Perspectives on algebraic design theory

Dane Flannery

University of Galway, Ireland

Warwick de Launey

Kathy Horadam

Padraig Ó Cáthain

Ronan Egan

José Andrés Armario

What are the designs of interest in algebraic design theory (ADT)?

A *pairwise combinatorial design* (PCD) is a (square) matrix with entries in some *ambient ring*, whose row pairs all satisfy a fixed constraint specified by an *orthogonality set* Λ: each pair of (distinct) rows of the PCD lies in Λ.

Many familiar designs are PCDs. ADT reduces many questions about these designs to study of possible Λ and ambient rings. For convenience, restrict—as usual!—to Hadamard matrices (not a stretch then to, e.g., weighing matrices, Butson Hadamard matrices).

E.g., an $n \times n$ Hadamard matrix is a PCD for Λ the set of all $2 \times n$ $\{\pm 1\}$-arrays X such that $XX^\top = n1_2$; can take ambient ring to be $\mathbb{Z}$.

Combinatorial design theory is a source of simply stated, concrete, yet difficult discrete problems, with the Hadamard conjecture being a prime example. It has become clear that many of these problems are essentially algebraic in nature. This book provides a unified vision of the algebraic themes which have developed so far in design theory. These include the applications in design theory of matrix algebra, the automorphism group and its regular subgroups, the composition of smaller designs to make larger designs, and the connection between designs with regular group actions and solutions to group ring equations. Everything is explained at an elementary level in terms of orthogonality sets and pairwise combinatorial designs—new and simple combinatorial notions which cover many of the commonly studied designs. Particular attention is paid to how the main themes apply in the important new context of cocyclic development. Indeed, this book contains a comprehensive account of cocyclic Hadamard matrices. The book was written to inspire researchers, ranging from the expert to the beginning student, in algebra or design theory, to investigate the fundamental algebraic problems posed by combinatorial design theory.

For additional information and updates on this book, visit
www.ams.org/bookpages/surv-175

AMS *on the* Web
www.ams.org

ISBN 978-0-8218-4496-0
9 780821 844960
SURV/175

SURV 175

Algebraic Design Theory

de Launey and Flannery

AMS

Mathematical Surveys and Monographs

Volume 175

Algebraic Design Theory

Warwick de Launey
Dane Flannery

American Mathematical Society

4-color Process / Pantone Process 232-6 , Pantone Process 228-1, Pantone Process 54-3

312 pages on 50 lb stock • Hardcover • Backspace 1 3/8"

What is the algebra in ADT?

A major part of the theory is concerned with *symmetry* of PCDs: structure of their automorphism groups.

In practice: matrix algebra, finite group theory, ring theory, character theory, group cohomology.

An *automorphism* of an $n \times n$ $\{\pm 1\}$-matrix D is a pair (P, Q) of $n \times n$ $\{\pm 1\}$-monomial matrices P, Q such that $PDQ^\top = D$.

The set of all automorphisms $\mathrm{Aut}(D)$ is a group; the stabilizer of D under action of $\mathrm{Mon}(n, \langle -1 \rangle)^2$ on the set of all $n \times n$ $\{\pm 1\}$-matrices (the orbit of D is its *equivalence* class; if D is a PCD—i.e., Hadamard—then everything in its equivalence class is too).

The subgroup of $\mathrm{Aut}(D)$ comprising all pairs of permutation matrices is its *permutation automorphism group* $\mathrm{PAut}(D)$.

Subgroups of $\mathrm{Aut}(D)$ that are of interest arise as follows (here in particular D can be any square matrix).

D is *group-developed* over a group G of order n if D up to permutation equivalence is an image of G's multiplication table: $D \approx [\phi(xy)]_{x,y\in G}$, some map ϕ on G.

Lemma

D is group-developed over $G \Leftrightarrow G$ acts regularly on D.

This is just the regular action of G on itself, with G indexing rows and columns of D:

$$P_g[\phi(xy)]P_g^\top = [\phi(xg^{-1}.y)]P_g^\top = [\phi(xg^{-1}.gy)] = D$$

giving a regular embedding $G \hookrightarrow \mathrm{PAut}(D)$.

Group development—*a purely algebraic notion*—gives effective tools from (computational) algebra to study PCDs.

However, group-development restricts *orthogonality*; e.g., group-developed Hadamard matrices must have square order.

de Launey and Horadam discovered a generalization of group development that is less restrictive when combined with orthogonality.

Set $U = \langle -1 \rangle$ (but often below U can be any finite abelian group). The *expanded matrix* of an $n \times n$ U-matrix D is

$$\mathcal{E}_D = \begin{bmatrix} D & -D \\ -D & D \end{bmatrix}.$$

D is said to be *cocyclic* if $\mathcal{E}_D$ is group-developed over a subgroup of $\mathrm{PAut}(\mathcal{E}_D)$ containing

$$\left(\begin{bmatrix} 0_n & 1_n \\ 1_n & 0_n \end{bmatrix}, \begin{bmatrix} 0_n & 1_n \\ 1_n & 0_n \end{bmatrix} \right).$$

as a central involution.

Theorem

D is cocyclic $\Leftrightarrow$ there exists a group G of order n and a 2-cocycle $\psi\colon G \times G \to U$ s.t. $D = [\psi(g,h)]_{g,h\in G}$ up to (full) equivalence.

Some definitions:

$Z^2(G,U) =$ group (abelian, under pointwise composition) of all cocycles $\psi\colon G \times G \to U$, i.e., such maps satisfying

$$\psi(x,y)\psi(xy,z) = \psi(x,yz)\psi(y,z) \quad \forall\, x,y,z \in G. \qquad (\star)$$

Coboundaries $\partial\phi$, where $\partial\phi(x,y) = \phi(x)\phi(y)\phi(xy)^{-1}$ for all maps $\phi\colon G \to U$, form a subgroup $B^2(G,U) \cong U^G/\mathrm{Hom}(G,U)$ of $Z^2(G,U)$.

$H^2(G,U) = Z^2(G,U)/B^2(G,U)$ is the second cohomology group of cocycle classes $[\psi] := \psi B^2(G,U)$, $\psi \in Z^2(G,U)$.

From now on, drop the superscript 2.

Each cocycle ψ determines a central extension E_ψ with element set $G \times U$ and multiplication defined by $(g,u)(h,v) = (gh, uv\psi(g,h))$; associativity of this multiplication is exactly $(\star)$.

Note that $U \cong \{(1,u) \mid u \in U\} \leq Z(E_\psi)$.

Re. the theorem: E_ψ acts centrally regularly on $\mathcal{E}_D$ for $D = [\psi(g,h)]_{g,h \in G}$.

If D is a cocyclic Hadamard matrix then the central extension groups E_ψ (*Hadamard groups*) were studied at length by Noboru Ito.

Note: $\mathrm{Aut}(D) \cong \mathrm{PAut}(\mathcal{E}_D)$; thus an Hadamard group embeds in the automorphism group of the original Hadamard matrix.

Group-development is the base case of cocyclic development: $[\partial\phi(g,h)]_{g,h\in G}$ is equivalent to $[\phi(gh)]_{g,h\in G}$.

To emphasize: the cocycle appears only because of a *centrally regular action* by a central extension of U by G on the expanded matrix.

And we have more freedom in cocyclic development vs. group development: e.g., cocyclic Hadamard matrices exist at non-square orders.

Indeed, many PCD constructions and (infinite) families of PCDs are cocyclic: inordinately many D have $\mathrm{PAut}(\mathcal{E}_D)$ that contain centrally regular subgroups.

Why this ubiquity of centrally regular actions?

While, e.g., codifying many known constructions, cocyclic development has perhaps been less successful in proving new existence results.

Theorem (de Launey and Kharaghani)

If q is odd and

$$k \geq 10 + 8 \left\lfloor \frac{\log_2(q-1)}{10} \right\rfloor,$$

then $\exists$ a cocyclic Hadamard matrix of order $2^k q$.

The proof is quintessential ADT; circulant (so group-developed) Hermitian and skew-Hermitian matrices are combined with cocyclic monomial matrices derived from a system of orthogonal designs, to produce cocyclic Butson Hadamard matrices over $\langle \mathrm{i} \rangle$, which yield the required cocyclic Hadamard matrices.

The bound in the theorem is about twice that for Hadamard matrices in general provided by Craigen, Holzmann, and Kharaghani.

From existence, to classification...the most noteworthy result on classifying cocyclic Hadamard matrices is that of Padraig Ó Catháin and Mark Röder.

They *completely* classified cHm at each order ≤ 36, relying on previous classifications of all Hadamard matrices, recognition of cocyclic development via $\mathrm{PAut}(\mathcal{E}_D)$, and an equivalence with relative difference sets.

Other work by Padraig with R. M. Stafford established non-existence of cocyclic matrices in a construction of Hadamard matrices: infinitely many "twin-prime-power" Hadamard matrices are *not* cocyclic.

Significant success by Assaf Goldberger and Giora Dula applying more powerful cohomological machinery; in particular to obtain new existence results for, e.g., weighing matrices.

Cohomology development subsumes cocyclic development.

Here the cohomology is in dimensions $0, 1$ as well as 2.

Also, trivial action on the underlying module is not assumed.

Cohomology-developed matrices are solutions of an "automorphism lifting problem"; cocyclic matrices are solutions of this problem that lift a group-developed matrix.

Unfinished work seeks to broaden Ito's non-existence results for cocyclic Hadamard matrices using the cohomology development approach.

Theorem (Ito)

(i) A cocyclic Hadamard matrix over a group G with cyclic Sylow 2-subgroup must be group-developed over G.

(ii) An Hadamard group of a cocyclic Hadamard matrix cannot have a dihedral Sylow 2-subgroup.

Re. (ii): this is about the *extension group*; $\exists$ many cocyclic Hadamard matrices *indexed* by dihedral groups.

Now we focus on the cocycles that appear in ADT.

Call $\psi \in Z(G,U)$ *orthogonal* if $[\psi(g,h)]_{g,h\in G}$ is Hadamard.
Call ψ *normalized* if $\psi(1,1) = 1$.

Lemma

Normalized ψ is orthogonal $\Leftrightarrow$ each non-initial row of $[\psi(g,h)]$ sums to 0.

Proof. Sleight of hand using $(\star)$.

N.B. orthogonality not respected by cohomological equivalence, i.e., ψ orthogonal $\not\Rightarrow \psi\partial\phi$ orthogonal.

Cf. work by J. A. Armario, et al.: *quasi-orthogonal* cocycles defined over groups of just even order. These are characterized by optimal row excess, just like orthogonal cocycles.

Obvious, dumb idea: construct all cocycles, then search for orthogonal ones.

For fixed G, *where* in $Z(G, U)$ to search for orthogonal cocycles?

Horadam discovered a certain action by G on $Z(G, U)$ that respects orthogonality. But of no help in the search problem by the Orbit-Stabilizer theorem.

If $|G|$ is not a square, then no coboundary is orthogonal, i.e., orthogonal cocycles are in non-trivial cohomology classes.

Universal coefficients theorem

$H(G, U) = I \times T$ where

I is the image of $\mathrm{Ext}(G/G', U)$ under inflation;

T is the image of a transgression map $\tau\colon \mathrm{Hom}(H_2(G), U) \to H(G, U)$.

Inflation and τ are injective homomorphisms.

Here $G' = [G, G]$ is the derived group of G, generated by all commutators $[g, h] := g^{-1}h^{-1}gh$ for $g, h \in G$;

$H_2(G)$ is the Schur multiplier $H^2(G, \mathbb{C}^\times)$.

A drawback of the UCT approach to computing cocycles for ADT is its non-canonical nature; whereas I may be canonically defined (& is easily calculated—reduces to 2-cohomology of cyclic groups and then Kronecker multiplication), τ and thus T depends on choice of presentation F/R for G (F free, R normal closure of relator words in F).

Can we characterize the canonical Ext component I?

Call $\psi \in Z(G,U)$ *symmetric* if $\psi(a,b) = \psi(b,a)$ for all $a,b \in G$; call ψ *almost symmetric* if $\psi(a,b) = \psi(b,a)$ for all $a,b \in G$ such that $ab = ba$.

The symmetric (resp., almost symmetric) cocycles form a subgroup $S(G,U)$ (resp., $A(G,U)$) of $Z(G,U)$.

Also $S(G,U)$, $B(G,U)$ are subgroups of $A(G,U)$.

Each cohomology class in I is represented by a symmetric cocycle; hence $I \subseteq A(G,U)/B(G,U)$.

Is the converse true? Certainly sometimes: e.g., if G has a presentation F/R s.t.

$(F' \cap R)/[R,F]$ is generated by a subset of $\{[x,y][R,F] \mid x,y \in F\}$, $\quad (\diamond)$

then yes, $I = A(G,U)/B(G,U)$.

(Note that $\{[x,y][R,F] \mid x,y \in F\}$ is a generating set for $F'/[R,F]$.)

The proof of this claim uses Hopf's formula in calculating τ:

$$H_2(G) \cong (F' \cap R)/[R,F].$$

Examples of G with presentations F/R that satisfy $(\diamond)$ are:

- abelian G (for which almost symmetric $=$ symmetric),
- metacyclic G.

What other classes, examples of G?

If $I = A(G,U)/B(G,U)$, then each almost symmetric cocycle is cohomologous to a symmetric cocycle.

But this is true always.

Theorem (Leutbecher)

$[\psi] \cap S(G,U) \neq \emptyset \Leftrightarrow [\psi] \cap A(G,U) \neq \emptyset$, i.e., $\psi \in A(G,U)$.

Thus $A(G,U) = S(G,U).B(G,U)$.

One direction is clear: as observed, $S(G,U), B(G,U) \subseteq A(G,U)$.

Here is a sketch of proof of the converse (see K. Wohlfahrt, Glasgow Math. J. **13**, 1972).

Switching to additive notation, define $\psi \in Z(G, U)$ inductively on G^n for $n \geq 3$ by

$$\psi(g_1, \ldots, g_n) = \psi(g_1, \ldots, g_{n-1}) + \psi(g_1 \cdots g_{n-1}, g_n).$$

Assume ψ normalized wlog. Using $(\star)$ it is then not hard to verify that:

$$\psi(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) = \psi(g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n);$$

$$\psi(g_1, \ldots, g_i, g_{i+1}, \ldots, g_n) = \psi(g_1, \ldots, g_i g_{i+1}, \ldots, g_n) + \psi(g_i, g_{i+1});$$

and consequently

$$\psi(g_1, \ldots, g_{i-1}, h, h^{-1}, g_{i+2} \ldots, g_n) = \psi(g_1, \ldots, g_{i-1}, g_{i+2}, \ldots, g_n) + \psi(h, h^{-1}).$$

Now suppose that ψ is almost symmetric.

Fix a set of representatives $\{c_1, c_2, \dots\}$ for the conjugacy classes of G.

Using almost symmetry of ψ and the above properties of the extended ψ, it can be shown that $\phi\colon G \to U$ given by

$$\phi\colon c_i^h \mapsto \psi(h^{-1}, c_i, h) - \psi(h^{-1}, h)$$

is well-defined, and satisfies

$$\phi(gh) - \phi(hg) = \psi(g,h) - \psi(h,g) \quad \forall\, g, h \in G. \tag{$*$}$$

Finally, it is immediate from $(*)$ that $\psi + \partial\phi \in S(G, U)$.

Alas, for the problem at hand, this result seems to be of little help; is ruling out existence of symmetric cocycles in elements of T (for some choice of F/R) significantly easier?