Design Theory

Padraig Ó Catháin

National University of Ireland, Galway

De Brún Centre Review, 13 May 2010

Design Theory in the de Brún Centre

- Focus on both computational and theoretical methods in design theory.
- A recurring theme is the use of algebraic methods, relying on computational group theory, in the analysis of designs.
- Conference on Design theory and applications: July 1-3 2009. Special Issue on Design Theory, *Cryptography and communications (Springer)*
- *People: P. Ó C., Dr. D. Flannery, Prof. K. Horadam (Information Theory and Security Research Group, RMIT, Melbourne), Dr. W. de Launey (CCR, San Diego), Dr. M. Röder, Dr. R.M. Stafford (NSA, USA)*

What is design theory?

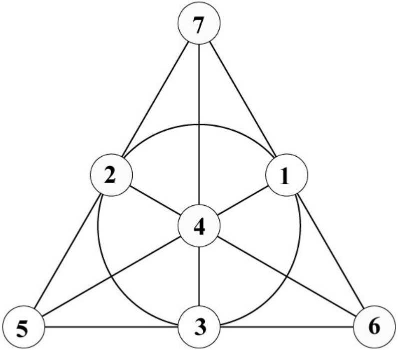
- A branch of combinatorics concerned with subset intersection problems.
- Designs are an abstraction of many combinatorial objects of independent interest, e.g. Latin squares, Hadamard matrices, strongly regular graphs.
- Origins in Fisher's work on the design of efficient experiments.

Definition

Let P be a set of size v, and B a collection of subsets of P, each subset of size k. We say that (P, B) is a t-(v, k, λ) *design* if the intersection of any t elements of B has size λ.

Example

- A 2-$(7, 3, 1)$ design.
- Let $P = \{1, 2, 3, 4, 5, 6, 7\}$.
- $B = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\}$



Questions in design theory

- Given parameters t, v, k and λ, does there exist a t-(v, k, λ) design?
- Given two designs with the same parameters, (P, B_1) and (P, B_2), are they equivalent? i.e. Does there exist a permutation $\sigma \in S_P$ such that $B_1^\sigma = B_2$?
- A more ambitious question: Given t, v, k, and λ, classify all t-(v, k, λ) designs up to equivalence.

Sample applications

- Design of multifactorial experiments.
- Hadamard matrices generate binary codes optimal with respect to the Plotkin bound.
- In group theory, some sporadic groups (e.g. the Mathieu groups, the Higman-Sims group) are most naturally defined as the automorphism groups of special designs.

Example of recent research: Classification of cocyclic Hadamard matrices

Joint work with Marc Röder, a former Marie Curie fellow in the de Brún centre.

- We completely classified all *cocyclic* Hadamard matrices of order < 40.
- For orders < 30, all Hadamard matrices had been previously classified.
- So for these orders, an algorithm which determines whether a given Hadamard matrix is cocyclic was sufficient.
- For orders $32, 36$, we used a theorem of de Launey, Flannery and Horadam which relates CHMs to relative difference sets.

Definition

Let H be a matrix of order n, with all entries in $\{1, -1\}$. Then H is a *Hadamard matrix* if and only if

$$HH^{\top} = nI_n.$$

- Existence of a Hadamard matrix of order $4n$ is equivalent to the existence of a 2-$(4n-1, 2n-1, n-1)$ design.
- Sylvester constructed Hadamard matrices of order $n = 2^t$.
- Hadamard constructed matrices of orders 12 and 20, and showed that the order had to be a multiple of 4.
- Paley constructed Hadamard matrices of order $n = p^t + 1$ for primes p, and conjectured that a Hadamard matrix of order n exists whenever $4 \mid n$.
- This is the *Hadamard conjecture*, and has been verified for all $n \leq 667$.

Cocyclic development

Definition

Let G a group and C an abelian group. We say that $\psi : G \times G \rightarrow C$ is a *cocycle* if

$$\psi(g, h)\psi(gh, k) = \psi(h, k)\psi(g, hk)$$

for all $g, h, k \in G$.

Definition

Let H be an $n \times n$ Hadamard matrix. Let G be a group of order n. We say that H is cocyclic if there exists a cocycle $\psi : G \times G \rightarrow \langle -1 \rangle$ such that

$$H = [\psi(g, h)]_{g,h \in G} .$$

Connection to relative difference sets

Theorem

(De Launey, Flannery & Horadam) The following statements are equivalent.

- *There is a cocyclic Hadamard matrix over G.*
- *There is a normal relative* $(4t, 2, 4t, 2t)$ *difference set in a central extension of* $N \cong C_2$ *by G, relative to* N.

Relative difference sets

- Let G be a finite group, with normal subgroup N. We say that $R \subset G$ is a relative difference set (RDS) with respect to N, if in the multiset of elements $\left\{r_1 r_2^{-1} \mid r_1, r_2 \in R\right\}$ every element of $G - N$ occurs exactly λ times, and no non-trivial element of N occurs.
- We are interested in difference sets with parameters $(4t, 2, 4t, 2t)$. That is difference sets in groups of order $8t$, relative to a forbidden subgroup of order 2, such that each element of $G - N$ may be expressed as a quotient of elements of the relative difference set in exactly $2t$ different ways.

Theorem

(Ó C. 2009) Let R be a $(4t, 2, 4t, 2t)$*-RDS. Then R corresponds to at least one and at most two equivalence classes of cocyclic Hadamard matrices. If there are two equivalence classes, then they are transpose equivalent.*

A procedure to construct all cocyclic Hadamard matrices of order $4t$

1. For each group of order $8t$, construct all $(4t, 2, 4t, 2t)$-RDSs.
2. From each RDS construct a Hadamard matrix and its transpose.
3. Test each new Hadamard matrix for equivalence with each Hadamard matrix previously found.

Step 2 is straightforward. (Linear algebra - milliseconds.)
Step 3: testing equivalence of Hadamard matrices is computationally expensive. We place each matrix in a canonical form, then test for **equality** with all previously found matrices. (For several thousand matrices - minutes.)

Results

- We calculated all $(4t, 2, 4t, 2t)$-RDSs in the groups of order 64 and 72.
- These were then converted into Hadamard matrices and tested for equivalence.
- Since Hadamard matrices are not generally transpose equivalent, the transposes of all surviving matrices were added to the list, and the list was reduced once more.
- 7373 RDSs were found in groups of order 32; these correspond to 100 inequivalent cocyclic Hadamard matrices.

Table of results

Order	Cocyclic	Indexing Groups	Extension Groups
2	1	1	2
4	1	2	3 / 5
8	1	3 / 5	9 / 14
12	1	3 / 5	3 / 15
16	5	13 / 14	45 / 51
20	3	2 / 5	3 / 14
24	16 / 60	8 / 15	14 / 52
28	6 / 487	2 / 4	2 / 13
32	$100/ \geq 3 \times 10^6$	49/51	261/267
36	$35 / \geq 3 \times 10^6$	12 /14	21 / 50

All data available at: www.maths.nuigalway.ie/$\sim$padraig

Selected publications

- de Launey & Flannery: Algebraic Design Theory. *American Mathematical Society*, to appear.
- LeBel, Flannery & Horadam: Group algebra series and coboundary modules, *Journal of Pure and Applied Algebra*
- Ó Catháin & Röder: Classification of Cocyclic Hadamard matrices of order 40, *Designs, Codes and Cryptography*
- Ó Catháin & Stafford: On twin prime power Hadamard matrices, *Cryptography and communications*
- Röder: *rds*, a refereed GAP package.
- Ó Catháin: MAGMA database of cocyclic Hadamard matrices.