

The result now follows from the previous lemma and the definition of a PBA in (6). □

A coboundary $\partial\tau$ corresponds to a group-invariant matrix (see [7]), and it is possible, whether $\partial\tau$ is a Hadamard matrix or not, when it is multiplied (elementwise) by certain extended back nega-cyclic matrices we will obtain a Hadamard matrix. This is precisely the situation that corresponds to a GPBA. We prove this by using results initially established by Flannery [2] and extended by Perera and Horadam [7], which construct canonical relative difference sets from Hadamard cocycles, and vice versa.

THEOREM 5.3. *Let $\mathbf{s}$ be any vector of integers greater than 1 and let $\mathcal{G} = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$. Let $\mathbf{z}$ be any type vector of length r, and let $f_J = \prod_{z_i=1} \gamma_{s_i}$ be the Jedwab cocycle corresponding to $\mathbf{s}$ and $\mathbf{z}$. Then $\tau : \mathcal{G} \to \mathcal{A}$ is a GPBA($\mathbf{s}$) of type $\mathbf{z}$ if and only if $\psi = f_J \partial\tau \in Z^2(\mathcal{G}, \mathcal{A})$ is Hadamard.*

PROOF. We have done the proof when $\mathbf{z} = \mathbf{0}$, so we assume this is not the case. We will use the results on the correspondence between short exact sequences and cocycles in [6, Chapter 2]. Let $\mathcal{E}$ be the extension group of $\mathcal{G}$ by $\mathcal{A}$ determined by ψ. That is, $\mathcal{E} = \{(\boldsymbol{\ell}, a) : \boldsymbol{\ell} \in \mathcal{G}, a \in \mathcal{A}\}$, where the group operation is defined for all $\boldsymbol{\ell}, \mathbf{m} \in \mathcal{G}$, $a, b \in \mathcal{A}$ by $(\boldsymbol{\ell}, a)(\mathbf{m}, b) = (\boldsymbol{\ell} + \mathbf{m}, ab\psi(\boldsymbol{\ell}, \mathbf{m}))$. We note that $\mathcal{E}$ is abelian because ψ is symmetric. We have the following short exact sequence

$$1 \to \mathcal{A} \stackrel{\iota'}{\to} \mathcal{E} \stackrel{\beta'}{\to} \mathcal{G} \to 0,$$

where $\iota'(a) = (\mathbf{0}, a)$ and $\beta'(\boldsymbol{\ell}, a) = \boldsymbol{\ell}$. Now, as $\psi \sim f_J$, the above sequence is equivalent to the Jedwab sequence (1) corresponding to f_J. Thus there is an isomorphism that makes the following diagram commute:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{A} & \stackrel{\iota'}{\longrightarrow} & \mathcal{E} & \stackrel{\beta'}{\longrightarrow} & \mathcal{G} & \longrightarrow & 0 \\ & & {\scriptstyle 1_{\mathcal{A}}}\downarrow & & {\scriptstyle \Gamma}\downarrow & & {\scriptstyle 1_{\mathcal{G}}}\downarrow & & \\ 1 & \longrightarrow & \mathcal{A} & \stackrel{\iota}{\longrightarrow} & G/K & \stackrel{\beta}{\longrightarrow} & \mathcal{G} & \longrightarrow & 0. \end{array}$$

We see that $\Gamma(\iota'(\mathcal{A})) = \iota(\mathcal{A}) = H/K = \{K, \boldsymbol{\ell}^* + K\}$. The isomorphism is given explicitly by

$$\Gamma(\boldsymbol{\ell}, a) = \iota(a\tau(\boldsymbol{\ell})) + \lambda(\boldsymbol{\ell}),$$

where $\lambda : \mathcal{G} \to G/K$ is the section of β given by $\lambda(\boldsymbol{\ell}) = \boldsymbol{\ell} + K$ in Section 3.

Now let $\mathcal{D} = \{(\boldsymbol{\ell}, 1) : \boldsymbol{\ell} \in \mathcal{G}\}$ and $D = \{\mathbf{g} + K : \tau'(\mathbf{g}) = 1\}$. Assume, *for the moment*, that $D = \Gamma(\mathcal{D})$. By Theorem 4.2, τ is a GPBA($\mathbf{s}$) of type $\mathbf{z}$ if and only if D is a $(4t, 2, 4t, 2t)$-RDS in G/K relative to H/K. By the isomorphism, Γ, these are then equivalent to $\mathcal{D} = \Gamma^{-1}(D)$ being a $(4t, 2, 4t, 2t)$-RDS in $\mathcal{E} = \Gamma^{-1}(G/K)$ relative to $\iota'(\mathcal{A}) = 0 \times \mathcal{A} = \Gamma^{-1}(H/K)$.

Finally, [7, Theorem 4.1] tells us that $\mathcal{D}$ is such an RDS if and only if ψ is a Hadamard cocycle.

It only remains to prove that $D = \Gamma(\mathcal{D})$. Recall the definition of the expansion, τ', in (5). Suppose, firstly, that $\tau'(\mathbf{g}) = 1$, and write $\mathbf{g} = \boldsymbol{\ell} + \mathbf{h}$ for $\mathbf{h} \in H$ and $\boldsymbol{\ell} = \mathbf{g} \bmod \mathbf{s}$. Then $\tau(\boldsymbol{\ell}) = 1$ if and only if $h \in K$, and so $\mathbf{g} + K = \boldsymbol{\ell} + \mathbf{h} + K = \iota(\tau(\boldsymbol{\ell})) + \boldsymbol{\ell} + K \in \Gamma(\mathcal{D})$. Conversely, let $\boldsymbol{\ell} \in \mathcal{G}$ and write $\tau(\boldsymbol{\ell}) = (-1)^\epsilon$, where $\epsilon = 0, 1$. Then $\Gamma(\boldsymbol{\ell}, 1) = \epsilon\boldsymbol{\ell}^* + \boldsymbol{\ell} + K$ and $\tau'(\epsilon\boldsymbol{\ell}^* + \boldsymbol{\ell}) = (-1)^\epsilon\tau(\boldsymbol{\ell}) = 1$. □

We now give an example to illustrate the construction of the orthogonal cocycle $f_J\partial\tau$ from τ in Theorem 5.3.

EXAMPLE 5.4. Let $\mathbf{s} = (2, 2)$ and $\mathbf{z} = (1, 0)$. Order the elements of $\mathcal{G} = \mathbb{Z}_2 \times \mathbb{Z}_2$ as follows: 00, 10, 01, 11. Let $\tau : \mathcal{G} \to \mathcal{A}$ be given by $\tau(00) = \tau(10) = \tau(01) = 1$ and $\tau(11) = -1$. It is easily checked that τ is a GPBA(2,2) of type (1,0). The corresponding cocycle $\gamma_{s_1}\partial\tau = \psi$ is the component-wise product matrix

$$\begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & + & + \\ + & - & + & - \end{pmatrix} \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{pmatrix} = \begin{pmatrix} + & + & + & + \\ + & - & - & + \\ + & - & + & - \\ + & + & - & - \end{pmatrix},$$

which is, indeed, a Hadamard matrix. In this example we note that $\partial\tau$ itself is Hadamard. This is because τ is a PBA(2,2). However, there are many examples where τ is a GPBA of non-zero type but not a PBA (that is where $f_J\partial\tau$ is Hadamard but $\partial\tau$ is not). For example, $\tau \equiv 1$ is a GPBA(2,2, ... ,2) of type (1,1, ... ,1) since $\psi = \gamma_2^r$ defines the Sylvester Hadamard matrix,

$$\begin{pmatrix} + & + \\ + & - \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} + & + \\ + & - \end{pmatrix},$$

where $\otimes$ denotes the Kronecker, or tensor, product of matrices. Clearly τ is not a PBA(2,2, ... ,2). □

Now let M be any abelian group of order $8t$ and N any subgroup of order 2. The existence of a splitting $(4t, 2, 4t, 2t)$-RDS in M relative to N is well known to be equivalent to that of a PBA and, hence, to that of a Hadamard coboundary. In other words, such splitting RDSs correspond to Hadamard matrices determined by the trivial cohomology class. For a non-splitting RDS of the same parameters in M relative to N we can combine Theorem 5.3 with Theorems 4.2 and 4.3 to obtain a generalization of this equivalence. It shows that these non-splitting RDSs correspond to Hadamard matrices determined by non-trivial symmetric cohomology classes in $H^2(M/N, \mathcal{A})$.

COROLLARY 5.5. *Let $\mathcal{G}$ and i^* be as in Theorem 4.3. Then, there is a non-splitting $(4t, 2, 4t, 2t)$-RDS in M relative to N if and only if the cocycle $\gamma_{s_{i^*}}\partial\tau$ is Hadamard for some $\tau : \mathcal{G} \to \mathcal{A}$.*

ACKNOWLEDGEMENT

The author would like to thank Professor Kathy Horadam for many helpful discussions and insights.

REFERENCES

1. A. Baliga and K. J. Horadam, Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$, *Aust. J. Comb.*, **11** (1995), 123–134.
2. D. L. Flannery, Cocyclic Hadamard matrices and Hadamard groups are equivalent, *J. Algebra*, **192** (1997), 749–779.
3. K. J. Horadam, D. L. Flannery and W. de Launey, Cocyclic Hadamard matrices and difference sets, Research Report No. 2, Royal Melbourne Institute of Technology, Department of Mathematics, 1997.
4. N. Ito, On Hadamard groups, *J. Algebra*, **168** (1994), 981–987.
5. J. Jedwab, Generalized perfect arrays and Menon difference sets, *Des. Codes Cryptogr.*, **2** (1992), 19–68.
6. G. Karpilovsky, *Projective Representations of Finite Groups*, Marcel Dekker, New York, 1985.
7. A. A. I. Perera and K. J. Horadam, Cocyclic generalised Hadamard matrices and central relative difference sets, *Des. Codes Cryptogr.*, **15** (1998), 187–200.
8. A. Pott, A survey on relative difference sets, in: *Groups, Difference Sets and the Monster*, K. T. Arasu *et al*. (ed.), de Gruyter, Berlin, 1996.
9. P. Wild, Infinite families of perfect binary arrays, *Electron. Lett.*, **24** (1988), 845–847.

Received 12 January 1999 and accepted in revised form 8 September 1999

G. HUGHES
Department of Mathematics,
Royal Melbourne Institute of Technology,
GPO Box 2476V, Melbourne, VIC 3001,
Australia