Computing 2-cocycles for central extensions and relative difference sets

D.L. Flannery
Department of Mathematics, National University of Ireland,
Galway, Ireland
dane.flannery@nuigalway.ie

E.A. O'Brien
Department of Mathematics, University of Auckland,
Private Bag 92019, Auckland, New Zealand
obrien@math.auckland.ac.nz

Abstract

We present an algorithm to compute $H^2(G, U)$ for a finite group G and finite abelian group U (trivial G-module). The algorithm returns a generating set for the second cohomology group in terms of representative 2-cocycles, which are given explicitly. This information may be used to find presentations for corresponding central extensions of U by G. An application of the algorithm to the construction of relative $(4t, 2, 4t, 2t)$-difference sets is given.

1 Introduction

Let G be a finite group and U a finite abelian group, written multiplicatively. Consider U as a trivial G-module. In [8], a method is given for determining explicitly a full set of representative 2-cocycles for the elements of the second

This work was supported in part by the Marsden Fund of New Zealand via grant #9144/3368248.

cohomology group $H^2(G,U)$, based on a version of the Universal Coefficient Theorem. Here we adapt the method as a practical algorithm to compute representatives for all elements in a generating set of $H^2(G,U)$, thereby yielding incidentally the primary invariants of this finite abelian group.

We have implemented the algorithm in MAGMA [1]. For this purpose, we restrict the permitted descriptions of G to those which provide a solution to the word problem.

In Section 2 we present the basic algorithm. It can be extended to return a presentation for the central extension of U by G corresponding to each 2-cocycle computed. We discuss this in Section 3. All isomorphism types of central extensions of U by G are so realised (of course, some may be realised more than once). In Section 4 we comment on aspects of our implementation. In the ultimate Section 5, we demonstrate an application to the construction of relative $(4t, 2, 4t, 2t)$-difference sets in central extensions. Various such difference sets, for small t, are listed.

In this paper, computation of 2-cohomology for trivial coefficients has a particular meaning and specific aim: we wish to know *completely* the action of 2-cocycles. Ellis and Kholodna [7] also consider this problem. Until now, cohomology programs available publicly did not allow computation of the sort of information that we require. The procedures written by Holt [11], and distributed as part of MAGMA, assume that G is a finite permutation group and U is an elementary abelian group; GAP 4 [10] also has some facilities for computing with cohomology (cf. [5, §6]).

The reader is referred to [8] and [3, 14] for the theory and proofs of results underlying Sections 2 and 5, respectively.

From now on, "cocycle" means "2-cocycle". As usual, for a set π of primes, $\mathsf{O}_\pi(G)$ denotes the largest normal π-subgroup of G.

2 The basic algorithm

Denote by $Z^2(G,U)$ the abelian group of all cocycles from G to U, under pointwise multiplication. The values $\psi(g,h)$ of $\psi \in Z^2(G,U)$ may be represented as a "cocyclic matrix" with entries in U. A complete cocyclic matrix contains much more data than is needed to write down a presentation for the corresponding central extension. Accordingly, to do this we need only compute the relevant matrix entries (see the paragraph after Proposition 2.1 below). By contrast, Section 5 features an application which requires knowledge of all cocyclic matrix entries.

If $\phi\colon G \to U$ is a set map with $\phi(1_G) = 1_U$ (ϕ is *normalised*), then there is a coboundary $\partial\phi \in Z^2(G,U)$ defined by $\partial\phi(g,h) = \phi(g)\phi(h)\phi(gh)^{-1}$. The group of all coboundaries from G to U is denoted $B^2(G,U)$, and we have $H^2(G,U) = Z^2(G,U)/B^2(G,U)$. It is proved in [8, §3] that $H^2(G,U) = I \times T$, where I is the (faithful) image of $\mathrm{Ext}(G/G',U) \leq H^2(G/G',U)$ under inflation, and T is the (faithful) image of $\mathrm{Hom}(H_2(G),U)$ under a certain transgression homomorphism. We explain how representatives for the elements in a generating set for each of these two factors may be found; cf. the discussion after [8, Corollary 3.3].

It is worth noting that the process of finding I is canonical, in the sense that resultant matrices will be the same up to equivalence (pre- and post-multiplication by a permutation matrix) regardless of ordering choices made during the process. But if $|I|$ and $|T|$ are not coprime, there will be more than one complement of I in $H^2(G,U)$. It is not possible by choice of transgression to select canonically one of these complements, nor to select canonically a particular representative cocycle for each class in a complement. These points may lead to difficulty in checking by hand computational results for T.

We consider I first. Denote by π_I the set of all primes dividing both $|G\colon G'|$ and $|U|$. Fix $p \in \pi_I$. Let $\mathrm{O}_p(G/G') = \langle\, g_1G' \,\rangle \times \cdots \times \langle\, g_nG' \,\rangle$, where $\langle\, g_iG' \,\rangle \cong C_{p^{e_i}}$, $e_i \geq 1$. Let $\mathrm{O}_p(U) = \langle\, u_1 \,\rangle \times \cdots \times \langle\, u_m \,\rangle$, where $\langle\, u_i \,\rangle \cong C_{p^{f_i}}$, $f_i \geq 1$. (To make notation less cumbersome, we will not indicate the dependence of the parameters n, m, e_i, f_i, nor the elements g_i, u_i, on the choice of p.) Then $\mathrm{O}_p(\mathrm{Ext}(G/G',U))$ is

$$\prod_{i=1}^{n}\prod_{j=1}^{m} \mathrm{Ext}(\langle\, g_iG' \,\rangle, \langle\, u_j \,\rangle).$$

Also note that

$$\mathrm{Ext}(C_{p^{e_i}}, C_{p^{f_j}}) = H^2(C_{p^{e_i}}, C_{p^{f_j}}) \cong C_{p^{\min\{e_i,f_j\}}}.$$

A representative cocyclic matrix $M_{i,j}$ for a generator of $\mathrm{Ext}(\langle\, g_iG' \,\rangle, \langle\, u_j \,\rangle)$ is the $p^{e_i} \times p^{e_i}$ matrix with rows and columns indexed $G', g_iG', g_i^2G', \ldots, g_i^{p^{e_i}-1}G'$

and rth row

$$1 \;\; 1 \;\; \ldots \;\; 1 \;\; u_j \;\; u_j \;\; \ldots \;\; u_j$$

where the first occurrence of u_j is in column $p^{e_i}-r+2$. Representative cocyclic matrices for the elements in a generating set of $\mathsf{O}_p(I)$ are found as follows: for each i, $1 \leq i \leq n$, and each j, $1 \leq j \leq m$, take the matrix Kronecker product

$$N_{i,j} = J_{p^{e_1}} \otimes \cdots \otimes J_{p^{e_{i-1}}} \otimes M_{i,j} \otimes J_{p^{e_{i+1}}} \otimes \cdots \otimes J_{p^{e_n}} \otimes J_t \otimes J_{|G'|} \qquad (1)$$

where J_s denotes the $s \times s$ all 1s matrix, and $t = |\mathsf{O}_{p'}(G/G')|$. (For each $N_{i,j}$, we record the order of the class of the associated cocycle in $H^2(G,U)$, viz. $p^{\min\{e_i,f_j\}}$.) Note that $N_{i,j}$ is symmetric. If the elements of $\mathsf{O}_{p'}(G/G')$ are $h_1G', h_2G', \ldots, h_tG'$ and those of G' are $k_1, k_2, \ldots, k_{|G'|}$, then $N_{i,j}$ has rows and columns indexed by

$$\{1, g_1, g_1^2, \ldots, g_1^{p^{e_1}-1}\} \otimes \cdots \otimes \{1, g_n, g_n^2, \ldots, g_n^{p^{e_n}-1}\} \otimes \{h_1, \ldots, h_t\} \otimes \{k_1, \ldots, k_{|G'|}\}$$

where the "Kronecker product" $\otimes$ of ordered sets of elements of G is defined in the obvious way.

Proposition 2.1 *As p runs over π_I, the collection of all cocyclic matrices $N_{i,j}$ as defined by* (1) *is a complete and irredundant set of representatives for the elements in a generating set of I.*

Fix p, and suppose $[\psi]$ is in $\mathsf{O}_p(I)$; say ψ has cocyclic matrix $N_{i,j}$ for some i and j. Given a pair g, h of elements of G we may find $\psi(g,h)$ without computing all of (1). Put $H/G' = \mathsf{O}_{p'}(G/G')$, and suppose $gH = g_1^{a_1} \cdots g_n^{a_n} H$ and $hH = g_1^{b_1} \cdots g_n^{b_n} H$. Then $\psi(g,h)$ is entry $(g_i^{a_i}, g_i^{b_i})$ of $M_{i,j}$.

Now we turn to T. Assume we have computed a Schur cover D of G, so that D has a recognised central subgroup $M \cong H_2(G)$ with $M \leq D'$ and $D/M \cong G$. Also assume that

(i) we can solve the word problem in D;

(ii) we have an isomorphism $\theta\colon G \to D/M$;

(iii) we have a transversal function $\sigma\colon D/M \to D$ that assigns to each coset of M in D exactly one of its elements, where that element is 1_D if the coset is M.

The first step in computing T is to find $\mu \in Z^2(G,M)$ arising from the central extension

$$1 \to M \xrightarrow{\text{inc.}} D \xrightarrow{\text{proj.}} D/M \to 1.$$

Using the transversal function σ, we define μ as follows:

$$\mu(g,h) = \sigma\theta(g)\sigma\theta(h)(\sigma\theta(gh))^{-1}.$$

Note that $\mu(g,h)$, as a product of elements and the inverse of an element in the image of σ, must be identified in the subgroup M of D.

Suppose that at this stage we have the entries of a cocyclic matrix for μ, where the matrix rows and columns are indexed by the elements of G in the order supplied. We must next construct a generating set for the group of all homomorphisms between the two finite abelian groups M and U. We now describe a procedure to do this. Naturally, it makes use of functor biadditivity and is similar to the procedure for computing I.

Denote by π_T the set of all primes dividing both $|M|$ and $|U|$. Fix $p \in \pi_T$. Let $\mathsf{O}_p(M) = \langle\, d_1 \,\rangle \times \cdots \times \langle\, d_n \,\rangle$, where $\langle\, d_i \,\rangle \cong C_{p^{e_i}}$, $e_i \geq 1$; and let $\mathsf{O}_p(U) = \langle\, u_1 \,\rangle \times \cdots \times \langle\, u_m \,\rangle$, where $\langle\, u_i \,\rangle \cong C_{p^{f_i}}$, $f_i \geq 1$. (This notation is independent of the notation used in the earlier discussion about I, but we are again suppressing its dependence on the choice of p.) Define for all i, $1 \leq i \leq n$, and all j, $1 \leq j \leq m$, the homomorphism $\phi_{i,j}\colon \langle\, d_i \,\rangle \to \langle\, u_j \,\rangle$ by

$$\phi_{i,j}(d_i) = \begin{cases} u_j^{p^{f_j - e_i}} & e_i < f_j \\ u_j & e_i \geq f_j. \end{cases}$$

Write $\overline{\phi}_{i,j}$ for the natural extension of $\phi_{i,j}$ to an element of $\mathrm{Hom}(M,U)$. (When computing $\overline{\phi}_{i,j}$, we also store its order, viz. $p^{\min\{e_i,f_j\}}$.) Then $\mathsf{O}_p(\mathrm{Hom}(M,U))$ is

$$\prod_{i=1}^{n}\prod_{j=1}^{m}\langle\, \overline{\phi}_{i,j} \,\rangle.$$

In connection with the next proposition, we note the last paragraph of [8, §3].

Proposition 2.2 *As p runs over π_T, the collection of all cocycles $\overline{\phi}_{i,j} \circ \mu$, where μ and $\overline{\phi}_{i,j}$ are defined as above (and i,j range as indicated, according to p), is a complete and irredundant set of representatives for the elements in a generating set of T.*

Remark 2.3 At the heart of our method for determining the splitting subgroup T of $H^2(G,U)$ is a transgression $\mathrm{Hom}(H_2(G),U) \hookrightarrow H^2(G,U)$. In principle, the entire problem of computing cocycles may be viewed as computing the image of another transgression, implicit in work of Horadam and de Launey. Let $R_2(G)$ be the abelian group on generators (g,h), $g,h \in G$, with relations $(g,h)(gh,k) = (g,hk)(h,k)$ for all $g,h,k \in G$. Put $R_2^*(G) = R_2(G)/\langle\,(1,1)\,\rangle$. In [13, Lemma 11.1], it is shown that $\mathrm{Hom}(R_2^*(G),U) \cong Z^2(G,U)$. Let F/R be the standard presentation of G; that is, F is free on $\{x_g \mid g \in G,\, g \neq 1\}$, and R is the kernel of the epimorphism $F \to G$ defined by $x_g \mapsto g$. We have an isomorphism θ of $R_2^*(G)$ onto $R/[R,F]$ induced by the epimorphism of $R_2(G)$ onto $R/[R,F]$ defined by $(g,h) \mapsto x_g x_h x_{gh}^{-1}[R,F]$, where x_1 is set to be 1. (Since $R/[R,F] \cong \mathbb{Z}^{|G|-1} \times H_2(G)$, a consequence of this observation is that $|Z^2(G,U)| = |U|^{|G|-1}|\mathrm{Hom}(H_2(G),U)|$.) Then $\mu \in Z^2(G,R_2^*(G))$ defined by $\mu(g,h) = (g,h)$ arises in the usual fashion from the central extension

$$1 \to R_2^*(G) \xrightarrow{\theta} F/[R,F] \xrightarrow{\varrho} G \to 1,$$

for the transversal function that sends $g \in G$ to $x_g[R,F] \in F/[R,F]$, where ϱ is natural projection composed with an isomorphism of F/R onto G. Further, the map $\lambda\colon \mathrm{Hom}(R_2^*(G),U) \to Z^2(G,U)$ defined by

$$\lambda(\phi)(g,h) = \phi((g,h)) = \phi \circ \mu(g,h)$$

is clearly an isomorphism, and composing this with natural projection onto $H^2(G,U)$ gives a transgression as in [16, Lemma 2.4.2]. To calculate $H^2(G,U)$ for nontrivial G with this transgression, we work in the finitely generated infinite group $F/[R,F]$, whereas with our choice of transgression we work in a Schur cover which is a finite subquotient of $F/[R,F]$.

In this section we have shown how to obtain a set of representatives for primary invariant generators of $H^2(G,U)$ as cocyclic matrices. It is easy to get representatives for all elements of $H^2(G,U)$ by forming entrywise products of the generators.

3 Determining central extensions

For $\psi \in Z^2(G,U)$, the associated canonical central extension E_ψ of U by G has as elements all (g,u), $g \in G, u \in U$, with multiplication defined by $(g,u)(h,v) = (gh, uv\psi(g,h))$. If E is any central extension of U by G then we may choose a transversal function for the cosets of U in E such that E is equivalent (and hence isomorphic) to E_ψ, where ψ is the cocycle arising from the transversal function. The set $\{[E_\psi] \mid \psi \in Z^2(G,U)\}$ of equivalence classes is in one-one correspondence with $H^2(G,U)$ and becomes an abelian group under Baer addition; this group is isomorphic to $H^2(G,U)$. Therefore $|H^2(G,U)|$ is an upper bound for the number of different isomorphism types of central extensions of U by G. This bound can be sharpened by calculating orbits in $H^2(G,U)$ under a familiar action of $\mathrm{Aut}(G) \times \mathrm{Aut}(U)$ on $H^2(G,U)$; see [5, Lemma 4.4] or [9, Theorem 2.2].

If enough entries of a cocyclic matrix for ψ are known, then E_ψ is known, for we can write down a presentation of this extension in an elementary way which we now briefly explain.

Suppose G has presentation

$$\langle\, x_1, \ldots, x_m \mid r_1 = \cdots = r_n = 1 \,\rangle$$

where $r_i = r_i(x_1, \ldots, x_m)$ is a word in the x_is: say $r_i = x_{i.1}^{\epsilon.1} \cdots x_{i.k_i}^{\epsilon.k_i}$, where $k_i \geq 1$ and each $\epsilon.j$ is 1 or -1. Let U be in primary invariant form: say

$$U = \langle\, u_1, \ldots, u_s \mid u_i^{\eta.i} = 1,\ [u_i, u_j] = 1 \ \ \forall\, i,j,\ 1 \leq i < j \leq s \,\rangle,$$

where $\eta.i$ is a prime power for all i. Then E_ψ has presentation

$$\begin{aligned} \langle\, e_1, \ldots, e_m, u_1, \ldots, u_s \mid r_1(e_1, \ldots, e_m) &= w_1, \ldots, r_n(e_1, \ldots, e_m) = w_n, \\ u_i^{\eta.i} &= 1,\ [u_i, u_j] = 1 \ \ \forall\, i,j,\ 1 \leq i < j \leq s, \\ [e_i, u_j] &= 1 \ \ \forall\, i,j,\ 1 \leq i \leq m,\ 1 \leq j \leq s \,\rangle, \end{aligned} \tag{2}$$

where the w_i are elements of U found as follows. Clearly, e_i stands for $(x_i, 1)$ in E_ψ, and so e_i^{-1} stands for $(x_i^{-1}, \psi(x_i, x_i^{-1})^{-1})$. Thus w_i is the projection in U of

$$(\, x_{i.1}^{\epsilon.1},\ \psi(x_{i.1}, x_{i.1}^{-1})^{(\epsilon.1-1)/2}\,) \cdots (\, x_{i.k_i}^{\epsilon.k_i},\ \psi(x_{i.k_i}, x_{i.k_i}^{-1})^{(\epsilon.k_i-1)/2}\,). \tag{3}$$

After performing the multiplication in E_ψ that brackets leftmost pairs of elements of E_ψ in (3), we see that

$$w_i = \prod_{j=2}^{k_i} \psi(\, x_{i.1}^{\epsilon.1} \cdots x_{i.(j-1)}^{\epsilon.(j-1)},\, x_{i.j}^{\epsilon.j}\,) \prod_{j=1}^{k_i} \psi(\, x_{i.j},\, x_{i.j}^{-1}\,)^{(\epsilon.j-1)/2} \tag{4}$$

for $k_i \geq 2$. The alternative multiplication strategy yields the same element of U, since ψ is a cocycle.

For each i, we compute the values of ψ appearing in (4) by the algorithm of Section 2, and hence obtain the presentation (2) of E_ψ.

A more specific and detailed exposition of these ideas is in [5, §4.1].

4 An implementation

Our implementation of these algorithms is distributed as part of Magma.

Let G be a finitely presented group. We can compute a Schur cover D of G using the Magma function `Darstellungsgruppe`, and also identify the Schur multiplier M of G in D.

As indicated earlier, we assume that the description of G allows us to solve the word problem. In practice, we currently assume that G is a finite soluble group, so that it has a power-conjugate presentation. For a treatment of such presentations, see [19, Chapter 9]. Under these assumptions, it is easy to fulfill the requirements (i)-(iii) listed in Section 2 needed to compute T. We plan to extend our implementation to accept other computationally effective descriptions of G.

A generating set for the group of all homomorphisms from one finite abelian group to another can also be readily computed in Magma, following Section 2.

Our implementation produces representatives for the elements in a generating set for $H^2(G,U)$ as cocyclic matrices and identifies the isomorphism type of $H^2(G,U)$. Employing the ideas in Section 3, it returns presentations for the corresponding central extensions of U by G. As we previously observed, calculation of these presentations may be achieved without completely calculating the cocyclic matrices.

5 Application to relative difference sets

Our machinery for computing cocycles may be applied to the generation of (normal) relative difference sets. We adopt the standard definition of *relative (v, m, k, λ)-difference set* in a group E of order vm, relative to a normal subgroup N of order m: it is a k-set D of elements of E such that in the multiset

$$\{de^{-1} \mid d, e \in D,\, d \neq e\},$$

each element of E not in N occurs λ times and no element of N occurs (N is the "forbidden subgroup"). For material on relative difference sets, see [6] or [18].

Let U be the cyclic group $\langle -1 \rangle$ of order 2. We say that $\psi \in Z^2(G, U)$ is *orthogonal* if a cocyclic matrix for ψ is Hadamard. If ψ is orthogonal and $|G| > 2$, then $|G|$ is divisible by 4. From now on, unless stated otherwise, we will assume that $|G| = 4t$ for some $t \geq 1$. See [14] for pertinent theory of cocyclic Hadamard matrices.

Theorem 5.1 ([3, Theorem 2.5, Corollary 2.6])

(i) *If D is a relative $(4t, 2, 4t, 2t)$-difference set in a group E relative to a normal subgroup $N \cong U$, then D is a transversal for the cosets of N in E and $\psi \in Z^2(E/N, U)$ arising from this transversal is orthogonal.*

(ii) *$\psi \in Z^2(G, U)$ is orthogonal if and only if $\{(g, 1) \mid g \in G\}$ is a relative $(4t, 2, 4t, 2t)$-difference set in E_ψ relative to U.*

Thus, the search for relative $(4t, 2, 4t, 2t)$-difference sets in (necessarily) central extensions of U by G, relative to U, is precisely the search for orthogonal elements of $Z^2(G, U)$. The question of whether orthogonal cocycles exist for all t is unresolved (see [14, Problem 5.4]): this is a special case of the Hadamard conjecture that there is a $4t \times 4t$ Hadamard matrix for all positive t. A non-constructive argument in [2], based on knowledge of Williamson Hadamard matrices, implies that relative $(4t, 2, 4t, 2t)$-difference sets exist for $1 \leq t \leq 25$. More general discussion about families of relative $(4t, 2, 4t, 2t)$-difference sets is in [3, §4].

Corollary 5.2 *Let $\psi \in Z^2(G,U)$, and let ϕ be a normalised set map from G to U. Then $\{(g,\phi(g)) \mid g \in G\}$ is a relative $(4t,2,4t,2t)$-difference set in E_ψ relative to U if and only if $\psi \cdot \partial\phi$ is orthogonal.*

Proof. The assignment $(g,u) \in E_{\psi\cdot\partial\phi} \mapsto (g, u\phi(g)) \in E_\psi$ defines an isomorphism respecting U. The corollary now follows from Theorem 5.1. □

Corollary 5.2 exhibits all normalised relative $(4t,2,4t,2t)$-difference sets with forbidden subgroup U in a given extension of U by G. Next we outline a direct method of constructing such difference sets (if indeed any exist).

First we compute $Z^2(G,U)$. Our algorithm yields a generating set for $H^2(G,U)$, which leaves us to compute $B^2(G,U)$. A coboundary $\partial\phi$ has matrix that is equivalent to the ("group-developed") matrix obtained from overwriting each entry in the multiplication table of G with its image under ϕ. But if $\mathsf{O}_2(G/G') \neq 1$ then a given coboundary $\partial\phi$ may arise from more than one normalised map $\phi\colon G \to U$. For suppose $\mathsf{O}_2(G/G')$ and $\mathsf{O}_2(H_2(G))$ have ranks r and s respectively: then $|Z^2(G,U)| = 2^{|G|-1+s}$ and $|B^2(G,U)| = 2^{|G|-1-r}$ (see Remark 2.3 for the first statement, from which the second follows at once by the Universal Coefficient Theorem). Suppose that $\partial\phi_1 = \partial\phi_2$ and that $\psi \cdot \partial\phi_1$ is orthogonal for some $\psi \in Z^2(G,U)$. We surely do not want to distinguish between the two relative difference sets in $E_{\psi\cdot\partial\phi}$ guaranteed by Corollary 5.2, for $\phi = \phi_1$ and $\phi = \phi_2$. And indeed they are equivalent, under the standard notion of equivalence of relative difference sets given in [18, p. 198]. For instance, they are equivalent if they correspond under an automorphism of $E_{\psi\cdot\partial\phi_1}$ leaving U invariant. Such an automorphism is defined by $(g,u) \mapsto (g, u\phi_1(g)\phi_2(g))$. On a related note, suppose $[\psi]$ and $[\chi]$ are in the same orbit under the $\mathrm{Aut}(G)$-action on $H^2(G,U)$ mentioned in Section 3. Then it is easily seen that E_ψ and E_χ are isomorphic by an isomorphism that fixes U elementwise and gives a bijection from the collection of all relative $(4t,2,4t,2t)$-difference sets with forbidden subgroup U in one extension to the collection of all such relative difference sets in the other.

See [12] for a lengthier exploration of relative difference set equivalence in cohomological terms. Since we do not seek a full classification of relative difference sets in central extensions, we will not consider further this equivalence criterion.

Suppose that each element of $Z^2(G,U)$ has been computed as a cocyclic matrix, or an equivalent one obtained from a cocyclic matrix by pre- or post-multiplication by a ± 1-permutation matrix. We then test whether each matrix is Hadamard by taking the scalar product of its first row with every other row: the matrix is Hadamard if and only if these products are all zero (see [14, Lemma 1.4]).

Assume we have a cocyclic Hadamard matrix over G. By the MAGMA procedures, we know the cocycle in question as $\psi \cdot \partial\phi$, where ψ is in the calculated set of representatives for the elements of $H^2(G,U)$, and ϕ is also known (in worst-case, all normalised maps from G to U are evaluated). An ordering $g_1, \ldots, g_{4t}$ of the elements of G indexes the rows and columns of a matrix for ψ and a group-developed matrix for ϕ. Write $(g_i, 1) \in E_\psi$ as f_i and the first row of a group developed matrix for ϕ as $u_1 \, \ldots \, u_{4t}$. Then by Corollary 5.2, a relative $(4t, 2, 4t, 2t)$-difference set in E_ψ relative to U is

$$\{f_1 u_1, \ldots, f_{4t} u_{4t}\}.$$

Our objective in the sequel is to determine, for $1 \le t \le 3$ and each isomorphism type E of group of order $8t$ with a central subgroup $U \cong \mathbb{Z}_2$, existence or otherwise of relative $(4t, 2, 4t, 2t)$-difference sets in E with forbidden subgroup U. We provide an example of such relative difference sets if they exist.

If there is an orthogonal coboundary over G then t is a square. Thus, for $2 \le t \le 3$, there are no relative difference sets in $G \times U$ relative to U. This is not to say there are no difference sets in $G \times U$ relative to some other central (and of course non-splitting) subgroup of order 2. Suppose $|G| = 4s^2$. A *Menon-Hadamard difference set in* G is a relative difference set in G with parameters $(4s^2, 1, 2s^2 - s, s^2 - s)$, or its complement, with parameters $(4s^2, 1, 2s^2 + s, s^2 + s)$. If $\partial\phi$ is an orthogonal coboundary, then the characteristic set of ϕ is a Menon-Hadamard difference set in G (see [3, Theorem 2.7]). In this way one may easily write down a Menon-Hadamard difference set in G given a relative difference set in $G \times U$, and vice versa. We illustrate this below.

For each of $t = 1$ and 2, we use the MAGMA implementation of the p-group isomorphism testing algorithm of [17] to identify the distinct isomorphism types of extensions that occur. For $t = 3$, we observe that if $H^2(G,U)$

has elements containing orthogonal cocycles, then it has just one, and the isomorphism type of the corresponding extension of U by G is uniquely determined by G. The notation $O\#n$ will refer to the nth group of order O in the `SmallGroups` library distributed with both GAP and MAGMA.

Details are similar in every case, and so we describe compilation of the list only for $t = 2$. Here, there are 128 normalised set maps $G \to U$, yet $|B^2(G,U)|$ is 32 when G is nonabelian or $\mathbb{Z}_2 \times \mathbb{Z}_4$, 16 when G is elementary abelian, and 64 when G is cyclic. By [9, Lemma 5.2], G cannot in fact be cyclic. Since Q_8 has trivial multiplier, $H^2(Q_8,U) \cong \mathrm{Ext}(Q_8/Q_8', U) \cong \mathbb{Z}_2^{(2)}$. After testing the elements of the nontrivial cocycle classes, we find none are orthogonal. Only four of the eight cohomology classes in $H^2(D_8,U)$ contain orthogonal cocycles. Two of these classes correspond to extensions isomorphic to 16#3. The remaining classes have associated extensions isomorphic to 16#9 or 16#4. (Examples of orthogonal cocycles over D_8 are also given in [9].) Only half of the cohomology classes in $H^2(\mathbb{Z}_2 \times \mathbb{Z}_4, U) \cong \mathbb{Z}_2^{(3)}$ contain orthogonal elements. One of these corresponds to $\mathbb{Z}_4^{(2)}$, two to $\mathbb{Z}_2 \times \mathbb{Z}_8$, and the remaining one to 16#4. There are orthogonal cocycles in each nontrivial cohomology class in $H^2(\mathbb{Z}_2^{(3)}, U) \cong \mathbb{Z}_2^{(6)}$. (We expect that a determination of the $\mathrm{Aut}(G)$-orbits in $H^2(G,U)$ would allow us to process a much smaller number of classes.) Seven classes give rise to abelian extensions, all isomorphic to $\mathbb{Z}_2^{(2)} \times \mathbb{Z}_4$. Otherwise, an extension has no elements of order greater than 4 and Frattini subgroup of order 2, so is isomorphic to one of 16#11, 16#12, or 16#13. After checking the first 13 cocycles returned by the MAGMA procedures, we find that all of these isomorphism types occur.

In summary: of the 14 nonisomorphic groups of order 16, precisely 9 have relative $(8,2,8,4)$-difference sets relative to some central subgroup of order 2.

Now we list power-conjugate presentations for all groups of orders 8, 16 and 24 in which relative difference sets with forbidden subgroup of order 2 exist. We write the forbidden subgroup as $U = \langle\, u \,\rangle$. The usual convention, followed throughout, is that trivial conjugate relations are not included in a presentation. We identify each group in the `SmallGroups` library. Immediately after each presentation we give an example of a relative difference set with forbidden subgroup U contained in the group with that presentation. Groups E numbered in the ranges $\mathbf{2}-\mathbf{3}$, $\mathbf{4}-\mathbf{5}$, $\mathbf{6}-\mathbf{8}$ and $\mathbf{9}-\mathbf{12}$ have E/U isomorphic to

$\mathbb{Z}_2^{(2)}$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, D_8 and $\mathbb{Z}_2^{(3)}$, respectively. Groups E numbered **1**, **13**, **14** and **15** have E/U isomorphic to $\mathbb{Z}_4$, A_4, D_{12} and $\mathbb{Z}_2^{(2)} \times \mathbb{Z}_3$, respectively. Yet this quotient may not be uniquely determined: E may have a central subgroup $U' \neq U$ that occurs as forbidden subgroup in a relative $(4t, 2, 4t, 2t)$-difference set in E, with $E/U' \not\cong E/U$. This happens for both $E \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ and $E \cong$ 16#4; in the latter case, $E/U' \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ for some such U'. For all other listed E, E/U is uniquely determined (of course, at order 24, E has just one central subgroup of order 2).

1. $8\#2 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ $\langle e_1, e_2, u \mid e_1^2 = e_2,\ e_2^2 = 1,\ u^2 = 1 \rangle$
$\{1,\ e_1u,\ e_2,\ e_1e_2\}$.

2. $8\#4 \cong Q_8$ $\langle e_1, e_2, u \mid e_1^2 = u,\ e_2^2 = u,\ u^2 = 1,\ e_2^{e_1} = e_2u \rangle$
$\{1,\ e_1,\ e_2,\ e_1e_2\}$.

3. $8\#5 \cong \mathbb{Z}_2^{(3)}$ $\langle e_1, e_2, u \mid e_1^2 = 1,\ e_2^2 = 1,\ u^2 = 1 \rangle$
$\{1,\ e_1u,\ e_2,\ e_1e_2\}$.

4. $16\#2 \cong \mathbb{Z}_4^{(2)}$ $\langle e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = e_3,\ e_3^2 = 1,\ u^2 = 1 \rangle$
$\{1,\ e_1u,\ e_2,\ e_3,\ e_1e_2,\ e_1e_3u,\ e_2e_3u,\ e_1e_2e_3u\}$.

5. $16\#5 \cong \mathbb{Z}_2 \times \mathbb{Z}_8$ $\langle e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = e_3,\ e_3^2 = u,\ u^2 = 1 \rangle$
$\{1,\ e_1,\ e_2u,\ e_3u,\ e_1e_2,\ e_1e_3,\ e_2e_3,\ e_1e_2e_3\}$.

6. 16#3 $\langle e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = e_3u,\ e_3^2 = 1,\ u^2 = 1,$
$e_2^{e_1} = e_2e_3 \rangle$
$\{1,\ e_1u,\ e_2,\ e_3,\ e_1e_2u,\ e_1e_3u,\ e_2e_3u,\ e_1e_2e_3\}$.

7. 16#4 $\langle e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = e_3,\ e_3^2 = 1,\ u^2 = 1,$
$e_2^{e_1} = e_2u \rangle$
$\{1,\ e_1,\ e_2,\ e_3,\ e_1e_2,\ e_1e_3,\ e_2e_3u,\ e_1e_2e_3u\}$.

8. 16#9 $\langle\, e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = e_3 u,\ e_3^2 = u,\ u^2 = 1,$
$e_2^{e_1} = e_2 e_3,\ e_3^{e_1} = e_3 u \,\rangle$
$\{\, 1,\ e_1 u,\ e_2,\ e_3,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3,\ e_1 e_2 e_3 \,\}\,.$

9. 16#10 $\cong \mathbb{Z}_2^{(2)} \times \mathbb{Z}_4$ $\langle\, e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = u,\ e_3^2 = u,\ u^2 = 1 \,\rangle$
$\{\, 1,\ e_1,\ e_2,\ e_3,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3,\ e_1 e_2 e_3 \,\}\,.$

10. 16#11 $\cong \mathbb{Z}_2 \times D_8$ $\langle\, e_1, e_2, e_3, u \mid e_1^2 = 1,\ e_2^2 = u,\ e_3^2 = u,\ u^2 = 1,$
$e_2^{e_1} = e_2 u,\ e_3^{e_1} = e_3 u \,\rangle$
$\{\, 1,\ e_1 u,\ e_2 u,\ e_3,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3,\ e_1 e_2 e_3 \,\}\,.$

11. 16#12 $\cong \mathbb{Z}_2 \times Q_8$ $\langle\, e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = u,\ e_3^2 = u,\ u^2 = 1,$
$e_2^{e_1} = e_2 u,\ e_3^{e_1} = e_3 u,\ e_3^{e_2} = e_3 u \,\rangle$
$\{\, 1,\ e_1,\ e_2,\ e_3,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3,\ e_1 e_2 e_3 \,\}\,.$

12. 16#13 $\langle\, e_1, e_2, e_3, u \mid e_1^2 = u,\ e_2^2 = u,\ e_3^2 = u,\ u^2 = 1,$
$e_3^{e_2} = e_3 u \,\rangle$
$\{\, 1,\ e_1,\ e_2,\ e_3,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3,\ e_1 e_2 e_3 \,\}\,.$

13. 24#3 $\langle\, e_1, e_2, e_3, u \ \mid e_1^3 = 1,\ e_2^2 = u,\ e_3^2 = u,\ u^2 = 1,$
$e_2^{e_1} = e_2 e_3,\ e_3^{e_1} = e_2,\ e_3^{e_2} = e_3 u \,\rangle$
$\{\, 1,\ e_1,\ e_2 u,\ e_3 u,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3 u,\ e_1 e_2 e_3,$
$e_1^2,\ e_1^2 e_2,\ e_1^2 e_3,\ e_1^2 e_2 e_3 \,\}\,.$

14. 24#4 $\langle\, e_1, e_2, e_3, u \ \mid e_1^2 = u,\ e_2^2 = u,\ e_3^3 = 1,\ u^2 = 1,$
$e_2^{e_1} = e_2 u,\ e_3^{e_1} = e_3^2 \,\rangle$
$\{\, 1,\ e_1 u,\ e_2 u,\ e_3 u,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3,\ e_1 e_2 e_3,$
$e_3^2 u,\ e_1 e_3^2,\ e_2 e_3^2,\ e_1 e_2 e_3^2 \,\}\,.$

15. 24#11 $\langle\, e_1, e_2, e_3, u \ \mid e_1^3 = 1,\ e_2^2 = u,\ e_3^2 = u,\ u^2 = 1,$
$e_3^{e_2} = e_3 u \,\rangle$
$\{\, 1,\ e_1 u,\ e_2 u,\ e_3 u,\ e_1 e_2,\ e_1 e_3,\ e_2 e_3,\ e_1 e_2 e_3,\ e_1^2 u,$
$e_1^2 e_2,\ e_1^2 e_3,\ e_1^2 e_2 e_3 \,\}\,.$

Only two of the nonabelian extensions in the preceding list, namely 16#11 and 16#12, contain a splitting subgroup of order 2. Further, the difference sets in **1** and **3** arise from orthogonal coboundaries, from which we derive the Menon-Hadamard difference sets $\{1,\ e_2,\ e_1e_2\}$ in $\langle e_1, e_2 \mid e_1^2 = e_2,\ e_2^2 = 1\rangle$ and $\{1,\ e_2,\ e_1e_2\}$ in $\langle e_1, e_2 \mid e_1^2 = e_2^2 = 1\rangle$. A more interesting example is the elementary abelian group G of order 16 on generators e_1, e_2, e_3, e_4, which has Menon-Hadamard difference set

$$\{1,\ e_4,\ e_2e_3,\ e_3e_4,\ e_1e_3e_4,\ e_1e_2e_3e_4\}$$

derived from the relative $(16, 2, 16, 8)$-difference set

$$\{1,\ e_1u,\ e_2u,\ e_3u,\ e_4,\ e_1e_2u,\ e_1e_3u,\ e_1e_4u,\ e_2e_3,\ e_2e_4u,\ e_3e_4,\ e_1e_2e_3u,\\ e_1e_2e_4u,\ e_1e_3e_4,\ e_2e_3e_4u,\ e_1e_2e_3e_4\}$$

in $G \times U$ relative to U, computed as above.

Using Magma V2.4 on a Sun UltraSPARC Enterprise 4000 server, it takes approximately 10 minutes of CPU time to compute the results presented here.

Our somewhat naïve approach is limited to groups of small order, since the search space for orthogonal cocycles grows exponentially with group order. In an attempt to address this limitation, our implementation permits random sampling of the search space. We are not aware of any general approach to reduce significantly the exponential complexity of the task. Results obtained by Ito apply in particular cases to exclude some cohomology classes from a search for orthogonal cocycles: for example, [15, Proposition 7] implies that there are no orthogonal cocycles over $\mathbb{Z}_4 \times \mathbb{Z}_3$ nor over 12#1. On the other hand, computational evidence suggests that dihedral and elementary abelian groups are good sources of orthogonal cocycles. The basic case for the latter type of group is covered by the proof of Dillon's conjecture in [4], which implies existence of an orthogonal coboundary over every elementary abelian 2-group of even rank.

References

[1] Wieb Bosma, John Cannon and Catherine Playoust (1997), "The Magma Algebra System I: The User Language", *J. Symbolic Comput.* **24**, 235–265.

[2] W. de Launey and K.J. Horadam (1993), "A weak difference set construction for higher dimensional designs", *Des. Codes Cryptogr.* **3**, 75–87.

[3] W. de Launey, D.L. Flannery and K.J. Horadam, "Cocyclic Hadamard matrices and difference sets", *Discrete Appl. Math.*, to appear.

[4] A. Drisko (1998), "Transversals in row-Latin rectangles", *J. Combin. Theory Ser. A* **84** (no. 2), 181–195.

[5] Bettina Eick and E.A. O'Brien (1999), "Enumerating p-groups", *J. Austral. Math. Soc. Ser. A*.

[6] J.E.H. Elliott and A.T. Butson (1966), "Relative difference sets", *Illinois J. Math.* **10**, 517–531.

[7] G. Ellis and I. Kholodna, "Computing second cohomology of finite groups with trivial coefficients", *Homology, Homotopy and Applications*, to appear.

[8] D.L. Flannery (1996), "Calculation of cocyclic matrices", *J. Pure Appl. Algebra* **112**, 181–190.

[9] D.L. Flannery (1997), "Cocyclic Hadamard matrices and Hadamard groups are equivalent", *J. Algebra* **192**, 749–779.

[10] The GAP Team (1998), GAP – *Groups, Algorithms, and Programming, Version* 4. Lehrstuhl D für Mathematik, RWTH Aachen, and School of Mathematical and Computational Sciences, University of St Andrews.

[11] D.F. Holt (1984), "The Calculation of the Schur Multiplier of a Permutation Group", *Computational Group Theory,* (Durham, 1982), pp. 307–318. Academic Press, London, New York.

[12] K.J. Horadam (1998), "Central relative $(v, w, v, v/w)$-difference sets", Research Report No. 3, Royal Melbourne Institute of Technology.

[13] K.J. Horadam and W. de Launey (1993), "Cocyclic development of designs" *J. Algebraic Combin.* **2**, 267–290.

[14] K.J. Horadam and W. de Launey (1995), "Generation of cocyclic Hadamard matrices", in *Computational Algebra and Number Theory*, W. Bosma and A. van der Poorten (eds.), pp. 279–290. Kluwer Academic, Dordrecht.

[15] N. Ito (1994), "On Hadamard groups", *J. Algebra* **168**, 981–987.

[16] Gregory Karpilovsky (1987), *The Schur multiplier.* Clarendon Press, Oxford.

[17] E.A. O'Brien (1994), "Isomorphism testing for p-groups", *J. Symbolic Comput.* **17**, 133–147.

[18] A. Pott (1996), "A survey on relative difference sets", in *Groups, difference sets and the Monster*, (Columbus, OH, 1993), pp. 195–232. Walter de Gruyter, Berlin.

[19] Charles C. Sims (1994), *Computation with finitely presented groups.* Cambridge University Press.