Journal of Algebraic Combinatorics, 2 (1993), 267–290
© Kluwer Academic Publishers, Boston. Manufactured in The Netherlands.

Cocyclic Development of Designs

K.J. HORADAM AND W. DE LAUNEY
Cryptomathematics Research, Communications Division, Electronics Research Laboratory, Defence Science and Technology Organisation, Australia.

Received July 10, 1992; Revised March 25, 1993

Abstract. We present the basic theory of *cocyclic development* of designs, in which group development over a finite group G is modified by the action of a cocycle defined on $G \times G$. Negacyclic and ω-cyclic development are both special cases of cocyclic development.

Techniques of design construction using the group ring, arising from difference set methods, also apply to cocyclic designs. Important classes of Hadamard matrices and generalized weighing matrices are cocyclic.

We derive a characterization of cocyclic development which allows us to generate all matrices which are cocyclic over G. Any cocyclic matrix is equivalent to one obtained by entrywise action of an asymmetric matrix and a symmetric matrix on a G-developed matrix. The symmetric matrix is a Kronecker product of back ω-cyclic matrices, and the asymmetric matrix is determined by the second integral homology group of G.

We believe this link between combinatorial design theory and low-dimensional group cohomology leads to (i) a new way to generate combinatorial designs; (ii) a better understanding of the structure of some known designs; and (iii) a better understanding of known construction techniques.

Keywords: orthogonal design, Hadamard matrix, difference set, group development, negacyclic development, ω-cyclic development, cocycle, cohomology group, homology group, extension group

1. Introduction

This paper describes a connection between combinatorial design theory and low-dimensional group cohomology. We believe this link leads to (i) a new way to generate combinatorial designs; (ii) a better understanding of the structure of some known designs; and (iii) a better understanding of known construction techniques.

In [3] de Launey introduced a general method for developing a design from its initial row. It extends the technique of group development modulo a finite group G and incorporates the techniques of negacyclic and ω-cyclic development. The method arose as a characterization of those (2-dimensional) combinatorial designs which can be extended in a particular way to give higher-dimensional designs whose axis-normal 2-dimensional sections satisfy the defining properties of

AMS Classification (1991): 05B10, 05B15, 05B20, 20J06.
See end of article for author addresses.

the original design. Specifically, ordinary group development over G is modified by the action of what we term here a *cocyclic development function* defined on $G \times G$. In [4], we showed that the designs so developed have a type of difference set construction based on an extension of G. This *cocyclic development* is far less restrictive than group development: in [3, 4] a number of known families of Hadamard matrices and orthogonal designs are shown to be cocyclic and in [4] it is conjectured that cocyclic Hadamard matrices exist for all orders $n \equiv 0 \pmod 4$.

Here, we present the basic theory of this development technique and describe its link with the low-dimensional cohomology of G.

In §2 and §3, we introduce the concepts of a *pairwise combinatorial design (PCD)* and a *weak difference set*. The *PCDs* provide a setting for our development theory, and weak difference sets are a generalization of difference sets. In §4 and §5, *cocyclic development functions* and *cocyclic PCDs* are described and related to weak difference sets and to the *abelian extension functions (AEFs)* of [4]. In §6 and §7, some fundamental extension properties of cocyclic *PCDs* are deduced. In §8 we pose three basic combinatorial questions about the cocyclic development of designs, and in §9 we present the main computational tool for this general theory: the *development table·* for G.

The remainder of the paper relates to the third basic question: given G, what are the cocyclic development functions over G? In §10, an AEF is identified as a 2-dimensional cocycle, which permits us in §11 and §12 to describe the group of $AEFs$ in terms of the second cohomology group of G. This connection is used in §13 to prove that a cocyclic matrix is equivalent to one constructed from an underlying group developed matrix by an entrywise action of a matrix possessing a natural decomposition into asymmetric and symmetric parts. The asymmetric matrix is determined by the second integral homology group of G and the symmetric matrix, determined by the first integral homology group of G, is a Kronecker product of back ω-cyclic matrices. The (Hadamard) product of these two matrices is the *minimal* development table for G and is isomorphic to the second cohomology group of G.

2. Pairwise combinatorial designs

Definition 2.1. Let X and Y be $m \times n$ matrices; we say Y is *equivalent to* X (written $X \sim Y$) if Y can be obtained from X by applying a sequence of row or column permutations. If $X = [x_{ij}]$, the equivalence class $\mathcal{X}$ containing X is called a *configuration*, and is denoted by parentheses: $\mathcal{X} = (x_{ij})$.

We introduce notation to specify a generalized inner product constraint on pairs of rows occurring in a design: let S be a finite set with at least two elements, and let Λ be a nonempty subset of the set of $2 \times n$ $(n \geq 1)$ configurations with entries from S. Let Π_S denote the group of permutations on S, and let Π_Λ denote the largest group of maps π in Π_S such that, for all configurations $\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \end{pmatrix}$ in Λ, $\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \pi(y_1) & \pi(y_2) & \cdots & \pi(y_n) \end{pmatrix}$ is also in Λ.

Definition 2.2. Let X and Y be $v \times v$ matrices over S; we say Y is *Λ-equivalent to* X (written $X \sim_\Lambda Y$) if Y can be obtained from X by a sequence of the operations:

(i) the rows or columns are permuted, or

(ii) a row or column $[x_i]$, $1 \leq i \leq v$ is replaced by the row or column $[\pi(x_i)], 1 \leq i \leq v$, for some $\pi \in \Pi_\Lambda$.

Similarly, the configurations $\mathcal{X}$ and $\mathcal{Y}$ inherit Λ-equivalence from their representatives X and Y.

We introduce a class of configurations which is closed under Λ-equivalence.

Definition 2.3. A *pairwise combinatorial design* $PCD(v, \Lambda)$ is a $v \times v$ configuration (x_{ij}) with entries from S such that, for all $s \neq t$, where $1 \leq s, t \leq v$, the $2 \times v$ configurations $\begin{pmatrix} x_{s1} & x_{s2} & \cdots & x_{sv} \\ x_{t1} & x_{t2} & \cdots & x_{tv} \end{pmatrix}$ and $\begin{pmatrix} x_{1s} & x_{2s} & \cdots & x_{vs} \\ x_{1t} & x_{2t} & \cdots & x_{vt} \end{pmatrix}$ lie in Λ.

Note the $(v, \Pi_R, \Pi_C, \beta, S)$-designs of [3, 4] include $PCD(v, \Lambda)$s. (Put $\Pi_R = \Pi_C = \Pi_\Lambda$, and let β be the constraint given in Definition 2.3.) Moreover (see [3], Examples 2.2–4.3), symmetric balanced incomplete block designs, Hadamard matrices, (balanced, generalized) weighing matrices, and orthogonal designs (*ODs*) are *PCDs* (In each case, these designs satisfy an orthogonality condition on their rows, and Λ lists the allowable pairs of orthogonal rows.)

3. Weak difference sets

The following notation is used:

(i) Let G be a finite group (multiplicatively written with identity 1) of order v. For indexing purposes it will be assumed throughout that G has a fixed order $G = \{a_1, a_2, \ldots, a_v\}$ where $a_1 = 1$.

(ii) If the rows and columns of a matrix X are indexed by G, this will be denoted by $X = [x_{a_i a_j}] (1 \leq i, j \leq v)$ or, more often, by $X = [x_{ab}] (a, b \in G)$.

A (v, k, λ)*-difference set over* G is a subset $D = \{d_1, d_2, \ldots, d_k\}$ of G such that the list of differences $d_i d_j^{-1} (1 \leq i, j \leq k, i \neq j)$ contains each nonidentity element of G exactly $\lambda (\geq 1)$ times. We may define a map $g_D : G \to \{0, 1\}$ so that $g_D(a) = 1$ if and only if $a \in D$. Then the $v \times v$ matrix $X = [g_D(a_i a_j)] (1 \leq i, j \leq v)$

is (the incidence matrix of) an $SBIBD(v, k, \lambda)$. (See, for example, [11, 1.II(2.2, 2.4)].) This process is reversible: if there exists a map $g : G \to \{0, 1\}$ such that $\mathcal{X} = (g(a_i a_j))(1 \leq i, j \leq v)$ is an $SBIBD(v, k, \lambda)$, then the set $\{a \mid a \in G \text{ and } g(a) = 1\}$ is a (v, k, λ)-difference set over G.

These standard concepts will now be generalized.

Definition 3.1. A *(v, Λ)-difference set over G* is a set $\{(a, g(a)) \mid a \in G\}$ where $g : G \to S$ is a map such that the $v \times v$ configuration $\mathcal{X} = (g(ab))\,(a, b \in G)$ is a $PCD(v, \Lambda)$.

Each (v, Λ)-difference set over G determines a $PCD(v, \Lambda)$ but the converse is generally not true. Nonetheless, a $PCD(v, \Lambda)$ may have a weaker difference set construction based on a group whose order is greater than v. It is on this idea that we now focus.

Definition 3.2. Suppose there exists a subset J of cardinality v of a group E and a map $g : E \to S$ such that the $v \times v$ configuration $\mathcal{X} = (g(ab))\,(a, b \in J)$ is a $PCD(v, \Lambda)$; then the set $\{(a, g(a)) \mid a \in E\}$ is called a *(v, Λ)-weak difference set over E.*

Example 3.1. Let $E = < i, j, k : i^2 = j^2 = k^2 = -1, ij = k >$ be the quaternions. Set $J = \{1, i, j, k\}$ and let S be the set of commuting indeterminates $\{0, \pm w, \pm x, \pm y, \pm z\}$. Then

$$D = \{(1, w), (i, x), (j, y), (k, z), (-1, -w), (-i, -x), (-j, -y), (-k, -z)\}$$

is a weak difference set which generates an $OD(4; 1, 1, 1, 1)$, $\mathcal{X}$, where

$$X = [g(ab)]_{a,b \in J} = \begin{bmatrix} w & x & y & z \\ x & -w & z & -y \\ y & -z & -w & x \\ z & y & -x & -w \end{bmatrix}.$$

Here Λ is the set of configurations $\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_2 \end{pmatrix}$ $x_i, y_i \in S$, $1 \leq i \leq n$, for which (in $\mathbf{Z}[w, x, y, z]$),

$$\sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} y_i^2 = \frac{n}{4}(w^2 + x^2 + y^2 + z^2) \text{ and } \sum_{i=1}^{n} x_i y_i = 0,$$

and $\Pi_\Lambda = \{\text{multiplication by } 1 \text{ or } -1\}$.

4. Development functions

The technique of f-developing a matrix from a row or column is described in the following definition. In [4] this is termed (f, G)-development.

Definition 4.1. Let $g : G \to S$ and $f : G \times G \to \Pi_S$ be set mappings. Then the matrix $X = [f(a, b)g(ab)]\,(a, b \in G)$ is said to be *f-developed from the row* $[g(a)]\,(a \in G)$ *by development function f (over G)*. We also say X is *f-developed from the column* $[g(b)]\,(b \in G)$. If f is the trivial map, then X is *G-developed*, or *group developed (over G)*. A configuration is said to be *f-developed* if it has a representative which is f-developed.

Of course, any matrix $[x_{ab}]$ over S is f-developed for some f and G: given g, define $f(a, b)$ to be any permutation such that $f(a, b)g(ab) = x_{ab}$. If f is unrestricted, the fact that a matrix is f-developed will imply nothing about its structure. We identify certain special properties which a development function may possess.

Definition 4.2. Let H be a group with identity 1 and let $f : G \times G \to H$ be a set mapping.

(i) We say f is *abelian* if, for all $a_i, a_j, b_i, b_j \in G$,

$$f(a_i, b_i)f(a_j, b_j) = f(a_j, b_j)f(a_i, b_i).$$

(ii) We say f is an *extension function* if for all $a, b, c \in G$,

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

(iii) We say f is *normalised* if $f(1, 1) = 1$.
(iv) We say f is a *suitable function* for $PCD(v, \Lambda)$s if $H = \Pi_\Lambda$.

The most critical of these is the "extension" property (ii). It determines the extension group of G used in the weak difference set construction of $PCD(v, \Lambda)$s, and permits extension of $PCD(v, \Lambda)$s to proper higher-dimensional designs (see Theorem 5.1 and §6 below).

Of most interest to us are functions possessing several of these properties.

Definition 4.3. Let H be a group with identity 1 and let $f : G \times G \to H$ be a set mapping.

(i) We say f is an *AEF* (abelian extension function) if it satisfies (i) and (ii) of Definition 4.2.
(ii) We say f is *Λ-robust* if it satisfies (ii) and (iv) of Definition 4.2.
(iii) We say f is a *Λ-cocyclic* development function if it satisfies (i), (ii), and (iv) of Definition 4.2. That is, it is a suitable *AEF* for $PCD(v, \Lambda)$s.

Berman's ω-cyclic matrices [1], and Delsarte's negacyclic matrices [5], are equivalent to matrices developed by an AEF. If $x_1, \ldots, x_v \in S$ and $\omega \in \Pi_S$, an *ω-cyclic matrix* has the form

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_{v-1} & x_v \\ \omega x_v & x_1 & \cdots & x_{v-2} & x_{v-1} \\ \vdots & \vdots & & \vdots & \vdots \\ \omega x_3 & \omega x_4 & \cdots & x_1 & x_2 \\ \omega x_2 & \omega x_3 & \cdots & \omega x_v & x_1 \end{bmatrix}.$$

Reversing the order of the columns of such a matrix gives a *back ω-cyclic matrix.* Negacyclic development sets ω equal to an element of order 2 (typically -1), and cyclic (group) development sets $\omega = 1$.

Example 4.1. (*ω-cyclic development*). If $G =< a : a^v = 1 >$ is cyclic, $g : G \rightarrow S$ is a set map and $\omega \in \Pi_S$, then a back ω-cyclic matrix is f-developed from the initial row $[g(a^i)](0 \leq i \leq v-1)$ by the AEF $f(a^i, a^j) = \omega^{\lfloor (i+j)/v \rfloor}$. The order of f (under the operation of pointwise multiplication of functions) is the same as the order of ω in Π_S.

The Λ-robust development functions f have the useful property that any row or column of an f-developed matrix may itself be f-developed to form a Λ-equivalent matrix. This can be seen for rows in equation (2) and for columns in equation (3) of the following equivalent definition of Λ-robustness.

THEOREM 4.1. *Let $f : G \times G \rightarrow \Pi_S$ be a development function; then f is Λ- robust if and only if, for every $a_0, b_0 \in G$, there exist maps $s_{a_0}, t_{b_0} : G \rightarrow \Pi_\Lambda$ and permutations σ_{a_0}, τ_{b_0} on G with the property that, for any map $g : G \rightarrow S$,*

$$f(a, b) \circ f(a_0, ab)g(a_0ab) = s_{a_0}(a) \circ f(\sigma_{a_0}(a), b)g(\sigma_{a_0}(a)b), \tag{2}$$

$$f(a, b) \circ f(ab, b_0)g(abb_0) = t_{b_0}(a) \circ f(a, \tau_{b_0}(b))g(a\tau_{b_0}(b)). \tag{3}$$

Proof. The forward implication follows on setting $s_{a_0}(a) = f(a_0, a)$, $t_{b_0}(b) = f(b, b_0)$, $\sigma_{a_0}(a) = a_0a$ and $\tau_{b_0}(b) = bb_0$. We prove the reverse implication. If (2) holds, let g run through all the constant functions to show that

$$f(a, b) \circ f(a_0, ab) = s_{a_0}(a) \circ f(\sigma_{a_0}(a), b),$$

and hence, because S has at least two elements, $\sigma_{a_0}(a) = a_0a$. Substituting back and setting $a = 1$, together with the corresponding results for columns, gives

$$f(1, b) = f(a, 1) = f(1, 1). \tag{4}$$

Hence $f(1,1)$ commutes with $f(a,b)$, and (1) follows. □

Now suppose f in Definition 4.2 is abelian. Since $f(G \times G)$ generates an *abelian* subgroup of H, we lose nothing by assuming that H is an abelian group C. Indeed, when H *is* abelian, there is a natural equivalence relation defined on $AEFs$ and hence on cocyclic development functions. Its origin is explained in §10.

Definition 4.4. Let C be an abelian group with identity 1.

(i) An equivalence relation $\sim$ is defined on the set of $AEFs : G \times G \to C$ to be:

$$f \sim f' \iff \exists\ \alpha : G \to C : f'(a,b) = \alpha(a)\alpha(b)(\alpha(ab))^{-1} f(a,b) \quad a, b \in G.$$

(So, the equivalence class of f is determined by those α which are not group homomorphisms.)

(ii) An $AEF\, f : G \times G \to C$ is termed *principal* if $f \sim \mathbf{1}$, where $\mathbf{1}$ is the trivial AEF which takes each (a,b) to 1.

We show that equivalent Λ-cocyclic development functions determine Λ-equivalent matrices.

LEMMA 4.1. *Let $f, f' : G \times G \to \Pi_\Lambda$ be AEFs, and let X be an f-developed matrix. If $f \sim f'$, then there exists an f'-developed matrix X' such that $X \sim_\Lambda X'$. In particular, if f is principal, then X is Λ-equivalent to a group developed matrix.*

Proof. If $X = [f(a,b)g(ab)]\,(a, b \in G)$, then there exists a mapping $\alpha : G \to C$ such that

$$X \sim_\Lambda [\alpha(a)\alpha(b)f(a,b)g(ab)] = [f'(a,b)\alpha(ab)g(ab)] = X'. \qquad \square$$

Finally we show that, modulo a principal AEF, each AEF has finite order dividing v.

LEMMA 4.2. *Let $f : G \times G \to C$ be an AEF. Then $f^v \sim \mathbf{1}$.*

Proof. Define $\alpha : G \to C$ to be $\alpha(g) = \prod_{c \in G} f(g,c)$. By Definition 4.2 (i) and (1)

$$\prod_{c\in G} f(a,b) = \prod_{c\in G} f(a,bc) \prod_{c\in G} f(b,c) \prod_{c\in G} f(ab,c)^{-1},$$

so $f^v(a,b) = \alpha(a)\alpha(b)(\alpha(ab))^{-1}$. □

5. Weak difference sets and cocyclic PCDs

Definition 5.1. A matrix is *Λ-robust* over G if it is f-developed for some Λ-robust development function f, and a configuration is *Λ-robust* if it has a representative which is Λ-robust over G. Similar definitions apply to the word *cocyclic*. When referring to $PCD(v, \Lambda)s$ the prefix "$\Lambda-$" may be dropped.

We note in Theorem 5.1 below that any cocyclic PCD has a weak difference set construction over an (unnormalized) extension of G by an abelian group C, with multiplication defined using the development function ([2, p. 92], [4]). This generalizes the standard result that the incidence matrix of a G-developed $SBIBD$ corresponds to a difference set over G.

The following notation is used: Let $f : G \times G \rightarrow H$ be an AEF.

(i) Define a *coefficient group* of f to be any abelian subgroup $C \leq H$ containing the abelian group $C(f)$ generated by $f(G \times G)$, i.e., $C \geq C(f) = < f(a, b), a, b, \in G >$.

(ii) Suppose C is a coefficient group of f. Let $E(f, C)$ be the *extension group* of G by C[1] with $E(f, C) = \{(x, a) : x \in C, a \in G\}$ and multiplication

$$(x, a)(y, b) = (f(a, b)xy, ab).$$

For simplicity, write $E(f)$ for $E(f, C(f))$.

(iii) Let $J(f) \subset E(f)$ be the v-element set $J(f) = \{(1, a) : a \in G\}$.

(iv) Suppose $H \leq \Pi_S$. For each $g : G \rightarrow S$, define $g_f : E(f) \rightarrow S$ by $g_f((x, a)) = x \circ g(a)$ for all $(x, a) \in E(f)$.

Some comments on the nature of the extension group $E(f, C)$ are appropriate. The simplest case occurs for $f = 1$, when $E(\mathbf{1}, C)$ is the direct product $C \times G$. Furthermore, equivalent $AEFs$ determine isomorphic extension groups. If f, f and α are as given in Definition 4.4 (i), then the mapping $\phi : E(f, C) \rightarrow E(f', C)$ defined by $\phi(x, a) = (x(\alpha(a))^{-1}, a)$ is readily shown to be a group isomorphism. In particular, the equivalence class of principal $AEFs$ determines the direct product extension $C \times G$.

THEOREM 5.1. *Let $f : G \times G \rightarrow \Pi_S$ be Λ-cocyclic, and let $g : G \rightarrow S$. Suppose $\mathcal{X} = (f(a, b)g(ab))(a, b \in G)$ is a $PCD(v, \Lambda)$; then $\mathcal{X} = (g_f((1, a)(1, b)))(a, b \in G)$, and $\{(e, g_f(e)) \mid e \in E(f)\}$ is a (v, Λ)-weak difference set over $E(f)$.*

Proof. Immediate from Definition 3.2 and the notation above. □

[1] Some authors call this the extension group of C by G.

An immediate corollary of Theorem 5.1 and the remarks preceding it, is that two cocyclic $PCD(v, \Lambda)$s developed from equivalent functions will have weak difference set constructions over the same extension group.

Section 3 of [4] lists families of cocyclic designs where the coefficient group $C = \Pi_\Lambda$ is the cyclic group of order two. Included, for instance, are examples of Hadamard matrices of all orders $4n \leq 100$. By contrast, no Hadamard matrix of order $4 < 4n \leq 12,100$ can be group developed modulo a cyclic group. In [4] we conjecture that cocyclic Hadamard matrices exist for all orders $n \equiv 0$ (modulo 4).

6. Robust designs and proper higher-dimensional designs

An important feature of the theory of robust development functions is their central role in the construction of proper higher-dimensional designs. We recast two earlier results [3, 4] in terms of PCDs. Equation (1) also appears (see [3, §2, §3, Eq. (3.3)]) in the context of higher-dimensional designs where *uniform collapsable functions* are discussed. Moreover, Theorem 6.2 below is obtained in [4] for the class of $(v, \Pi_R, \Pi_C, \beta, S)$-designs, which includes $PCDs$.

Definition 6.1. A *proper n-dimensional pairwise combinatorial design* $PCD^n(v, \Lambda)$ is an n-dimensional array $(x_{i_1,i_2,\ldots,i_n})(i_j = 1, \ldots, v, 1 \leq j \leq n)$ of entries from S such that, for all $1 \leq s < t \leq n$, the $v \times v$ arrays $(x_{i_1,\ldots,i_s,\ldots,i_t,\ldots,i_n})(i_s, i_t = 1, 2, \ldots, v)$ obtained by fixing all indices except i_s and i_t, are all $PCD(v, \Lambda)$s.

THEOREM 6.1. *Let* $\mathcal{X} = (f(a, b)g(ab))(a, b \in G)$ *be a robust f-developed* $PCD(v, \Lambda)$*; then* $\mathcal{X}_3 = (g_f((1, a)(1, b)(1, c))) = (f(a, b) \circ f(ab, c)g(abc))\,(a, b, c \in G)$ *is a* $PCD^3(v, \Lambda)$.

THEOREM 6.2. *Let* $\mathcal{X} = (f(a, b)g(ab))\,(a, b \in G)$ *be a cocyclic f-developed* $PCD(v, \Lambda)$*; then* $\mathcal{X}_n = (g_f((1, a_1)(1, a_2)\cdots(1, a_n)))\ (a_1, a_2, \ldots, a_n \in G)$ *is a* $PCD^n(v, \Lambda)$.

Proof (Outline). For all $a_1, a_2, \ldots, a_n \in G$, put

$$h(a_1, a_2, \ldots, a_n) = f(a_1, a_2) \circ f(a_1a_2, a_3) \circ f(a_1a_2\cdots a_{n-1}, a_n)g(a_1a_2\cdots a_n).$$

The argument of [3] is sufficient to prove that $(h(a_1, a_2, \ldots, a_n))(a_1, a_2, \ldots, a_n \in G)$ is a $PCD^n(v, \Lambda)$, and a direct calculation (see [4, proof of 2.11]) shows this design is the same as $\mathcal{X}_n$. □

7. The expanded design of a cocyclic PCD

For $u \geq v$, let $X = [x_{ij}](1 \leq i, j \leq u)$ be a matrix such that for any $v \times v$ "window" of the form $X_{st} = [x_{ij}](s < i \leq s + v$ and $t < j \leq t + v)$, the configuration $\mathcal{X}_{st}$ is a $PCD(v, \Lambda)$. Then the configuration $\mathcal{X}$ will be said to have the (v, Λ)-*window property*. It is shown below that any cocyclic $PCD(v, \Lambda)$ can generate a group developed configuration which has the (v, Λ)-window property.

Definition 7.1. Let $\Pi = \{\rho_1, \rho_2, \dots, \rho_m\}$ be a subgroup of Π_S, and let $\mathcal{X} = (x_{ij})(1 \leq i, j \leq v)$ be a configuration with elements from S. Let $\Omega(\Pi, X) = (\omega_{(k,i),(l,j)}) = (\rho_k \circ \rho_l(x_{ij}))(1 \leq k, l \leq m$ and $1 \leq i, j \leq v)$ be termed the *Π-expanded design of $\mathcal{X}$.*

The $mv \times mv$ matrix $[\omega_{(k,i),(l,j)}] = [\rho_k \circ \rho_l(x_{ij})]$ of Definition 7.1 may usefully be regarded as a Kronecker product $X \times [\Pi] = [x_{ij}] \times [\rho_k \circ \rho_l]$ in which a copy of X in each position of the group multiplication table of Π is acted on by the corresponding element of Π. Now suppose X is a $PCD(v, \Lambda)$ and $\Pi \leq \Pi_\Lambda$. The representative of $\Omega(\Pi, X)$ with this order on its rows and columns is an $m \times m$ block matrix of $v \times v$ matrices which are Λ-equivalent to X. Indeed, every $v \times v$ window is Λ-equivalent to X. For, suppose a $v \times v$ window submatrix overlaps the (k, l), $(k, l + 1)$, $(k + 1, l)$ and $(k + 1, l + 1)^{th}$ block matrices. Application of ρ_k^{-1} and ρ_{k+1}^{-1} to the appropriate rows and ρ_l^{-1} and ρ_{l+1}^{-1} to the appropriate columns, transforms the window into a submatrix, itself equivalent by row and column permutations to X. Moreover, when f is cocyclic and $X = [f(a, b)g(ab)]$, the $C(f)$-expanded design

$$\Omega(C(f), X) = (g_f((x, a)(y, b))) \quad ((x, a), (y, b) \in E(f))$$

is developed modulo $E(f)$. Hence the following is true.

THEOREM 7.1. *If $\mathcal{X}$ is a cocyclic $PCD(v, \Lambda)$ developed by f, then $\Omega(C(f), X)$ has an $E(f)$-developed representative which has the (v, Λ)-window property.*

Example 7.1. The $OD(4; 1, 1, 1, 1)$, $\mathcal{X}$, in Example 3.1 is cocyclic. ($G = \{e, u, v, uv\}$ is the elementary abelian group of order 4 and f, given by the table

	e	u	v	uv
e	1	1	1	1
u	1	−1	1	−1
v	1	−1	−1	1
uv	1	1	−1	−1

is cocyclic by [3, 3, Ex.3.10]. $C(f) = \{1, -1\}$ is the cyclic group of order 2, and $E(f)$ is the quaternions Q_8.) The representative of $\Omega(C(f), X)$ with rows and columns ordered according to the list $(1, 1)$, $(1, i)$, $(1, j)$, $(1, k)$, $(-1, 1)$, $(-1, i)$, $(-1, j)$, $(-1, k)$ gives an 8×8 Q_8-developed configuration

$$\begin{pmatrix} X & -X \\ -X & X \end{pmatrix}$$

where every 4 × 4 window is a representative of an $OD(4;\,1,\,1,\,1,\,1)$.

8. Three combinatorial questions

We state three questions which are basic to the study of cocyclic designs.

(i) Given a group G and a $PCD(v,\,\Lambda)$, $\mathcal{X}$ say, how can one determine whether $\mathcal{X}$ is cocyclic over G?
(ii) Given a group G, when does there exist a $PCD(v,\,\Lambda)$ which is cocyclic over G?
(iii) Given a group G and a set Λ, what are the Λ-cocyclic development functions over G?

Some remarks on questions (i) and (ii) follow. The main focus of the remainder of this paper will be question (iii), which we solve using the cohomology groups of G.

Expanded designs can help answer the first question. In general, if X is cocyclic, a subgroup of the automorphism group of $\Omega(\Pi_\Lambda,\,X)$ will be isomorphic to $E(f)$ for some f. Assuming we know the coefficient group $C(f)$, $\Omega(C(f),\,X)$ can be constructed without knowledge of f. By Theorem 7.1, that design would be $E(f)$-developed, and examination of the design may help resolve the question. When G is abelian, and $f(a,\,b) = f(b,\,a)$ for all $a,\,b \in G$, then $E(f)$ is abelian, so the $E(f)$-developed design is symmetric. In this case, some progress could be made by an application of Fourier theory to appropriate expanded designs.

With regard to question (ii), the structure of Λ may lead to an equation in the integral group ring $\mathbf{Z}(E(f))$. For example, an f-developed cocyclic Hadamard matrix over G corresponds to a solution to the following equation over $\mathbf{Z}(E(f))$:

$$\left(\sum_{x\in G} s_x((1,x)-(-1,x))\right)\left(\sum_{x\in G} s_x((1,x)^{-1}-(-1,x)^{-1})\right)$$
$$= 2v((1,\,1)-(-1,\,1)).$$

Once an equation in $\mathbf{Z}(E(f))$ is obtained, we may use techniques (arising from character theory and number theory) similar to those used to "solve for" difference sets. In §13 we indicate a different approach to question (ii) using development tables.

9. The development table

In all three questions, we begin with the group G. Fortunately, we can study cocyclic development without needing to specify a coefficient group. This is done by means of the development table, an important computational tool for cocyclic design theory.

Even before a coefficient group is specified, any AEF must satisfy the equations (1). Regard these as v^3 simultaneous linear equations with integer coefficients in the v^2 variables (a, b): that is,

$$(a, b) + (ab, c) = (b, c) + (a, bc), \ a, b, c \in G. \tag{5}$$

The set of vectors $\vec{x} = (x(a, b))_{a,b \in G}$ formally satisfying (5) forms a **Z**-module under coordinatewise addition; that is, an abelian group, which we denote by $A(G, -)$. We may apply echelon row reduction over **Z** to equations (5), to reduce the number of indeterminates and the number of equations which constrain them. Indeed, it is always possible to find a set of indeterminates where the only constraints are "order constraints" of the form $mZ = 0$, where m is a positive integer, and Z is an indeterminate. Performing the corresponding reductions on the components of $\vec{x}$ leads, by the fundamental theorem of finitely generated abelian groups, to a standard presentation of $A(G, -)$. To determine all AEFs with a given coefficient group C, it is then sufficient to assign indeterminates to elements of C in all possible ways which satisfy the order constraints. This corresponds to finding the set $Hom(A(G, -), C)$ of all group homomorphisms from $A(G, -)$ to C.

The development table provides a compact expression for a typical element of $A(G, -)$. If $\vec{x}$ is expressed in terms of (possibly constrained) indeterminates, then the corresponding development table is the matrix $[x(a, b)]_{a,b \in G}$, together with the set of constraining equations.

Definition 9.1. A *development table for* G is a pair (D, S) such that $D = [d(a, b)]_{a,b \in G}$, where $\vec{d}$ is a typical element of $A(G, -)$, S is a set of constraints obtained from (5) by row reduction over **Z**, and $d(a, b)$ is a linear combination of indeterminates which are constrained only by the equations in S. (For brevity of expression we will usually use multiplicative notation for entries in D.)

For example, for $G = < a : a^2 = 1 > \cong \mathbf{Z}_2$ the 8 relations (5) reduce to $(1, a) = (a, 1) = (1, 1)$, so a development table for G is $(D, \emptyset)$, where

$$D = \begin{bmatrix} Z & Z \\ Z & A \end{bmatrix},$$

and Z and A are unconstrained indeterminates. In this case $A(\mathbf{Z}_2, -) \cong \mathbf{Z}^2$. Other examples are given in [3, 3.8, 3.10] for $G \cong \mathbf{Z}_v, \mathbf{Z}_2^2$, in [4, Table 3] for $G \cong \mathbf{Z}_2^3$ and in [4, 4.5] for G a finite abelian group.

Our aim is to obtain a simple development table for G, with either the minimum number of indeterminates or a distinctive pattern of entries.

After reduction, the generators (indeterminates) in a standard presentation of $A(G, -)$ fall into two categories: those of infinite order (unconstrained) and those of finite order (constrained). Each category can be isolated by factoring out the other; that is, by adding an equation $Z = 0$ for each indeterminate Z in the category to be discarded, and continuing the echelonisation.

Because equivalent AEFs determine equivalent cocyclic matrices, by Lemma 4.1, we also want to derive similar tables for the *inequivalent* AEFs. An important consequence of Lemma 4.2 bears on this: if the echelon row reduction of the equations (5) is performed modulo v, the resulting set of solutions contains at least one representative of each inequivalent AEF and is necessarily finite. Hence there are only *finitely* many inequivalent AEFs.

Using group cohomology, we will show that the unconstrained indeterminates in a standard presentation of $A(G, -)$ correspond to known techniques of group and ω-cyclic development, and the constrained indeterminates add asymmetry to the development tables. In particular (see Lemma 4.1), the technique of group development over G is embodied in the principal AEFs, and corresponds to the subgroup $B(G, -)$ of $A(G, -)$ consisting of solutions to (5) of the form $\vec{x} = (x(a, b) = x(a) + x(b) - x(ab))_{a, b \in G}$. Factoring $B(G, -)$ out allows us (in §13) to present the desired *minimal development tables* of inequivalent AEFs, which have a minimum number of indeterminates and a distinctive structure.

Before doing this, we must introduce a little cohomology theory for G, with coefficients in C, and describe the cocyclic development functions in this context.

10. The cohomological connection

In the next three sections we will describe the AEFs anew, in terms of the first and second integral homology group of G. We shift emphasis of specify a *finitely generated* abelian coefficient group C and consider all AEFs $f : G \times G \rightarrow \Pi_S$ whose image groups $C(f)$ are subgroups of C. We now let C be additively written with identity 0. Since C is abelian, any map $f : G \times G \rightarrow C$ is an AEF by (1) exactly when it satisfies

$$f(a, b) + f(ab, c) - f(b, c) - f(a, bc) = 0 \quad a, b, c \in G, \tag{6}$$

and is normalized if

$$f(1, 1) = 0. \tag{7}$$

The cohomological connection with the design theory of §§4–9 rests on the following observation. A map satisfying (6) and (7) is known in group cohomology as a *factor set* or, alternatively, as a 2-dimensional *cocycle* of the normalized standard complex for computing the cohomology of G with trivial coefficients in C [2, pp.92–93]. Each factor set determines a (normalized) central extension of G by C just as each AEF determines an unnormalized extension of G by C (see notation (ii) in §5).

The following notation is used:
(i) $A(G, C) = \{f : G \times G \to C, f \text{ an } AEF\} = Hom(A(G, -), C)$
(ii) $B(G, C) = \{f \in A(G, C), f \sim 1\}$.

Both $A(G, C)$ and the set of factor sets are abelian groups under pointwise addition of functions, and are finitely generated because C is. The equivalence class $B(G, C)$ of principal AEFs is a subgroup of $A(G, C)$; similarly, the equivalence class of principal factor sets is a subgroup of the group of factor sets. The quotient group $A(G, C)/B(G, C)$ is finitely generated and hence finite, since by Lemma 4.2 it has exponent dividing v. Three simple facts are noted.

PROPOSITION 10.1.

(i) $B(G, C) \cong \{\textit{set maps} : G \to C\}/\{\textit{group homomorphisms}: G \to C\}$,
(ii) $A(G, C)/B(G, C) \cong \frac{\{\textit{factor sets}:G\times G\to C\}}{\{\textit{principal factor sets}:G\times G\to C\}}$,
(iii) $A(G, C)/B(G, C)$ *is finite and has exponent dividing* v.

The group of equivalence classes of factor sets is isomorphic to $H^2(G; C)$, the "second cohomology group of G with trivial coefficients in C" (see [2, §3] or [7, pp. 209–210], for example). So, by Proposition 10.1(ii),

$$A(G, C)/B(G, C) \cong H^2(G; C). \tag{8}$$

Thus, in principle, all we need to know about inequivalent AEFs is embodied in the more familiar group $H^2(G; C)$.

We state some of its properties. The interested reader may find full expositions in homological algebra texts such as [2, 7], or an overview in [8]. By the "Universal Coefficient Theorem" [7, V. Thm. 3.3], it is known that $H^2(G; C)$ decomposes as a direct sum:

$$H^2(G; C) \cong Ext_{\mathbf{Z}}(G/G', C) \oplus Hom(H_2(G), C). \tag{9}$$

Here, G' is the commutator subgroup of G, G/G' is the (finite) abelianization of G and $H_2(G)$ is the second integral homology group of G. For abelian groups F and H, $Ext_{\mathbf{Z}}(F, H)$ is a specific abelian group (see [7, III.4] and Proposition 10.2 below) depending only on F and H, and $Hom(F, H)$ is the abelian group of all group homomorphisms from F to H.

By (iii) in Proposition 10.1 and (8), $H^2(G; C)$ is a direct sum of finite cyclic groups of orders dividing v. Setting $C = \mathbf{Z}$ and noting (9) shows that $H_2(G)$ also has this form. Essentially (see [9]), it consists of relations satisfied by commutators in G, modulo those which are universally satisfied. An algorithm to compute $H_2(G)$ (which is also called the *Schur multiplicator* of G), is given in [8, pp. 83–84].

Example 10.1.

(i) G finite abelian. If G has torsion invariant decomposition

$$G = \bigoplus_{i=1}^{M} \mathbf{Z}_{m_i} \quad \text{where } m_i \text{ divides } m_{i+1}, \quad 1 \leq i \leq M-1,$$

then (as was calculated directly in [4]), $H_2(G) \cong \mathbf{Z}_{m_1}^{M-1} \oplus \mathbf{Z}_{m_2}^{M-2} \oplus \cdots \oplus \mathbf{Z}_{m_{M-1}}$ and if the summand $\mathbf{Z}_{m_i}$ of G is generated by x_i then the summands $\mathbf{Z}_{m_i}$ of $H_2(G)$ are generated by the classes of $[x_i, x_{i+j}]$, $1 \leq j \leq M-i$. Clearly $G/G' \cong G$.

(ii) G a split extension of a cyclic group by a cyclic group.

$$G = < a, b : a^r = 1, b^s = 1, b^{-1}ab = a^t > \text{ where } t^s \equiv 1 \text{ (modulo } r).$$

By [10, pp.253–255] $H_2(G) \cong \mathbf{Z}_g$, where $g = g.c.d.(s, r)$. By inspection $G/G' \cong < a : a^w = 1 > \oplus < b : b^s = 1 >$, where $w = g.c.d.(r, t-1)$.

The abelian group $Ext_{\mathbf{Z}}(G/G', C)$ is calculated by a standard technical result.

PROPOSITION 10.2. [7, III.4]. *Let F and H be abelian groups, with F finite and H finitely generated. If the primary invariant decomposition of F is* $F = \bigoplus_{i=1}^{L} \mathbf{Z}_{q_i}$, $q_i = p_i^{t_i}$, p_i *a prime,* $1 \leq i \leq L$, *and, if* $H \cong \mathbf{Z}^k \oplus \left(\bigoplus_{j=1}^{N} \mathbf{Z}_{n_j}\right)$, *then*

(*i*) $Ext_{\mathbf{Z}}(F, H) \cong \bigoplus_{i=1}^{L} Ext_{\mathbf{Z}}(\mathbf{Z}_{q_i}, H)$,

(*ii*) $Ext_{\mathbf{Z}}(\mathbf{Z}_{q_i}, H) \cong \mathbf{Z}_{q_i}^{k} \oplus (\bigoplus_{j=1}^{N} \mathbf{Z}_{g_{ij}})$, *where*$g_{ij} = g.c.d.(q_i, n_j)$.

To summarize: up to equivalence, each AEF has order dividing v (by (iii) in Proposition 10.1) and a decomposition as a sum of two AEFs (by (8) and (9)). Indeed, we shall be much more precise. However, practical application of these powerful results requires that we describe the isomorphisms (8) and (9) in more detail.

11. The group of abelian extension functions

We use part of the (inhomogeneous, unnormalized) standard complex or "bar resolution," tensored by $\mathbf{Z}$, which consists of a sequence of frce abelian groups of finite rank, together with abelian group homomorphisms with special properties.

The following notation is used: let $M_0(G) = \mathbf{Z}$ and for $m \geq 1$, let $M_m(G)$ be the free abelian group of rank v^m generated by the elements of G^m, that is

$$M_m(G) = Ab < (x_1, x_2, \ldots, x_m), x_1, x_2, \ldots, x_m \in G > .$$

For $m \geq 0$, define the abelian group homomorphism $\partial_{m+1} : M_{m+1}(G) \to M_m(G)$ on each infinite cyclic generator by: $\partial_1(a_1) = 0$ and, for $m \geq 1$,

$$\partial_{m+1}(x_1, x_2, \ldots, x_{m+1}) = (-1)^{m+1}(x_1, x_2, \ldots, x_m) + (x_2, x_3, \ldots, x_{m+1}) + \sum_{i=1}^{m}(-1)^i(x_1, \ldots, x_i x_{i+1}, \ldots, x_{m+1}).$$

Put $I_m = \partial_{m+1}(M_{m+1}(G))$, $K_{m+1} = Kernel(\partial_{m+1})$ and note that $I_m \leq K_m$. The quotient K_m/I_m is usually called *the mth integral homology group of G* and is denoted $H_m(G)$. In particular, $H_1(G) \cong G/G'$. Put $R_m(G) = M_m(G)/I_m$, and let $\delta_{m+1} : R_{m+1}(G) \to M_m(G)$ be the quotient map induced by ∂_{m+1}. Note that $H_m(G) \leq R_m(G)$.

We can now describe $A(G, C)$ and $B(G, C)$ in terms of those groups and homomorphisms for which $m = 1, 2$. By definition, $R_2(G)$ is the abelian group generated by $\{(a, b),\ a, b \in G\}$, subject to the relations $\{-(a, b) + (b, c) - (ab, c) + (a, bc),\ a, b, c \in G\}$, so is isomorphic to the group $A(G, -)$ of §9. That is,

$$A(G, -) \cong R_2(G).$$

LEMMA 11.1. *Define* $\phi : A(G, C) \to Hom(R_2(G), C)$ *to be*

$$\phi(h)\left(\sum_{b \in G \times G} n(b)(b) + I_2\right) = \sum_{b \in G \times G} n(b)h(b),\ h \in A(G, C).$$

(*i*) $A(G, C) \cong Hom(R_2(G), (C)$.
(*ii*) If $h \in B(G, C)$, then $\phi(h)(H_2(G)) = 0$.

Proof. It is readily checked that ϕ is well defined and an isomorphism. Similarly, $\{\alpha : G \to C\} \cong Hom(M_1(G), C)$, and ϕ takes an element in $B(G, C)$ to an element $\alpha\delta_2$ for some $\alpha \in Hom(M_1(G), C)$. Indeed $\alpha\delta_2(H_2(G)) = 0$, giving the second result. □

From now on, without further comment, we will use (i) of Lemma 11.1 to regard an AEF equally as a set mapping $f : G \times G \to C$ satisfying (6) or as an abelian group homomorphism $f : R_2(G) \to C$. So to determine $A(G, C)$ we need only express $R_2(G)$ as a direct sum of cyclic groups.

THEOREM 11.1. *With* $v = |G|$ *and the notation above,*

(*i*) $R_2(G)/H_2(G) \cong \mathbf{Z}^v$.
(*ii*) $R_2(G) = N_2(G) \oplus H_2(G)$ *where* $N_2(G) \cong [R_2(G)/H_2(G)]$.
(*iii*) $A(G, C) \cong Hom(N_2(G), C) \oplus Hom(H_2(G), C) \cong C^v \oplus Hom(H_2(G), C)$.

Proof. Any group homomorphism $h : F \rightarrow H$ factors through $F/Ker(h)$ as $h = h^* \circ \pi : F \rightarrow F/Ker(h) \rightarrow H$ where π is the canonical quotient map and h^* is the injection induced from h. Thus we have the following commuting diagram of abelian groups with short exact columns.

$$\begin{tikzcd}
I_2 \arrow[r, "="] \arrow[d] & I_2 \arrow[d] & & & \\
K_2 \arrow[r] \arrow[d] & M_2(G) \arrow[r, "\pi"] \arrow[d] & M_2(G)/K_2 \arrow[r, "\partial_2^*"] \arrow[d, "\cong"] & M_1(G) \arrow[r] \arrow[d, "="] & M_1(G)/Im\partial_2^* \\
H_2(G) \arrow[r] & R_2(G) \arrow[r, "\pi"] & R_2(G)/H_2(G) \arrow[r, "\partial_2^*"] & M_1(G) &
\end{tikzcd} \tag{10}$$

We show $M_2(G)/K_2 \cong \mathbf{Z}^v$. The subgroup $\partial_2^*(M_2(G)/K_2)$ is free abelian, and since ∂_2^* is an injection, $M_2(G)/K_2$ is free abelian of rank at most v. For any $a \in G$ with order $o(a)$, define $\tau(a) = \sum_{i=0}^{o(a)-1}(a, a^i) + K_2$. Then $\partial_2^*(\tau(a)) = o(a)(a)$ and if $a \neq b$, then $o(a)(a) \neq o(b)(b)$; so this group has rank v. By isomorphism, $R_2(G)/H_2(G)$ is also free abelian of rank v; consequently $R_2(G)$ is a direct sum $N_2(G) \oplus H_2(G)$ where $N_2(G) \cong R_2(G)/H_2(G)$. Finally, (iii) follows from the facts that $Hom(X \oplus Y, C) \cong Hom(X, C) \oplus Hom(Y, C)$ and $Hom(\mathbf{Z}, C) \cong C$. □

Since $H_2(G)$ is finite, it is the torsion subgroup of $R_2(G)$, and $N_2(G)$ is a torsion-free complement.

The isomorphism Theorem 11.1(ii) implies that any $AEF f : G \times G \rightarrow C$ has a decomposition as a sum $f = f_s + f_c$ where f_s annihilates the subgroup $H_2(G)$ of $R_2(G)$ and f_c annihilates the subgroup $N_2(G)$. For abelian G, this result was obtained directly in [4, 4.9].

Definition 11.1. The AEF $f \in A(G, C)$ is *symmetric* if $f(H_2(G)) = 0$. Let $S(G, C)$ denote the subgroup of symmetric AEFs. The *commutator part* of an AEF is its restriction to $H_2(G)$.

By Theorem 11.1(iii) we see that $S(G, C) \cong Hom(N_2(G), C)$. Note that Lemma 11.1(ii) implies that every principal AEF is symmetric: i.e., $B(G, C) \leq S(G, C)$. These remarks together with the isomorphisms (8) and (9) imply the final results of this section.

COROLLARY 11.1.

(i) $A(G, C) = S(G, C) \oplus Hom(H_2(G), C)$
(ii) $S(G, C)/B(G, C) \cong Ext_{\mathbf{Z}}(G/G', C)$.

12. The group of symmetric AEFs

We show that any Λ-cocyclic matrix developed by a symmetric AEF is Λ-equivalent to one obtained by entrywise action of a *symmetric* matrix on a group developed matrix. Moreover, the symmetric matrix is the Kronecker product of back ω-cyclic matrices.

By (ii) of Corollary 11.1, the group $S(G, C)/B(G, C)$ of equivalence classes of symmetric *AEF*s over G is isomorphic to $Ext_{\mathbf{Z}}(G/G', C)$, and hence also to the group

$$S(G/G', C)/B(G/G', C)$$

of equivalence classes of symmetric *AEF*s *over the abelianization* G/G'.

Note that, if $h : G \to H$ is a homomorphism of finite groups and $f \in A(H, C)$, then $f^+ = f \circ (h \times h) \in A(G, C)$ (cf. [4, 3.2.ii]). Setting $H = G/G'$ and $h = \pi : G \to G/G'$ shows that any *AEF* f over G/G' determines a *lifted AEF* f^+ over G. By [4, 4.9], any $f \in S(G/G', C)$ always satisfies the symmetry relation $f(x, y) = f(y, x)$, $x, y \in G/G'$; consequently, the lifted *AEF* f^+ satisfies

$$f^+(a, b) = f^+(b, a), \quad a, b \in G. \tag{11}$$

Direct calculation shows that lifting two inequivalent *AEF*s in $S(G/G', C)$ produces two inequivalent *AEF*s in $S(G, C)$, so any element of $S(G, C)$ is equivalent to a lifted *AEF* satisfying the symmetry relation (11).

PROPOSITION 12.1. *If* $f_s \in S(G, C)$, *it has a decomposition*

$$f_s = f_A^+ + f_B, \quad f_A^+ = f_A \circ (\pi \times \pi), \quad f_A \in S(G/G', C), \quad f_B \in B(G, C),$$

and any other such decomposition $f_s = f_{A^*}^+ + f_{B^*}$ *arises as* $f_{A^*}^+ = f_A^+ + h^+$, $f_{B^*} = f_B - h^+$, *for some* $h \in B(G/G', C)$.

In fact, any $f_A \in S(G/G', C)$ itself has a unique decomposition as a sum of symmetric *AEF*s, one for each cyclic factor of G/G'. (See [4, 4.10]: for finite abelian groups H and K, the group of symmetric *AEF*s on $H \times K$ is the direct product of the groups of symmetric *AEF*s on H and K.) By (i) of Example 10.1 it also follows that for any cyclic group $\mathbf{Z}_q$, $H_2(\mathbf{Z}_q) = 0$; so all the *AEF*s over $\mathbf{Z}_q$ are symmetric and $S(\mathbf{Z}_q, C)/B(\mathbf{Z}_q, C) \cong H^2(\mathbf{Z}_q; C)$.

PROPOSITION 12.2. *Let the primary invariant decomposition of* G/G' *be* $G/G' = \oplus_{j=1}^{L} \mathbf{Z}_{q_j}$, $q_j = p_j^{t_j}$, p_j *a prime*, $1 \leq j \leq L$. *Then*

(*i*) $S(G/G', C) \cong \bigoplus_{j=1}^{L} S(\mathbf{Z}_{q_j}, C)$,
(*ii*) $S(G, C)/B(G, C) \cong \bigoplus_{j=1}^{L} S(\mathbf{Z}_{q_j}, C)/B(\mathbf{Z}_{q_j}, C) \cong \bigoplus_{j=1}^{L} H^2(\mathbf{Z}_{q_j}; C)$.

Together, Proposition 12.1 and (i) of Proposition 12.2 give us a complete decomposition of any symmetric *AEF*.

THEOREM 12.1 **(Structure Theorem for Symmetric AEFs).** *Let $f \in S(G, C)$, and let the primary invariant decomposition of G/G' be $\bigoplus_{j=1}^{L} \mathbf{Z}_{q_j}$, where $q_j = p_j^{t_j}$, p_j a prime, and $1 \leq j \leq L$. Then*

$$f = (\bigoplus_{j=1}^{L} f_{s_j})^{+} + f_B,$$

where $f_{s_j} \in S(\mathbf{Z}_{q_j}, C), f_B \in B(G, C)$ and the decomposition is unique up to the choice of coset representative f_B of the coset $f_B + B(G/G', C)^{+}$ in $B(G, C)$.

It is a remarkable fact that each coset of symmetric AEFs over a cyclic group contains a specific ω-cyclic development function (see Example 4.1), which is the *natural* choice of coset representative for design theoretic purposes. By (ii) of Proposition 10.2 the second cohomology group for a cyclic group with cyclic coefficients is known:

$$H^2(\mathbf{Z}_v;\mathbf{Z}) \cong H^2(\mathbf{Z}_v;\mathbf{Z}_v) \cong \mathbf{Z}_v,\ H^2(\mathbf{Z}_v;\mathbf{Z}_n) \cong \mathbf{Z}_g,\ g = g.c.d.(v, n). \tag{12}$$

We write the group operation in $A(\mathbf{Z}_v, \mathbf{Z})$ and in $A(\mathbf{Z}_v, \mathbf{Z}_n)$ multiplicatively and use the isomorphisms $< x > \cong \mathbf{Z}$, $< x : x^n = 1 > \cong \mathbf{Z}_n$ and $< a : a^v = 1 > \cong \mathbf{Z}_v$.

LEMMA 12.1.

(*i*) *Define $w : \mathbf{Z}_v \times \mathbf{Z}_v \to \mathbf{Z}$ to be $w(a^i, a^j) = x^{\lfloor (i+j)/v \rfloor}, 0 \leq i, j \leq v - 1$. Then $w^l \in S(\mathbf{Z}_v, \mathbf{Z})$, and $w^l \sim w^m$ if and only if $l \equiv m\,(\text{modulo}\, v)$. Indeed, any function $f \in S(\mathbf{Z}_v, \mathbf{Z})$ is equivalent to some power of w.*

(*ii*) *if $g = g.c.d.(v, n)$, define $w : \mathbf{Z}_v \times \mathbf{Z}_v \to \mathbf{Z}_n$ to be $w(a^i, a^j) = x^{(n/g)\lfloor (i+j)/v \rfloor}$, $0 \leq i, j \leq v-1$. Then $w^l \in S(\mathbf{Z}_v, \mathbf{Z}_n)$, and $w^l \sim w^m$ if and only if $l \equiv m\,(\text{modulo}\, g)$. Indeed, any function $f \in S(\mathbf{Z}_v, \mathbf{Z}_n)$ is equivalent to some power of w.*

Proof. We only prove (i); the proof for (ii) is similar. The argument of [3, 4.6, second part of proof] shows w is an AEF. It, and its powers, clearly satisfy (11). If $w^l \sim w^m$ then there exists $\alpha : \mathbf{Z}_v \to \mathbf{Z}$ such that

$$w^{l-m}(a^i, a^j) = x^{(l-m)\lfloor (i+j)/v \rfloor} = \alpha(a^i)\alpha(a^j)\alpha(a^{i+j})^{-1},\ 0 \leq i, j \leq v - 1.$$

Put $i = j = 0$ to show $\alpha(1) = 1$ and put $i = 1$ to show $\alpha(a^j) = \alpha(a)^j$, $1 \leq j \leq v-1$. Consequently $\alpha(a)^v = x^{l-m}$, so $v \mid (l - m)$. Conversely, if $l - m = dv$, set $\alpha(a^i) = x^{di}$, $0 \leq i \leq v-1$ to show $w^l \sim w^m$. Hence w generates an order v cyclic group of inequivalent AEFs, which, by the first part of (12), forms a complete set of equivalence class representatives. □

Geramita and Seberry [6, 4.198] note that if v is odd, any negacyclically developed matrix over $\mathbf{Z}_v$ is (using our terms) Λ-equivalent, for $\Pi_\Lambda \cong \mathbf{Z}_2$, to a cyclically developed matrix. This is easily explained by (ii) of Lemma 12.1, and is in fact the simplest illustration of a very general phenomenon. Since, by (12) $H^2(\mathbf{Z}_v;\mathbf{Z}_2) \cong \mathbf{Z}_2$ or 0 according as v is even or odd, there are at most two equivalence classes of cocyclic orthogonal designs over $\mathbf{Z}_v$ (assuming $C \cong \Pi_A \cong \mathbf{Z}_2$ consists of the permutations on S given by multiplication by ± 1). When v is odd, the sole equivalence class (of the trivial AEF $w^0 = 1$) is that of cyclic development. When v is even, the nontrivial equivalence class (of the AEF w of order 2) is that of negacyclic development.

THEOREM 12.2. *There are $g =$ g.c.d.(v, n) inequivalent cocyclic development functions over $\mathbf{Z}_v$ with coefficients in $\mathbf{Z}_n$, all of which are symmetric. When $g = 1$, the sole equivalence class is that of cyclic (group) development. When $g > 1$, the nontrivial equivalence classes are those of ω^k-cyclic development, $k = 1, \cdots, g-1$, where ω is an element of order g in $\mathbf{Z}_n$.*

13. The minimal development table

Finally, we apply this link between group cohomology and design theory to extract a minimal development table for G. It is isomorphic to $H^2(G;-)$ (with unspecified coefficient group), and provides a complete (finite) list of inequivalent cocyclic development functions.

Recall from §9 that a development table it is presentation in matrix form of $A(G, -) \cong R_2(G)$, so by (ii) of Theorem 11.1 it is possible to find a development table with the minimum number of indeterminates.

A *minimum* development table so derived from the isomorphism $A(G, -) \cong N_2(G) \oplus H_2(G)$ has v unconstrained indeterminates corresponding to v "symmetric" generators of $N_2(G)$ and (usually) some order-constrained indeterminates corresponding to the "commutator" generators of $H_2(G)$.

Our minimal development table is a presentation of $A(G, -)/B(G, -)$ in matrix form. A development table is obtained from a minimal development table by superimposing on it a group development table corresponding to a presentation of the subgroup $B(G, -)$.

On setting $S(G, -)$ to be the subgroup of $A(G, -)$ isomorphic to $N_2(G)$, the results of Proposition 12.2(ii) and Lemma 12.1 allow us to determine a minimal set of "symmetric" generators for $S(G, -)/B(G, -)$, each with finite order dividing v.

For a cyclic group of prime power order, the minimal development table is just the matrix $[w^l(a, b)]$ for the ω-cyclic development of Lemma 12.1(i).

Definition 13.1. Let $v = p^t$ be a prime power, and let A be an indeterminate of order dividing v in an abelian group. The *minimal development table* of $\mathbf{Z}_v$ is the (symmetric) $v \times v$ matrix

$$MD(\mathbf{Z}_v) = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & A \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & A & A \\ 1 & A & \cdots & A & A \end{bmatrix}, A^v = 1.$$

The symmetric minimal development table for an arbitrary G is built up from Definition 13.1 by Kronecker products, and the commutator minimal development table is given by Hadamard products of the matrices corresponding to the generators of $Hom(H_2(G), -)$.

Definition 13.2. Let G be a finite group of order v and let J_r be the $r \times r$ all 1s matrix.

(i) Let the primary invariant decomposition of G/G' be $G/G' = \bigoplus_{j=1}^{L} \mathbf{Z}_{q_j}$, $q_j = p_j^{t_j}$, p_j a prime, $1 \leq j \leq L$. The *symmetric minimal development table* $MD_s(G)$ of G is the $v \times v$ Kronecker product matrix

$$MD_s(G) = J_{|G'|} \times MD(\mathbf{Z}_{q_1}) \times MD(\mathbf{Z}_{q_2}) \times \cdots \times MD(\mathbf{Z}_{q_L}).$$

(ii) Let $f_1, f_2, \ldots, f_M$ be a minimal generating set for the torsion subgroup of $A(G, -)$. A *commutator minimal development table* $MD_c(G)$ of G is the $v \times v$ Hadamard product matrix, together with the corresponding order constraints

$$MD_c(G) = [f_1(a, b)] \circ [f_2(a, b)] \circ \cdots \circ [f_M(a, b)] \, (a, b \in G).$$

Definition 13.3. Let G be a finite group of order v. A *minimal development table* $MD(G)$ of G is a $v \times v$ Hadamard product matrix

$$MD(G) = MD_s(G) \circ MD_c(G).$$

Example 13.1.

(i) G a 4-group $G \cong \mathbf{Z}_2 \times \mathbf{Z}_2 = \{e, a, b, ab\}$. Then

$$MD_s(G) = \begin{bmatrix} 1 & 1 \\ 1 & A \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & B \end{bmatrix}, A^2 = B^2 = 1,$$

and, from (i) of Example 10.1 or [3, 3.10],

$$MD_c(G) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & K & 1 & K \\ 1 & K & 1 & K \end{bmatrix}, \quad K^2 = 1.$$

(ii) G a cyclic group of order 6, $G \cong \mathbf{Z}_6 \cong \mathbf{Z}_3 \times \mathbf{Z}_2 = \{e, a, a^2, b, ab, a^2b\}$. Then

$$MD(G) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & A \\ 1 & A & A \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & B \end{bmatrix}, \quad A^3 = B^2 = 1.$$

(iii) G a dihedral group of order $2r$, r odd, $G = \{e, a, a^2, \ldots, a^{r-1}, b, ab, a^2b, \ldots, a^{r-1}b\}$, cf (ii) of Example 10. Then $|G'| = r$; $G/G' \cong < b : b^2 = 1 >$; $H_2(G) \cong 0$ and

$$MD(G) = J_r \times \begin{bmatrix} 1 & 1 \\ 1 & A \end{bmatrix}, \quad A^2 = 1.$$

(iv) $G = Ab < x_1, x_2, x_3 : 2x_1 = 2x_2 = 2x_3 > \cong \mathbf{Z}_2^3$, with elements ordered lexicographically (cf. (i) of Example 10.1). Then $|G'| = 1, L = 3, q_1 = q_2 = q_3 = 2$ and

$$MD_s(G) = \begin{bmatrix} 1 & 1 \\ 1 & A \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & B \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & C \end{bmatrix}, \quad A^2 = B^2 = C^2 = 1.$$

and, from (i) of Example 10.1 or [4, Table 3], for $K^2 = L^2 = M^2 = 1$

$$MD_c(G) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & K & 1 & K & 1 & K & 1 & K \\ 1 & K & 1 & K & 1 & K & 1 & K \\ 1 & L & M & LM & 1 & L & M & LM \\ 1 & L & M & LM & 1 & L & M & LM \\ 1 & KL & M & KLM & 1 & KL & M & KLM \\ 1 & KL & M & KLM & 1 & KL & M & KLM \end{bmatrix}.$$

(v) G the quaternions, $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. It may be shown that $H_2(G) = 0$, so that every AEF on G is symmetric. Clearly

$$G/G' \cong < a : a^2 = 1 > \oplus < b : b^2 = 1 > .$$

$$MD(G) = J_2 \times \begin{bmatrix} 1 & 1 \\ 1 & A \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & B \end{bmatrix}, \quad A^2 = B^2 = 1.$$

(vi) G a dihedral group of order 8, $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ (cf. (ii) of Example 10.1). Then

$$G/G' \cong < a : a^2 = 1 > \oplus < b : b^2 = 1 >; \quad H_2(G) \cong \mathbf{Z}_2,$$

and the generator of $H_2(G)$ is given by the class of $[a^2, b]$. So

$$MD_s(G) = J_2 \times \begin{bmatrix} 1 & 1 \\ 1 & A \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & B \end{bmatrix}, \quad A^2 = B^2 = 1,$$

and

$$MD_c(G) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & K & 1 & 1 & 1 & K & 1 \\ 1 & 1 & 1 & K & 1 & 1 & K & 1 \\ 1 & K & K & K & 1 & 1 & K & 1 \\ 1 & K & 1 & 1 & 1 & 1 & K & 1 \end{bmatrix}, \quad K^2 = 1.$$

The minimal development table answers question (iii) (see §8), and is therefore of central value in answering question (ii). For instance, to look for cocyclic ODs over G, the indeterminate entries of $MD(G)$ are assigned values in a cyclic group of order 2, and the resultant matrix is superimposed on an arbitrary G-developed matrix. Then the simultaneous equations resulting from the row-orthogonality requirement are solved.

We shall pursue this question elsewhere, but we close with a small example of the application of this theory. Consider the non-cyclic group (i) of Example 13.1 $G \cong \mathbf{Z}_2 \times \mathbf{Z}_2$, and let S, Λ and $\Pi_\Lambda = \{1, -1\} \cong \mathbf{Z}_2$ be as given in Example 3.1. Any cocyclic OD over G is Λ-equivalent and hence OD-equivalent ([6, p. 74]), to one of the form

$$\begin{bmatrix} e & f & g & h \\ f & eA & h & gA \\ g & hK & eB & fBK \\ h & gAK & fB & eABK \end{bmatrix},$$

$$A, B, K \in \Pi_\Lambda, \quad A^2 = B^2 = K^2 = 1, \quad e, f, g, h \in S.$$

The resulting simultaneous equations are

$$(1 + A)(ef + gh) = 0, \ (1 + B)(eg + fhK) = 0, \ (1 + ABK)(eh + fgB) = 0.$$

The eight inequivalent cocyclic development functions specified by the values of the vector (A, B, K) determine the four nonisomorphic extensions of $\mathbf{Z}_2 \times \mathbf{Z}_2$ by $\mathbf{Z}_2$ for the corresponding weak difference set constructions (Theorem 5.1) as follows:

$\mathbf{Z}_2^3 : (1, 1, 1)$
$\mathbf{Z}_4 \times \mathbf{Z}_2 : (1, -1, 1), (-1, 1, 1), (-1, -1, 1)$
$D_8 : (1, 1, -1), (1, -1, -1), (-1, 1, -1)$
$Q_8 : (-1, -1, -1).$

For each choice of (A, B, K), the simultaneous equations may be solved to give all possible cocyclic ODs over $\mathbf{Z}_2 \times \mathbf{Z}_2$. In particular, we list the cocyclic ODs which are *full* (no entries are 0):

for $(1,1,-1)$, $(1,-1,-1)$, $(-1,1,-1)$ there are none,
for $(1, 1, 1)$ the only solution (also cyclically developed modulo $\mathbf{Z}_4$) is

$$\begin{bmatrix} e & e & e & -e \\ e & e & -e & e \\ e & -e & e & e \\ -e & e & e & e \end{bmatrix}, \quad e \in S, \neq 0,$$

for $(1,-1,1)$, $(-1,1,1)$, $(-1,-1,1)$ the only solutions are

$$\begin{bmatrix} e & e & f & -f \\ e & -e & -f & -f \\ f & -f & e & e \\ -f & -f & e & -e \end{bmatrix}, \quad e, f \in S, \neq 0,$$

while for $(-1,-1,-1)$ the simultaneous equations hold vacuously and the solutions are (cf. Example 3.1)

$$\begin{bmatrix} e & f & g & h \\ f & -e & h & -g \\ g & -h & -e & f \\ h & g & -f & -e \end{bmatrix}, \quad e, f, g, h \in S, \neq 0,$$

This last result means there is exactly one equivalence class of $OD(4;1,1,1,1)$s, not two (as stated in [6, Theorem 4.1]), since by [3, 4.3. (iii)] all $OD(4;1,1,1,1)$s are cocyclic. (This may also be checked directly.)

References

1. G Berman, "Families of generalised weighing matrices," *Can. J. Math.* **30** (1978), 1016–1028.
2. K.S. Brown, *Cohomology of groups*, Graduate Texts in Math. 87, Springer-Verlag, New York, 1982.
3. W. de Launey, "On the construction of n-dimensional designs from 2-dimensional designs," *Australas. J. Combin.* **1** (1990), 67–81.
4. W. de Launey and K.J. Horadam, "A weak difference set construction for higher dimensional designs", *Designs, Codes and Cryptography* **3** (1993), 75–87.
5. P. Delsarte, J.M. Goethals, and J.J. Seidel, "Orthogonal matrices with zero diagonal II", *Can. J. Math.* **23** (1971), 816–832.
6. A.V. Geramita and J. Seberry, *Orthogonal Designs*, Lecture Notes in Pure and Appl. Math. 45, Dekker, New York, 1979.
7. P.J. Hilton and U. Stammbach, *A Course in Homological Algebra*, Graduate Texts in Math. 4, Springer-Verlag, New York, 1971.
8. D.L. Johnson, *Presentation of Groups*, London Math. Soc. Lecture Note Ser. 22, Cambridge University Press, Cambridge, 1976.
9. C. Miller, "The second homology group of a group; relations among commutators", *Proc. Amer. Math. Soc.* **3** (1952), 588–595.
10. C.T.C. Wall, "Resolutions for extensions of groups," *Math. Proc. Cambridge Philos. Soc.* **57** (1961), 251–255.
11. W.D. Wallis, A.P. Street, and J.S. Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, Lecture Notes in Math. 292, Springer-Verlag, Berlin, 1972.

Author Addresses

K.J. Horadam: Department of Mathematics, R.M.I.T, GPO Box 2476V, Melbourne Vic 3001, Australia
W. De Launey: c/o CMR, DSTO, PO Box 4924, Kingston, ACT 2604, Australia