On the Asymptotic Existence of Cocyclic Hadamard Matrices

Warwick de Launey
Center for Communications Research
4320 Westerra Court
La Jolla CA92121, USA

H. Kharaghani*
Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta, T1K3M4
Canada

March 12, 2009

Abstract

Let q be an odd natural number. We prove there is a cocyclic Hadamard matrix of order $2^{10+t}q$ whenever $t \geq 8\lfloor \frac{\log_2(q-1)}{10} \rfloor$. We also show that if the binary expansion of q contains N ones, then there is a cocyclic Hadamard matrix of order $2^{4N-2}q$.

1 Introduction

In the early 1990's, de Launey and Horadam [7] noted that many of the familiar constructions for Hadamard matrices imposed a special kind of regular group action on the resulting design. Eventually [2, 3, 6] it became clear that such a group action made the Hadamard matrix equivalent to a maximal-sized, relative difference set with a central forbidden subgroup of order two. Such Hadamard matrices are said to be cocyclic because they have an associated 2-cocycle. The wide applicability of the cocyclic difference method was exciting news because suddenly the algebraic machinery of difference methods could be brought to bear on the Hadamard conjecture. In fact, de Launey and

*Supported by an NSERC Discovery Grant - Group.

Horadam [4] conjectured that there is a cocyclic Hadamard matrix of order $4t$ for all integers $t \geq 1$. This conjecture is called the cocyclic Hadamard conjecture.

Let q be an odd natural number. Towards the end of the paper [5] de Launey and Smith adapted ideas of Seberry [8] to prove that there is a cocyclic Hadamard matrix of order $2^t q$ whenever $t \geq \lfloor 8 \log_2 q \rfloor$. This asymptotic existence result was additional evidence in favor of the cocyclic Hadamard conjecture, but the exponent of 2 required was almost four times Seberry's original bound $2\log_2(q-3)$, and far larger than the best known cut-off value $5 + 4\lfloor \frac{\log_2(q-1)}{10} \rfloor$ for general Hadamard matrices. In this paper, we adapt the ideas of [1] to show that there is a cocyclic Hadamard matrix of order $2^t q$ whenever $t \geq 10 + 8\lfloor \frac{\log_2(q-1)}{10} \rfloor$.

The construction method of [1] has the following overall pattern. Fix an odd integer $q = 2p+1$, where $p > 1$. First, $2M$ paired complementary sequences of combined length $2p$ are constructed. Second, these sequences are used to make Hermitian and skew-Hermitian circulant matrices whose supports disjointly cover all off-diagonal entries in a $q \times q$ array. Third, these circulants are combined with signed permutation matrices with special pairwise amicability and anti-amicability properties to form the desired (complex) Hadamard matrix.

In order to adapt the ideas of [1] to obtain a cocyclic Hadamard matrix, we must see how each of the above steps needs to be altered to ensure that the resulting complex Hadamard matrix is cocyclic. It happens that nothing needs to be done in the first two steps. The third step requires fundamental changes, but luckily all of the underlying theory needed has been worked out in [5]. So it is sufficient to assemble the necessary components from the papers [1] and [5]. However, there are aspects of the theory which are not spelt out in [5] as explicitly as we need here, and there are minor errors in both papers [1] and [5] which need to be corrected. So in this paper, we have tried to give a direct and self-contained exposition.

The rest of this paper is organized as follows. In the next section, we discuss cocycles and cocyclic matrices. In Section 3, we obtain the set of cocyclic signed permutation matrices together with a Hadamard matrix with the same cocycle. In Section 4, we cover sequences. In Section 5, we show how to obtain the Hermitian and skew-Hermitian circulants from the sequences given in Section 4. In Section 6, we put all the material together to obtain the cocyclic Hadamard matrices. In Section 7, we discuss the implications of our results, and suggest avenues for further research.

2 Preliminaries

In this paper, we will need to construct a set of $n \times n$ cocyclic signed permutation matrices $P_0, P_1, \ldots, P_{t-1}, Q_0, Q_1, \ldots, Q_{s-1}$ and a Hadamard matrix H of order n such that for all $i = 0, 1, \ldots, t-1$, and $j = 0, 1, \ldots, s-1$,

(I) there is a 2-cocycle $f : G \times G \to \langle -1 \rangle$ and maps $g, g_i, h_j : G \to \{0, \pm 1\}$ such that

$H = [f(x,y)g(xy)]_{x,y\in G}$, $P_i = [f(x,y)g_i(xy)]_{x,y\in G}$ and $Q_j = [f(x,y)h_j(xy)]_{x,y\in G}$,

(II) $P_0, P_1, \ldots, P_{t-1}$ are pairwise anti-amicable (i.e., $P_i P_j^\top = -P_j P_i^\top$ for $i \neq j$),

(III) $Q_0, Q_1, \ldots, Q_{s-1}$ are pairwise anti-amicable,

(IV) $P_i Q_j^\top = Q_j P_i^\top$.

The paper [5] shows that for each pair $s,t \geq 2$ the smallest value of n is a power of 2. Moreover, it contains all the ingredients for a method for computing that power of 2, and constructing the matrices H, P_i, Q_j. However, the paper [5] does not give an explicit method, and we will need to construct these matrices for all $t = s = 2M+1$, where $M > 0$. So in this paper, we will give an explicit method, using the ideas of [5], to construct these matrices. Along the way, we will correct errors in the statement of [5, Theorem 7.3], and provide a complete proof. All of this requires a fair amount of background knowledge. Furthermore, the reader will need to see how the cocyclic properties of the components of our construction ensures that the resulting Hadamard matrix is indeed cocyclic. This section contains a summary of the theory of binary cocycles and matrices with binary cocycles which is sufficient to meet these needs.

2.1 Some Central Products

We use the following notation for various groups. For the cyclic group of order n we use the notation $\mathbb{Z}_n$. We usually use additive notation for this abelian group. For the quaternion group of order 8 and the dihedral group of order 8, we use the following respective notations

$$\begin{aligned} \mathrm{Q}_8 &= \langle a,b \mid a^2 = b^2 = -1,\ [a,b] = -1 \rangle, \\ \mathrm{D}_8 &= \langle a,b \mid a^2 = -1, b^2 = 1,\ [a,b] = -1 \rangle. \end{aligned}$$

For the finite groups G and H containing a distinguished central involution -1, we let $G \curlyvee H$ denote the direct product group $G \times H$ factored out by the group $\langle(-1,-1)\rangle$. This group is an example of a central product. It has $|G||H|/2$ elements. For example, the group

$$\begin{aligned} \mathrm{Q}_8 \curlyvee \mathrm{D}_8 = \langle a,b,c,d \mid\ & a^2 = b^2 = c^2 = -1, d^2 = 1, \\ & [a,b] = -1, [c,d] = -1, [a,c] = [a,d] = [b,c] = [b,d] = 1 \rangle \end{aligned}$$

has 32 elements. We have $\mathrm{D}_8 \curlyvee \mathrm{D}_8 \cong \mathrm{Q}_8 \curlyvee \mathrm{Q}_8$ and $\mathrm{Q}_8 \curlyvee \mathbb{Z}_4 \cong \mathrm{D}_8 \curlyvee \mathbb{Z}_4$. We use the notation

$$\begin{aligned} A_\ell &= \overbrace{\mathrm{D}_8 \curlyvee \mathrm{D}_8 \curlyvee \ldots \mathrm{D}_8 \curlyvee \mathrm{Q}_8}^{\ell \text{ terms}}, \\ B_\ell &= \mathrm{D}_8 \curlyvee \mathrm{D}_8 \curlyvee \ldots \mathrm{D}_8 \curlyvee \mathrm{D}_8, \\ C_\ell &= \mathrm{D}_8 \curlyvee \mathrm{D}_8 \curlyvee \ldots \mathrm{D}_8 \curlyvee \mathrm{D}_8 \curlyvee \mathbb{Z}_4. \end{aligned}$$

The groups A_ℓ and B_ℓ both have order $2^{2\ell+1}$, and the group C_ℓ has order $2^{2\ell+2}$.

2.2 Binary Cocycles and Central Extensions of $\mathbb{Z}_2$

Let G be a finite group. A *binary cocycle with indexing group G* is a mapping $f : G \times G \to \{-1, 1\}$ such that for all $a, b, c \in G$,

$$f(a,b)f(ab,c) = f(b,c)f(a,bc)\,. \tag{1}$$

f is *normalized* if $f(1,1) = 1$. Notice that if f_1 and f_2 are binary cocycles with indexing group G, then the *pointwise product mapping* $f_1 f_2$, where $f_1 f_2(a,b) = f_1(a,b) f_2(a,b)$, is a binary cocycle. Moreover, if $\rho : G \to \langle -1 \rangle$ is any map, then c_ρ, where

$$c_\rho(a,b) = \rho(ab)^{-1}\rho(a)\rho(b)\,, \tag{2}$$

is a binary cocycle. Cocycles with the special form (2) are called *coboundaries*. If $f_1 = f_2 c_\rho$ for some coboundary c_ρ, then f_1 and f_2 are said to be *cohomologous*.

Binary cocycles are closely related to central extensions of $\mathbb{Z}_2$. We will exploit this connection, when we construct the matrices H, P_i, Q_j satisfying conditions (I)-(IV). Our approach will be to construct the extension group first, and then extract the cocycle f.

A *central extension of $\mathbb{Z}_2$ by a finite group G* is a group R containing a central involution, which we denote by -1, such that the factor group $R/\langle -1 \rangle$ is isomorphic to the group G. This is equivalent to the sequence of group homomorphisms

$$1 \to \langle -1 \rangle \to R \xrightarrow{\pi} G \to 1 \tag{3}$$

being exact: that is, the kernel of each homomorphism in the sequence is the image of the previous homomorphism. The sequence (3) is called a *short exact sequence*. A cocycle *associated to the sequence* (3) may be obtained by choosing a transversal map τ. A *transversal map for the sequence* (3) is a map $\tau : G \to R$ such that $\pi \circ \tau(x) = x$ for all $x \in G$. Given such a map, we define a cocycle $f_\tau : G \times G \to \langle -1 \rangle$ via the equation

$$f_\tau(a,b) = \tau(ab)^{-1}\tau(a)\tau(b)\,. \tag{4}$$

(N.B., $\tau(a)\tau(b)\tau(ab)^{-1} = \tau(ab)^{-1}\tau(a)\tau(b)$.)

Conversely, if f is a normalized binary 2-cocycle with indexing group G, and we think of $\sigma(a)$ as a formal object indexed by the element $a \in G$, then the set of elements $\pm\sigma(a)$ ($a \in G$) forms an extension group R_f of G under the operation

$$(-1)^k \sigma(a)(-1)^\ell \sigma(b) = f(a,b)(-1)^{k+\ell}\sigma(ab)\,.$$

(The cocycle equation (1) is equivalent to this operation being associative.) We then have the short exact sequence of group homomorphisms

$$1 \to \langle -1 \rangle \to \mathrm{R}_f \xrightarrow{\pi} G \to 1\,, \tag{5}$$

where $\pi(\pm\sigma(a)) = a$. We may then write $f = f_\tau$, where $\tau : G \to \mathrm{R}_f$ is the transversal map defined by the equation $\tau(a) = \sigma(a)$ for all $a \in G$.

Let G_1 and G_2 be finite groups, and let $G = G_1 \times G_2$. For $i = 1,2$, let $f_i : G_i \times G_i \to \langle -1 \rangle$ be cocycles. Define the *direct product cocycle* $f = f_1 \times f_2 : G \times G \to \langle -1 \rangle$ so that for all $x_i, y_i \in G_i$

$$f_1 \times f_2 \,(x_1 x_2, y_1 y_2) = f_1(x_1, y_1) f_2(x_2, y_2)\,. \tag{6}$$

We have the following standard result.

Lemma 2.1. *Let $f_i : G_i \times G_i \to \langle -1 \rangle$ $(i = 1,2)$ be cocycles, and let f be the product cocycle $f_1 \times f_2$. Then $R_f = R_{f_1} \curlyvee R_{f_2}$.*

2.3 Complex Matrices with Binary Cocycles

Let i denote the complex square root of -1. A $(0, \pm 1, \pm \mathrm{i})$-matrix A is in *cocyclic form* with binary cocycle f and mapping $g : G \to \{0, \pm 1, \pm \mathrm{i}\}$ if

$$A = [f(a,b)g(ab)]_{a,b \in G}\,.$$

For Kronecker products $A_1 \otimes A_2$ of matrices A_1 and A_2, we have the following standard result.

Lemma 2.2. *Suppose that for $i = 1,2$, $A_i = [f_i(a,b)g_i(ab)]_{a,b \in G_i}$, then*

$$A_1 \otimes A_2 = [f_1 \times f_2(ac, bd) g(abcd)]_{ac,bd \in G_1 \times G_2}\,,$$

where $g : G_1 \times G_2 \to \langle -1 \rangle$ is such that $g(ac) = g_1(a)g_2(c)$ for all $a \in G_1$ and $c \in G_2$.

2.4 Binary Cocycles and Monomial Representations

There is a connection between cocycles and monomial representations of groups containing a central involution. These representations are essential to our construction. Let

$$\delta_y^x = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

If $f : G \times G \to \langle -1 \rangle$ is a cocycle, then the mapping

$$(-1)^k \sigma(x) \mapsto P^{(f)}_{(-1)^k x} = (-1)^k [\delta_b^{ax} f(a,x)]_{a,b \in G} \tag{7}$$

is a faithful monomial representation of R_f. Such a representation depends on the choice of cocycle f, but the full notation is a little cumbersome, so when the choice of cocycle is clear from the context, we just write $P_{(-1)^k x}$. We have

$$P_{(-1)^k x} P_{(-1)^\ell y} = P_{f(x,y)(-1)^{k+\ell} xy} \qquad \text{and} \qquad P_{((-1)^k x)^{-1}} = P^{-1}_{(-1)^k x} = P^{\top}_{(-1)^k x}\,. \tag{8}$$

Note that

$$(\forall x \neq y) \qquad P_{(-1)^k x} \wedge P_{(-1)^\ell y} = 0 \tag{9}$$

Moreover, we have for all maps $g : G \to \{0, \pm 1, \pm \mathrm{i}\}$

$$[g(ab)f(a,b)]_{a,b\in G} = U^{(f)} \sum_{x\in G} g(x) P_x^{(f)}\,, \tag{10}$$

where

$$U^{(f)} = [\delta_1^{ab} f(a,a^{-1})]_{a,b\in G}\,.$$

Consequently, any $(0, \pm 1, \pm \mathrm{i})$-matrix of the form on the right hand side of equation (10) is cocyclic with binary cocycle f.

Lemma 2.3. *Let H be a $(0, \pm 1, \pm \mathrm{i})$- matrix. Then f is a binary cocycle of H if and only if there is a map $g : G \to \{0, \pm 1, \pm \mathrm{i}\}$ such that H is equivalent to the matrix $H' = \sum_{x\in G} g(x) P_x^{(f)}$; i.e., there exist $(0, \pm 1)$-monomial matrices P, Q such that $PHQ^\top = H'$.*

2.5 Binary Collection Cocycles and Central Extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2^m$

In this paper, we will need to determine the isomorphism class of a particular central extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2^m$. The paper [5] gives a general method for solving this type of problem. In this subsection, we give a more direct treatment which allows us to determine the isomorphism class of the extension group of the cocycle f for the matrices H, P_i, Q_j satisfying the constraints (I)-(IV).

In this case, we have a short exact sequence of the form

$$1 \to \langle -1 \rangle \to R(Q) \xrightarrow{\pi} G \cong \mathbb{Z}_2^m \to 1\,,$$

where $Q = [q_{ij}]$ is an $m \times m$ upper-triangular matrix over GF(2) and $R(Q)$ and G have the presentations

$$G = \langle a_1, a_2, \ldots, a_m | a_i^2 = 1,\ [a_j, a_i] = 1\ (i < j)\ \rangle\,,$$

and

$$R(Q) = \langle b_1, b_2, \ldots, b_m | b_i^2 = (-1)^{q_{ii}}, [b_j, b_i] = (-1)^{q_{ij}}\ (i < j)\ \rangle\,. \tag{11}$$

The presentation (11) is an example of a power-commutator presentation. Let V^m denote the m-dimensional vector space over GF(2). For $u = (u_1, u_2, \ldots, u_m) \in V^m$, write a^u for $a_1^{u_1} a_2^{u_2} \ldots a_m^{u_m}$, and b^u for $b_1^{u_1} b_2^{u_2} \ldots b_m^{u_m}$. Then every element of $R(Q)$ may be written in the form $\pm b^u$. A process called *collection* (wherein $b_j b_i$ $(i < j)$ is replaced by $b_i b_j (-1)^{q_{ij}}$, b_i^2 is replaced by $(-1)^{q_{ii}}$, and the powers of -1 are collected to the left) may be used to reduce any product $b^u b^v$ to its canonical form $(-1)^k b^{u+v}$. Choosing τ so that $\tau(a^u) = b^u$, equation (4) implies

$$f_\tau(a^u, a^v) = (b^{u+v})^{-1} b^u b^v\,. \tag{12}$$

So we may compute $f_\tau(a^u, a^v)$ by applying collection to the word $(b^{u+v})^{-1} b^u b^v$ in $R(Q)$. Consequently, we call f_τ a *binary collection cocycle*. The relations in the presentation (11), and the fact that the commutators are all central imply the elegant identity

$$f_\tau(a^u, a^v) = (-1)^{vQu^\top}\,. \tag{13}$$

The structure of $R(Q)$ is discussed in [5, Subsection 5.2]. We have (see [5, equation (34)])

$$R(Q) = F(R(Q)) \times \mathrm{Hub}(R(Q)), \tag{14}$$

where, for some $k \geq 0$,

$$F(R(Q)) \cong \mathbb{Z}_2^k,$$

and $\mathrm{Hub}(R(Q))$ is one of the groups A_ℓ, B_ℓ or C_ℓ. Each of these groups has a unique central involution (denoted by -1). The group $F(R(Q)) \times \langle -1 \rangle$ is the characteristic subgroup of $R(Q)$ comprised of the identity and all the central involutions in $R(Q)$. The isomorphism class of $\mathrm{Hub}(R(Q))$ is determined by the number $\xi(R(Q))$ of order four elements it contains and the rank k of $F(R(Q))$. Equation (13) implies that

$$(b^u)^2 = f_\tau(a^u, a^u) = (-1)^{uQu^\top}$$

and equations (12) and (13) imply that

$$[b^u, b^v] = (b^{v+u} f_\tau(a^v, a^u))^{-1} (b^{u+v} f_\tau(a^u, a^v)) = f_\tau(a^u, a^v) f_\tau(a^v, a^u) = (-1)^{uPv^\top},$$

where $P = Q + Q^\top$. So

$$k = \dim(\ker(P)) - \begin{cases} 1 & \text{if } uQu^\top = 1 \text{ for some } u \in \ker(P), \\ 0 & \text{otherwise,} \end{cases} \tag{15}$$

and

$$\xi(R(Q)) = 2|\{u \mid uQu^\top = 1\}|. \tag{16}$$

Direct calculation reveals that

$$\xi(R(Q)) = \begin{cases} 2^k(2^{2\ell} + 2^\ell) & \text{if } \mathrm{Hub}(R(Q)) \cong A_\ell, \\ 2^k(2^{2\ell} - 2^\ell) & \text{if } \mathrm{Hub}(R(Q)) \cong B_\ell, \\ 2^{2\ell+k+1} & \text{if } \mathrm{Hub}(R(Q)) \cong C_\ell. \end{cases} \tag{17}$$

An element $u \in V^m$ is called *anisotropic (with respect to Q)* if $uQu^\top = 1$. Thus, in the case where $\mathrm{Hub}(R(Q)) \ncong C_\ell$ for all ℓ, calculating the number of anisotropic elements of V^m with respect to Q, will determine the isomorphism class of $R(Q)$, and, in the case where $\mathrm{Hub}(R(Q)) \cong C_\ell$ for some ℓ, determination of the number of isotropic elements in $\ker(P)$ will decide the isomorphism class of $R(Q)$.

2.6 Cocyclic Hadamard Matrices

A *Hadamard matrix H has cocycle f* if there are signed permutation matrices P and Q and a mapping $g : G \to \langle -1 \rangle$ such that

$$H = P[f(a,b)g(ab)]_{a,b \in G} Q^\top. \tag{18}$$

In other words, H is Hadamard equivalent to a (± 1)-matrix in cocyclic form with cocycle f.

Once we have the matrices P_i, Q_j satisfying conditions (I)-(IV) for some cocycle f, we must construct a Hadamard matrix H with the same cocycle. As it happens, when the matrices P_i, Q_j have minimal order, f must be a binary collection cocycle. Theorem 4.3 of [5] implies that nearly all the binary collection cocycles of the previous subsection are cocycles of some *Sylvester Hadamard matrix* $H_m = [(-1)^{xy^\top}]_{x,y\in V^m}$.

Lemma 2.4. *Let Q be an $m \times m$ upper triangular matrix over* GF(2). *If there is a symmetric $m \times m$ matrix $S = T + T^\top$ over* GF(2) *with zero diagonal such that $N = S + Q$ is invertible, then the collection cocycle f_τ where*

$$f_\tau(a^u, a^v) = (-1)^{uQ^\top v^\top},$$

is a cocycle of the Sylvester Hadamard matrix H_m. Indeed, H_m is equivalent to the matrix

$$\sum_{u\in V^m} (-1)^{uTu^\top} P_u^{(f_\tau)}. \tag{19}$$

Proof. By Lemma 2.3, it is sufficient to prove that H_m is equivalent to the matrix (19). By equation (10),

$$\begin{aligned} U^{(f_\tau)} \sum_{u\in V^m} (-1)^{uTu^\top} P_u^{(f_\tau)} &= [(-1)^{(u+v)T(u+v)^\top} f_\tau(a^u, a^v)]_{u,v\in V^m} \\ &= [(-1)^{uTu^\top}(-1)^{vTv^\top}(-1)^{uTv^\top}(-1)^{uT^\top v^\top}(-1)^{uQ^\top v^\top}]_{u,v\in V^m}, \end{aligned}$$

which is equivalent to

$$[(-1)^{uN^\top v^\top}]_{u,v\in V^m}$$

which is equivalent to H_m since $N^\top$ is invertible. □

Notice that Lemma 2.4 (with $T = 0$ and $Q = I$) implies H_m is cocyclic for all $m \geq 1$. Since $H_1 \otimes H_2$ is a Hadamard matrix if H_1 and H_2 are, Lemma 2.2 implies the following well-known result.

Theorem 2.5. *If there is a cocyclic Hadamard matrix of order n, then there is a cocyclic Hadamard matrix of order $2^m n$ for all $m \geq 0$.*

2.7 Complex Hadamard Matrices with a Binary Cocycle

The method of [1] first yields a complex Hadamard matrix, and then a standard construction gives a (real) Hadamard matrix of twice the order. As stated in the introduction, we will adapt the method of [1] to produce a cocyclic Hadamard matrix, but in fact we will first produce a complex Hadamard matrix with a binary cocycle. In this short subsection, we show how such a matrix leads to a cocyclic Hadamard matrix.

A *complex Hadamard matrix of order n* is an $n \times n$ $(\pm 1, \pm \mathrm{i})$-matrix H such that $HH^* = nI_n$. We say a complex Hadamard matrix H has a binary cocycle if there is a

binary cocycle $f : G \times G \to \langle -1 \rangle$ and a map $g : G \to \langle \mathrm{i} \rangle$ such that for some $(0, \pm 1, \pm \mathrm{i})$-monomials P and Q

$$H = P[f(a,b)g(ab)]_{a,b \in G} Q .$$

Such a complex Hadamard matrix yields a cocyclic Hadamard matrix of order $2n$. Write $PHQ = A + \mathrm{i}B$ where A and B are real matrices. Then A and B are disjoint $(0, \pm 1)$-matrices such that

$$AA^\top + BB^\top = nI_n \qquad \text{and} \qquad AB^\top = BA^\top .$$

There are uniquely determined maps $g_A : G \to \{0, \pm 1\}$ and $g_B : G \to \{0, \pm 1\}$ such that

$$A = P[f(a,b)g_A(ab)]_{a,b \in G} Q , \qquad \text{and} \qquad B = P[f(a,b)g_B(ab)]_{a,b \in G} Q .$$

So the real block matrix

$$\begin{bmatrix} A+B & A-B \\ A-B & -A-B \end{bmatrix} = [f'((x,a),(y,b))g'((x,a)(y,b))]_{(x,a),(y,b) \in \mathbb{Z}_2 \times G} ,$$

where

$$g'((x,a)(y,b)) = \begin{cases} g_A(ab) + g_B(ab) & \text{if } x = y, \\ g_A(ab) - g_B(ab) & \text{if } x \neq y, \end{cases}$$

is a Hadamard matrix with cocycle $f' : G' \times G' \to \langle -1 \rangle$ where $G' = \mathbb{Z}_2 \times G$, and

$$f'((x,a),(y,b)) = (-1)^{xy} f(a,b) .$$

Here we use additive notation for $\mathbb{Z}_2$; so $(-1)^{xy} = -1$ if and only if $x = y = 1$. Lemma 2.1 implies the extension group is $\mathbb{Z}_4 \curlyvee R_f$. We have proved the following theorem.

Theorem 2.6. *If there is a complex Hadamard matrix C of order n with binary cocycle, then there is a cocyclic Hadamard matrix H of order $2n$. If $f : G \times G \to \langle -1 \rangle$ is the cocycle for C, then H has cocycle f' with indexing group $\mathbb{Z}_2 \times G$ and extension group $\mathbb{Z}_4 \curlyvee R_f$.*

3 Constructing the Matrices P_i, Q_j and H

We are now ready to state and prove a corrected version of [5, Theorem 7.3]. (Theorems 7.1 and 7.2 of [5] are correct.) Because we have not presented all the machinery needed to prove uniqueness for the minimal case, we will not prove that part here.

Definition 3.1. Let $f : G \times G \to \langle -1 \rangle$ be a binary cocycle. A pair of amicable orthogonal designs $\mathrm{AOD}(n; 1^{s_1}, 1^{s_2})$ with cocycle f is a pair of orthogonal designs $\mathrm{OD}(n; 1^{s_i})$, $D_i = [g_i(xy)f(x,y)]_{x,y \in G}$, $(i = 1,2)$ such that $D_1 D_2^\top = D_2 D_1^\top$.

Remark 3.2. Let $a_0, a_1, \ldots, a_{t-1}, b_0, b_1, b_2, \ldots, b_{s-1}$ be commuting indeterminates. Notice that $D_1 = \sum_{i=0}^{t-1} a_i P_i$ and $D_2 = \sum_{i=0}^{s-1} b_i Q_i$ comprise an $\mathrm{AOD}(|G|; 1^s, 1^t)$ with cocycle f if and only if the matrices P_i, Q_i satisfy the conditions (II)–(IV) for the cocycle f.

Theorem 3.3. *For all integers $s > 2$ and $t > 1$ define the group*

$$T_{s,t} = \begin{cases} B_{(s+t-2)/2} & s-t \equiv 0 \pmod 8 \\ B_{(s+t-1)/2} & s-t \equiv \pm 1 \pmod 8 \\ C_{(s+t-2)/2} & s-t \equiv \pm 2 \pmod 8 \\ A_{(s+t-1)/2} & s-t \equiv \pm 3 \pmod 8 \\ A_{(s+t-2)/2} & s-t \equiv 4 \pmod 8. \end{cases}$$

Let -1 be the unique central involution in $T_{s,t}$. An $\mathrm{AOD}(n;1^s;1^t)$ with cocycle f exists if and only if there is a homomorphic injection of $T_{s,t}$ into R_f which maps the central involution -1 to the distinguished central involution in R_f.

Proof. By Remark 3.2, we may suppose there are matrices P_i and Q_j satisfying conditions (I)-(IV) for some cocycle $f : G \times G \to \langle -1 \rangle$. We will show that if the order of R_f is minimized, then $R_f \cong T_{s,t}$.

By equation (10), there are elements $x_0, x_1, \ldots, x_{t-1}, y_0, y_1, \ldots, y_{s-1} \in R_f$ such that for all $i = 0, 1, \ldots, t-1$ and $j = 0, 1, \ldots, s-1$

$$UP_i = P_{x_i} \qquad \text{and} \qquad UQ_j = P_{y_j}.$$

For $i = 0, 1, \ldots, t-1$, put $u_i = x_i x_0^{-1}$ and, for $j = 0, 1, \ldots, s-1$, put $u_{t+j} = y_j x_0^{-1}$. We then have for $1 \le i \le s+t-1$,

$$P_{u_i}^2 = P_{x_i} P_{x_0}^\top P_{x_i} P_{x_0}^\top = (-1)^{n_{0i}} P_{x_i} P_{x_0}^\top P_{x_0} P_{x_i}^\top = (-1)^{n_{0i}} I,$$

and, for $1 \le i < j \le s+t-1$,

$$[P_{u_i}, P_{u_j}] = [P_{u_i}^{-1}, P_{u_j}^{-1}] = P_{u_i} P_{u_j} P_{u_i}^\top P_{u_j}^\top = P_{u_i} (-1)^{n_{ij}} P_{u_i} P_{u_j}^\top P_{u_j}^\top = (-1)^{n_{0i}+n_{0j}+n_{ij}} I,$$

where, for $0 \le i < j \le s+t-1$,

$$n_{ij} = \begin{cases} 1 & 0 \le i < j \le t-1, \\ 1 & t \le i < j \le s+t-1, \\ 0 & \text{otherwise.} \end{cases}$$

Now define the $(s+t-1) \times (s+t-1)$ matrix $Q = [q_{ij}]$ over $\mathrm{GF}(2)$ so that, for $1 \le i < j \le s+t-1$,

$$q_{ii} = n_{0i}, \qquad \text{and} \qquad q_{ij} = n_{0i} + n_{0j} + n_{ij}.$$

Then the $s+t$ permutation matrices P_i and Q_j ($i = 0, 1, \ldots, t-1$ and $j = 0, 1, \ldots, s-1$), where $P_0 = U, P_i = UP_{u_i}$, and $Q_j = UP_{u_{t+j}}$, satisfy the constraints (I)-(IV) if and only if the elements u_i satisfy the equations

$$u_i^2 = (-1)^{q_{ii}}, \qquad \text{and} \qquad \left[u_j, u_i\right] = (-1)^{q_{ij}}, \tag{20}$$

for all $1 \le i < j \le s+t-1$. Our goal now is to identify the smallest extension group R_f containing elements u_i satisfying (20).

We show that $R_f \cong \mathrm{Hub}(R(Q))$. By the minimality of the order of R_f, we have

$$R_f = \langle u_1, u_2, \ldots, u_{s+t-1} \rangle ,$$

and there is an epimorphism $\phi : R(Q) \to R_f$. Observe that R_f is non-abelian, and that $R(Q)/\langle -1 \rangle \cong \mathbb{Z}_2^{s+t-1}$ is abelian. So $R_f \cong R(Q)/N$, where N is a normal subgroup of $R(Q)$ not containing the central involution -1. Now since $[a,bc] = [a,c][a,b]^c$, and $[ab,c] = [a,c]^b[b,c]$, we have

$$[R(Q),R(Q)] = \langle -1 \rangle .$$

So any non-abelian subgroup of $R(Q)$ contains -1. Moreover, since N must not contain -1, N must be abelian. Indeed, if there is an element $r \in R(Q)$ and an element $s \in N$ such that $[r,s] \neq 1$, then $[r,s] = -1$, and $-1 = (s^{-1})^r s \in N$ - a contradiction. So N is central in $R(Q)$. Finally, since $R(Q)/\langle -1 \rangle$ is elementary abelian, every non-identity element in $R(Q)$ is of order 2 or 4, and the square of any order four element is -1. Therefore, every non-identity element of N is a central involution. Consequently, $N\langle -1 \rangle = F(R(Q))\langle -1 \rangle$. So $N\mathrm{Hub}(R(Q)) = N\langle -1 \rangle \mathrm{Hub}(R(Q)) = F(R(Q))\langle -1 \rangle \mathrm{Hub}(R(Q)) = R(Q)$, and, since $N \cap \mathrm{Hub}(R(Q)) = 1$, $R(Q) = N \times \mathrm{Hub}(R(Q))$. Therefore $R_f \cong R(Q)/N \cong \mathrm{Hub}(R(Q))$, as claimed.

To determine $R_f \cong \mathrm{Hub}(R(Q))$, we use the procedure set out in Subsection 2.5. In this case, Q is an $(s+t-1) \times (s+t-1)$ upper-triangular matrix with above-diagonal entries all equal to 1. The first $t-1$ diagonal entries of Q equal 1, and the remaining s are 0. So $P = Q + Q^T$ is the matrix $J_{s+t-1} - I_{s+t-1}$. We have

$$\begin{aligned}
\ker P &= \begin{cases} \langle (1,\ldots,1) \rangle & s \equiv t \pmod 2, \\ 0 & \text{otherwise,} \end{cases} \\
(1,\ldots,1)Q(1,\ldots,1)^\top &= \begin{cases} 0 & s-t \equiv 0,3 \pmod 4, \\ 1 & \text{otherwise,} \end{cases} \\
\xi(R(Q)) &= 2 \sum_{w_1 - w_2 \equiv 1,2(4)} \binom{t-1}{w_1} \binom{s}{w_2} .
\end{aligned}$$

Writing Σ_i for $\sum_{w_1-w_2 \equiv i\,(4)} \binom{t-1}{w_1}\binom{s}{w_2}$, we have

$$\begin{aligned}
&2(\Sigma_1 + \Sigma_2 - \Sigma_0 - \Sigma_3) \\
&\quad = \sum_{w_1,w_2} \left(-(\mathrm{i})^{w_1-w_2} - (\mathrm{i})^{-w_1+w_2} - (\mathrm{i})^{1+w_1-w_2} + (\mathrm{i})^{1-w_1+w_2} \right) \binom{t-1}{w_1} \binom{s}{w_2} \\
&\quad = -(1+\mathrm{i})^{t-1}(1-\mathrm{i})^s - (1-\mathrm{i})^{t-1}(1+\mathrm{i})^s \\
&\qquad -\mathrm{i}(1+\mathrm{i})^{t-1}(1-\mathrm{i})^s + \mathrm{i}(1-\mathrm{i})^{t-1}(1+\mathrm{i})^s .
\end{aligned}$$

So

$$\begin{aligned}
4(\Sigma_1 + \Sigma_2) &= 2^{t+s} - (1+\mathrm{i})^t(1-\mathrm{i})^s - (1-\mathrm{i})^t(1+\mathrm{i})^s \\
&= 2^{t+s} - (\sqrt{2})^{t+s}(e^{(t-s)\mathrm{i}\pi/4} + e^{-(t-s)\mathrm{i}\pi/4}) \\
&= 2^{t+s} - (\sqrt{2})^{t+s} 2\cos(t-s)\pi/4 .
\end{aligned}$$

So

$$\xi(R(Q)) = \begin{cases} 2(2^{t+s-2} - 2^{(t+s-2)/2}) & \text{if } t-s \equiv 0 \pmod 8, \\ 2^{t+s-1} - 2^{(t+s-1)/2} & \text{if } t-s \equiv \pm 1 \pmod 8, \\ 2^{t+s-1} & \text{if } t-s \equiv \pm 2 \pmod 8, \\ 2^{t+s-1} + 2^{(t+s-1)/2} & \text{if } t-s \equiv \pm 3 \pmod 8, \\ 2(2^{t+s-2} + 2^{(t+s-2)/2}) & \text{if } t-s \equiv 4 \pmod 8, \end{cases}$$

Consequently,

$$\mathrm{Hub}(R(Q)) \cong \begin{cases} B_{(t+s-2)/2} & \text{if } t-s \equiv 0 \pmod 8, \\ B_{(t+s-1)/2} & \text{if } t-s \equiv \pm 1 \pmod 8, \\ C_{(t+s-2)/2} & \text{if } t-s \equiv \pm 2 \pmod 8, \\ A_{(t+s-1)/2} & \text{if } t-s \equiv \pm 3 \pmod 8, \\ A_{(t+s-2)/2} & \text{if } t-s \equiv 4 \pmod 8, \end{cases}$$

and

$$F(R(Q)) \cong \begin{cases} \mathbb{Z}_2 & \text{if } t-s \equiv 0 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

□

The proof of the above theorem gives an explicit method for constructing the matrices P_i and Q_j and cocycle f satisfying conditions (I)-(IV). For $s = t = 2M+1$, the extension group is $B_{2M} \cong R(Q')$, where Q' is the $4M \times 4M$ upper-triangular matrix over GF(2) with all above diagonal entries equal to 1, and the first $2M$ diagonal entries equal to 1. The cocycle f is the collection cocycle f_τ defined by equation (13) for $Q = Q'$. So for $u, v \in V^{4M}$,

$$f(a^u, a^v) = (-1)^{vQ'u^\top}. \tag{21}$$

To form the matrices P_i, Q_j, using the presentation (11) with $Q = Q'$, we set

$$P_0 = U\,, \quad Q_0 = UP_{b_1 b_2 \ldots b_{4M}}\,, \quad P_i = UP_{b_i}\,, \quad \text{and} \quad Q_i = UP_{b_{2M+i}}\,, \tag{22}$$

where $i = 1, 2, \ldots, 2M$, This leaves the explicit construction of a map $g : \mathbb{Z}_2^{4M} \to \langle -1 \rangle$ such that $H = [f(x,y)g(xy)]$ is a Hadamard matrix. The proof of the following theorem meets this need.

Theorem 3.4. *Let $M \geq 1$ be an integer. Let Q' be the $4M \times 4M$ upper-triangular binary matrix defined above, and let f be the cocycle defined by equation* (21)*. The signed permutation matrices $P_0, P_1, \ldots, P_{2M}, Q_0, Q_1, \ldots, Q_{2M}$ of order 2^{4M} defined by* (22) *satisfy the conditions (I)-(IV) with cocycle f. The extension group is B_{2M}, and the indexing group is $(V^{4M}, +) \cong \mathbb{Z}_2^{4M}$. Moreover, there is a binary matrix T such that H_{4M} is equivalent to the matrix $H = \sum_{v \in V^{4M}} (-1)^{vTv^\top} P_v^{(f)}$.*

Proof. The properties of the matrices P_i, Q_j have just been proved above. Therefore, by Lemma 2.4, it is sufficient to exhibit for each $M \geq 1$, a symmetric matrix $S = T + T^\top$ with

zero diagonal such that $Q' + S$ is invertible over GF(2). For $M = 1$, we have

$$Q' = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad S = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \quad Q' + S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

For $M > 1$, we take $S = T + T^\top$, where $T = [t_{ij}]$ is the $4M \times 4M$ matrix such that

$$t_{ij} = \begin{cases} 1 & \text{if } i = 2M+1 \text{ and } j > 2M+2, \\ 0 & \text{otherwise.} \end{cases}$$

□

Thus for any $s = t = 2M+1$, we have an explicit construction for the matrices P_i, Q_j, H satisfying conditions (I)-(IV). Moreover, we know the order n can be no smaller than 2^{4M}.

4 Complementary Sequences with Zero Aperiodic Autocorrelation

As in [1], our constructions will employ complementary sequences. In this section, we bring together the existence results from [1] needed for our construction. Let

$$(a_{11}, a_{12}, \ldots, a_{1,n_1}), (a_{21}, a_{22}, \ldots, a_{2,n_2}), \ldots, (a_{r1}, a_{r2}, \ldots, a_{r,n_r})$$

denote r sequences of complex fourth roots of unity. So $a_{ij} \in \{\pm 1, \pm \mathrm{i}\}$. The integer n_i is called the *length* of the ith sequence, and the sum of the lengths $\sum_{i=1}^{r} n_i$ is called the *combined length*.

The sequences have zero aperiodic autocorrelation if

$$\sum_{i=1}^{r} \sum_{j=1}^{n_i - a} a_{i,j} \overline{a_{i,j+a}} = 0,$$

for all integers $a > 0$. Notice that the lengths n_i exceeding 1 must appear an even number of times in the sequence $n_1, n_2, \ldots, n_r$. So if $n_i > 1$ for all i, then we may suppose that $n_{2i} = n_{2i-1}$. In this case, we say that the sequences are *paired*.

For any non-negative integer q, let $N(q)$ denote the number of 1's in the binary expansion of q. Combining pairs of Golay sequences of length 2^k, we have

Theorem 4.1. *Let $q = 2p+1$ be an odd natural number, then there are $2N(p)$ real $(1,-1)$-sequences with $n_{2i} = n_{2i-1}$, zero aperiodic autocorrelation and combined length $2p$.*

Real sequences offer important advantages over complex sequences. However, complex sequences seem to be much more abundant, and they are all we need for our construction. Let $L(p)$ denote the least number of paired complex sequences with zero autocorrelation needed for a combined length of $2p$. So Theorem 4.1 implies that $L(p) \leq 2N(p)$. The asymptotic power of this paper's approach to constructing cocyclic Hadamard matrices depends on the behavior of $L(p)$. We make the following conjecture without further comment here.

Conjecture 4.2. *For any $\varepsilon > 0$, $L(p)$ is eventually less than $\varepsilon \log_2 p$.*

The following result was proved in [1].

Theorem 4.3. *Let $q = 2p+1 > 0$ be an integer, and let $t = \lfloor \frac{\log_2(q-1)}{10} \rfloor$. Then for some $L \leq 4t+4$, there are L complex sequences $(a_{i1}, a_{i2}, \ldots, a_{i,n_i})$ with zero aperiodic autocorrelation and combined length $2p$ such that $n_{2i} = n_{2i-1}$. Equivalently,*

$$L(p) \leq 4 + 4\left\lfloor \frac{\log_2(q-1)}{10} \right\rfloor. \tag{23}$$

Note that in general Theorem 4.3 gives a much lower bound than Theorem 4.1.

5 A Family of Hermitian and Skew-Hermitian Circulants

In this section, we show how the complementary sequences described in the previous section may be used to make special sets of circulant Hermitian and skew-Hermitian complex matrices. These techniques are discussed in [1], however, here we make certain things more explicit, and draw out what is needed for our constructions.

Let $q = 2p+1$ denote an odd natural number where $p \geq 1$. Let $\{(a_{i1}, a_{i2}, \ldots, a_{i,n_i})\}_{i=1}^{2M}$ be $2M$ $(\pm 1, \pm \mathrm{i})$-sequences with $n_{2i} = n_{2i-1}$, zero aperiodic autocorrelation and combined length $2p = n_1 + n_2 + \cdots + n_{2M}$. For $i = 1, 2, \ldots, M$, form the $q \times q$ circulant matrix A_i with initial row

$$\begin{aligned}(0^{1+p-n_1-n_3-\cdots-n_{2i-1}}, a_{2i-1,1}, a_{2i-1,2}, \ldots, a_{2i-1,n_{2i-1}}, 0^{n_1+n_3+\cdots+n_{2i-3}}, \\ 0^{n_2+n_4+\cdots+n_{2i-2}}, a_{2i,1}, a_{2i,2}, \ldots, a_{2i,n_{2i}}, 0^{p-n_2-n_4-\cdots-n_{2i}})\end{aligned} \tag{24}$$

and, for $i = 1, 2, \ldots, M$, form the $q \times q$ circulant matrix B_i with initial row

$$\begin{aligned}(0^{1+p-n_1-n_3-\cdots-n_{2i-1}}, a_{2i-1,1}, a_{2i-1,2}, \ldots, a_{2i-1,n_{2i-1}}, 0^{n_1+n_3+\cdots+n_{2i-3}}, \\ 0^{n_2+n_4+\cdots+n_{2i-2}}, -a_{2i,1}, -a_{2i,2}, \ldots, -a_{2i,n_{2i}}, 0^{p-n_2-n_4-\cdots-n_{2i}})\end{aligned} \tag{25}$$

Then $A_i, B_i, A_i^\top, B_i^\top$ have the same support. For $i = 1, 2, \ldots, M$, we may set

$$\begin{aligned} S_i &= (A_i + A_i^*)/2 & T_i &= (B_i + B_i^*)/2 \\ U_i &= (A_i - A_i^*)/2 & V_i &= (B_i - B_i^*)/2 \end{aligned}$$

The matrices S_i, T_i are Hermitian circulants, and the matrices U_i, V_i are skew-Hermitian circulants. Moreover, $S_i \pm U_i$ and $T_i \pm V_i$ are $(0, \pm 1, \pm \mathrm{i})$-matrices. We have

$$S_i S_i^* + U_i U_i^* = (A_i + A_i^*)^2/4 - (A_i - A_i^*)^2/4 = A_i A_i^* ,$$

and

$$T_i T_i^* + V_i V_i^* = (B_i + B_i^*)^2/4 - (B_i - B_i^*)^2/4 = B_i B_i^* .$$

In fact, the matrices U_i, V_i, S_i and T_i satisfy the following theorem.

Theorem 5.1. *Let $q = 2p+1 > 1$ be an odd natural number. If there are $2M$ paired complex sequences with zero aperiodic autocorrelation and combined length $2p$, then there are $4M$ circulant $(0, \pm 1, \pm \mathrm{i})$-matrices $S_1, S_2, \ldots, S_M$, $T_1, T_2, \ldots, T_M$, $U_1, U_2, \ldots, U_M$, $V_1, V_2, \ldots, V_M$ such that*

1. *for $i = 1, 2, \ldots, M$, the matrices S_i and T_i are Hermitian, and the matrices U_i and V_i are skew-Hermitian.*
2. *$I_q + \sum_{i=1}^{M} (\pm S_i \pm U_i)$ and $I_q + \sum_{i=1}^{M} (\pm T_i \pm V_i)$ are $q \times q$ $(\pm 1, \pm \mathrm{i})$-matrices.*
3. *$\sum_{i=1}^{M} (S_i S_i^* + T_i T_i^* + U_i U_i^* + V_i V_i^*) = 4p I_q$.*

6 Combining the Circulants with the Signed Permutation Matrices

We now construct a complex Hadamard matrix with binary cocycle, and then a cocyclic Hadamard matrix of twice the order.

Theorem 6.1. *Let $q = 2p+1 > 1$ be an odd integer. If there are $2M$ paired $(\pm 1, \pm \mathrm{i})-$sequences with zero aperiodic autocorrelation and combined length $2p$, then there is a complex Hadamard matrix of order $q 2^{4M+1}$ with extension group $\mathbb{Z}_{2q} \times B_{2M}$ and indexing group $\mathbb{Z}_q \times \mathbb{Z}_2^{4M+1}$. Consequently, there is a cocyclic Hadamard matrix with extension group $\mathbb{Z}_{2q} \times C_{2M}$ and indexing group $\mathbb{Z}_q \times \mathbb{Z}_2^{4M+2}$.*

Proof. By Theorem 5.1, there are $4M$ circulant $q \times q$ $(0, \pm 1, \pm \mathrm{i})$-matrices $S_1, S_2, \ldots, S_M$, $T_1, T_2, \ldots, T_M, U_1, U_2, \ldots, U_M, V_1, V_2, \ldots, V_M$ satisfying conditions (1)–(3) of Theorem 5.1. Let $H, P_0, P_1, \ldots, P_{2M}, Q_0, Q_1, \ldots, Q_{2M}$ of order 2^{4M} be the matrices supplied by Theorem 3.4. Let W be the matrix $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. Form the complex Hadamard matrix

$$X = I_2 \otimes (I_q \otimes P_0 H + \sum_{i=1}^{M} (S_i \otimes P_{2i} H + U_i \otimes Q_{2i-1} H)) \\ + \mathrm{i} W \otimes (I_q \otimes Q_0 H + \sum_{i=1}^{M} (T_i \otimes Q_{2i} H + V_i \otimes P_{2i-1} H)) .$$

We claim that X is a complex Hadamard matrix with binary cocycle and extension group $\mathbb{Z}_{2q} \times B_{2M}$. Then Theorem 2.6 implies there is a cocyclic Hadamard matrix with extension group $\mathbb{Z}_4 \curlyvee B_{2M} \times \mathbb{Z}_{2q} \cong C_{2M} \times \mathbb{Z}_{2q}$ and indexing group $\mathbb{Z}_q \times \mathbb{Z}_2^{4M+2}$.

To see that X is a complex Hadamard matrix takes a few steps. First observe that X is a $(\pm 1, \pm \mathrm{i})$-matrix. The matrices $P_i H, Q_j H$ are (± 1)-matrices, and I_2 and W are disjoint $(0,1)$-matrices summing to the all 1's matrix $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]$. So condition (2) of Theorem 5.1 implies that X is a $(\pm 1, \pm \mathrm{i})$-matrix. Next observe that, if A and C are matrices of the same dimension, and B and D are matrices of the same dimension, then $(A \otimes B)(C \otimes D)^* = AC^* \otimes BD^*$. Therefore, the (anti-) amicability properties of the matrices I_q, U_i, V_i, S_i, T_i and the matrices P_i and Q_i imply that $X = I_2 \otimes \sum_{i=0}^{M} A_i + \mathrm{i}W \otimes \sum_{i=0}^{M} B_i$, where $A_i B_j^* = B_j A_i^*$ for all $i, j = 0, 1, \ldots, M$, and, for $i \neq j$, $A_i A_j^* = -A_j A_i^*$ and $B_i B_j^* = -B_j B_i^*$. So the cross terms in the computation for XX^* cancel out. Finally note that, if P is a signed permutation matrix of order n and H is an Hadamard matrix of the same order, then $(PH)(PH)^* = PHH^*P^* = nPP^* = nI_n$. So, using condition (2) of Theorem 5.1,

$$XX^* = I_2 \otimes \left(2I_q + \sum_{i=1}^{M} (S_i S_i^* + U_i U_i^* + T_i T_i^* + V_i V_i^*)\right) \otimes 2^{4M} I_{2^{4M}} = q 2^{4M+1} I_{q 2^{4M+1}}.$$

So X is a complex Hadamard matrix.

Next we show that X has a binary cocycle. By Theorem 3.4, the matrices $P_i H$ and $Q_i H$ are linear combinations of the monomials $P_x^{(f_1)}$, where $R_{f_1} \cong B_{2M}$. So Lemma 2.3 implies that the matrices $P_i H$ and $Q_i H$ are cocyclic with cocycle $f_1 : \mathbb{Z}_2^{4M} \times \mathbb{Z}_2^{4M} \to \langle -1 \rangle$ and extension group B_{2M}. The matrices U_i, V_i, S_i, T_i are cocyclic with trivial cocycle $f_2 : \mathbb{Z}_q \times \mathbb{Z}_q \to \langle -1 \rangle$, where $f_2(a,b) = 1$ for all $a, b \in \mathbb{Z}_q$. Finally, I_2 and W are cocyclic with trivial cocycle $f_3 : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \langle -1 \rangle$. So $R_{f_2} \cong \mathbb{Z}_q \times \langle -1 \rangle$, and $R_{f_3} \cong \mathbb{Z}_2 \times \langle -1 \rangle$. Consequently, by Lemma 2.2, the complex Hadamard X has cocycle $f = f_1 \times f_2 \times f_3$, and, by Lemma 2.1, the extension group is $R_{f_1} \curlyvee R_{f_2} \curlyvee R_{f_3} \cong B_{2M} \curlyvee (\mathbb{Z}_q \times \langle -1 \rangle) \curlyvee (\mathbb{Z}_2 \times \langle -1 \rangle) \cong B_{2M} \times \mathbb{Z}_{2q}$. So X is a complex Hadamard matrix with cocycle as claimed. □

Corollary 6.2. *Let $q = 2p + 1 > 1$ be an odd integer. If the binary expansion of q has N ones, then there is a cocyclic Hadamard matrix of order $2^{4N-2}q$. The extension group is $C_{2(N-1)} \times \mathbb{Z}_{2q}$ and the indexing group is $\mathbb{Z}_2^{4N-2} \times \mathbb{Z}_q$.*

Proof. By Theorem 4.1, there are $2(N-1)$ paired $(\pm 1)-$sequences with zero autocorrelation and combined length $2p$. Now apply Theorem 6.1 with $M = N - 1$. □

Even in the worst case, where $N = \log_2 q$, we have a cocyclic Hadamard matrix of order $2^{4\log_2 q - 2}q$ which is a substantial improvement over the result in [5].

We now obtain a much better asymptotic result using the sequences from Theorem 4.3.

Corollary 6.3. *For any odd natural number $q = 2p + 1 > 1$, there is a cocyclic Hadamard matrix with extension group $\mathbb{Z}_{2q} \times C_{L(p)}$ and indexing group $\mathbb{Z}_q \times \mathbb{Z}_2^{2L(p)+2}$. In particular, there is a cocyclic Hadamard matrix of order $q2^k$ for all $k \geq 10 + 8\left\lfloor \frac{\log_2(q-1)}{10} \right\rfloor$.*

Proof. By the definition of $L(p)$, we may apply Theorem 6.1 with $2M = L(p)$. By Theorem 4.3, we may apply Theorem 6.1 with $2M \leq 4 + 4\left\lfloor \frac{\log_2(q-1)}{10} \right\rfloor$ to get a cocyclic Hadamard matrix of order $q2^{4M+2}$. Now apply Theorem 2.5 to obtain cocyclic Hadamard matrices for all $k \geq 4M+2$. □

7 Concluding Remarks

By [3, Theorem 2.4], Corollaries 6.2 and 6.3 imply the existence of large classes of Hadamard matrices with regular group actions and large classes of maximal-size, relative difference sets with central forbidden subgroup of order two. Thus at least for large powers of two, there are Hadamard matrices with very special structure. This extra structure makes the algebraic techniques (such as group ring theory and representation theory) commonly used to study relative difference sets relevant to resolving the Hadamard conjecture. In order to proceed along these lines, we must develop better tools for handling relative difference sets in non-abelian groups.

We now make a few remarks about the limitations and implications of the construction of Theorem 6.1. Our construction shows that it is possible to adapt the method of [1] to obtain cocyclic Hadamard matrices, but our bound on the exponent in the power of two is about twice the bound obtained for general Hadamard matrices. Once the number of complementary sequences is fixed, the exponent of two is determined by the order of the signed permutation matrices P_i, Q_i needed for the construction. Asking that these matrices be cocyclic doubles the exponent. The theory described in this paper shows that this exponent cannot be lowered. However, the above limitation on the power of two is not as important as one might think. If Conjecture 4.2 is true, then Corollary 6.3 implies that, for any $\varepsilon > 0$, there is an integer k such that for all $q > k$, there is a cocyclic Hadamard matrix or order $q2^{2+\varepsilon \log_2 q}$. We therefore propose the following problem.

Problem 7.1. *Show that there are sufficiently many complex complementary sequences that the construction of Theorem 6.1 could be used to prove that for any $\varepsilon > 0$, there is an integer k such that for all $q > k$, there is a cocyclic Hadamard matrix of order $q2^{2+\varepsilon \log_2 q}$.*

Solving this problem, which may be within our reach, would be a striking advance. It wholly depends on improving our understanding of the asymptotic behaviour of the quantity $L(p)$. Notice that dropping the requirement that the Hadamard matrix be cocyclic has no bearing on Problem 7.1, since its resolution depends on establishing Conjecture 4.2.

References

[1] R. Craigen, W. H. Holzmann and H. Kharaghani, On the asymptotic existence of complex Hadamard matrices, J. Combin. Des., **5** (1997), 319–327.

[2] Warwick de Launey, *Cocyclic Hadamard matrices and relative difference sets*, Ohio State Conference on Groups and Difference Sets, and The Hadamard Centenary Conference, University of Wollongong, 1993.

[3] Warwick de Launey and D. L. Flannery, and K. J. Horadam, Cocyclic Hadamard matrices and difference sets, Discrete Appl. Math. **102** (2000), no 1-2, 47–61, Coding, cryptography and computer security (Lethbridge, AB, 1998).

[4] Warwick de Launey and K. J. Horadam, A weak difference set construction for higher-dimensional designs, Des. Codes Cryptogr. **3** (1993), no. 1, 75–87.

[5] Warwick de Launey and Michael 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. Combin. Th., Series A **93** (2001), 37–92.

[6] D. L. Flannery, Cocyclic Hadamard matrices and Hadamard groups are equivalent, J. Algebra **192** (1997), no. 2, 749–779.

[7] K. J. Horadam and Warwick de Launey, Cocyclic development of designs, J. Algebraic Combin. **2** (1993), no. 3, 267–290.

[8] Jennifer Seberry Wallis, On the existence of Hadamard matrices, J. Combin. Th., **21** (1976), no. 2, 188-195.

Acknowledgement: The authors thank the referees for their valuable help in the preparation of this article.

Note Added in Proof: The following asymptotic existence result has been proved in a recent paper (W. de Launey, On the Asymptotic Existence of Hadamard Matrices, JCTA, to appear). It is a weak version of the conclusion to Problem 7.1.

Theorem 7.2. *Let $\varepsilon > 0$. Let $H(x)$ denote the number of odd positive integers $k \leq x$ for which there is a cocyclic Hadamard matrix of order $2^\ell k$, for some positive integer $\ell \leq 2 + \varepsilon \log_2 k$. Then there is a constant $c_1(\varepsilon)$, dependent only on ε, such that, for all sufficiently large x, $H(x) > c_1(\varepsilon)x$.*