An application of doubly transitive groups in design theory

Padraig Ó Catháin

National University of Ireland, Galway

St Andrews, 28 June 2010

Transitivity, multiple transitivity

- Let G be a permutation group on a finite set X.
- G is *transitive* if $x^G = \{y \in X \mid x^g = y, g \in G\} = X$.
- G has an action on the set of n-tuples of X: $[x_1, x_2 \ldots x_n]^g = \left[x_1^g, x_2^g, \ldots x_n^g\right]$.
- G is n-transitive if the induced action on the set of n-tuples is transitive.
- In particular, G is 2-transitive if for any $w, x, y, z \in X$ with $w \neq x$ and $y \neq z$ there exists $g \in G$ such that

$$w^g = y, \qquad x^g = z.$$

- The 2-transitive groups have been classified (using the CFSG).

Burnside's Theorem

- Classification of 2-transitive groups is via analysis of socles.
- Let N be a normal subgroup of G.
- N is *minimal* if 1 is the only normal subgroup of G properly contained in N.
- $Soc(G)$ is the subgroup of G generated by all minimal normal subgroups of G.

Theorem (Burnside)

Let G be a finite doubly transitive permutation group acting on X. Then $Soc(G)$ is either an elementary abelian group acting regularly on X, or a non-abelian simple group acting non-regularly on X.

Affine case

- Since we have an elementary abelian group, R, acting regularly, $|X| = p^n$ for prime p.
- G is an extension of R by some group H.
- Identifying R with a vector space of dimension n over $\mathbb{F}_p$, we may consider H a subgroup of $GL(n, p)$.
- The solvable case is considered by Huppert, Passman and others: H is semilinear.
- In the insoluble case, H contains $SL_n(q)$, $Sp_{2n}(q)$ or $G_2(q)'$ as a normal subgroup.

Non-Affine case

- G contains a nonabelian simple group, N, as a normal subgroup.
- Again $G = NH$, and so $N \leq G \leq Aut(N)$.
- The action of N is $3/2$-transitive, which in particular implies that N acts primitively.
- So determination of the non-affine doubly transitive groups consists of an analysis of the primitive permutation actions of the finite simple groups.
- The groups of Lie type are considered by Curtis, Kantor and Seitz.
- Detailed analysis of the sporadics is 'folklore' and has never been published.

Motivation

A question of K. Horadam: Do *Hadamard matrices* developed from *twin prime power difference sets* have the *cocyclic property*?

- We say that the $n \times n$ matrix H is *Hadamard* if every entry of H is in $\{\pm 1\}$ and
$$HH^\top = nI_n.$$
- Necessary conditions for the existence of a Hadamard matrix are that $n = 1, 2$ or $4t$ for $t \in \mathbb{N}$.
- It is not known if a Hadamard matrix of order n exists for all such n, the smallest unknown case being $n = 668$.
- We want 'algebraic' constructions for Hadamard matrices.

Difference sets

- Let G be a finite group and D a subset of G.
- D is a *difference set* if every non-identity element of G occurs as a 'difference' of elements of D a constant number of times.
- That is, for any $g \neq 1 \in G$, there are exactly λ ordered pairs (d_1, d_2) of elements of D such that $d_1 d_2^{-1} = g$.
- e.g. Let $G = \mathbb{Z}/7\mathbb{Z}$, and $D = \{1, 2, 4\}$ then every non-identity element of G occurs once as a difference of elements of D.

Theorem (Stanton & Sprott)

Let C_{p^a} and C_{q^b} be elementary abelian groups. If $p^a - q^b = 2$ then there exists a difference set in $C_{p^a} \times C_{q^b}$.

- Suppose $|G| = 4t - 1$, $D \subseteq G$ a difference set with $|D| = 2t - 1$ and every element is represented $t - 1$ times. Then we call D a *Hadamard difference set*.
- Let M be a $(0, 1)$-matrix with rows and columns indexed by elements of G, and $m_{i,j} = 1$ if $g_i g_j^{-1} \in D$ and $m_{i,j} = 0$ otherwise. We say that M is the matrix *associated* with D.

Denoting the all $+1$s matrix of order $4t - 1$ by J, we have

$$MM^{\top} = tI + (t - 1)J.$$

Let $S = 2M - J$. Then

$$SS^{\top} = 4tI - J.$$

So appending a row and column of $+1$s to S, we obtain a Hadamard matrix.

Matrix Automorphisms

- Let M be an $n \times n$ matrix with entries in a commutative ring, R. Then the pair of R-monomial matrices (P, Q) is an *automorphism* of M if
$$PMQ^{\top} = M.$$
- The automorphisms of M form a group.
- This group has an induced permutation action on a set of size n: if σ maps r_i to r_j then $i^{\overline{\sigma}} = j$. Denote this (permutation) group by $\mathcal{A}(M)$.

Group Development

- Let G be a finite group, and let $X_G = \{X_g \mid g \in G\}$ be a set of commuting indeterminates indexed by the elements of G.
- Take an ordering on the elements of G. The *group matrix* of G is

$$M(G) = \left[X_{gh^{-1}}\right]_{g,h\in G}.$$

- Let $f : X_G \to R$ be a set-map into any ring. Then $\left[f(X_{gh^{-1}})\right]$ is a *matrix group developed over G*.

Theorem

If M is group developed, then $\mathcal{A}(M)$ contains a regular subgroup isomorphic to G.

Let D be a difference set in G. Then the matrix associated with D is group developed over G. *Cocyclic development* is a generalisation of group development. If M is cocyclic, $\mathcal{A}(M)$ is transitive.

- Let D be a difference set in G, and let M be the matrix associated with D. Let H be the Hadamard matrix (of order $4n$) developed from D.
- Then H contains a submatrix of order $4n - 1$ which is essentially the same as M. In particular its automorphism group is permutation isomorphic to that of D.
- So $\mathcal{A}(H)$ contains a subgroup which stabilises the first point and is transitive on the remaining points.
- So $\mathcal{A}(H)$ is transitive if and only if it is 2-transitive.

Hadamard matrices with transitive automorphism groups

We went through the classification of 2-transitive groups and ruled all of them out as candidates for a 2-transitive action on a TPP-Hadamard matrix, (except $PSL_3(p^k)$ for some primes). This was surprisingly easy.

Theorem (Ito)

Let $\Gamma \leq \nu(\mathrm{Aut}(H))$ *be a non-affine doubly transitive permutation group acting on the set of rows of a Hadamard matrix* H*. Then the action of* Γ *is one of the following.*

- $\Gamma \cong M_{12}$ *and* H *is the unique Hadamard matrix of order* 12*.*
- $PSL_2(p^k) \trianglelefteq \Gamma$ *acting naturally on* $p^k + 1$ *points, for* $p^k \equiv 3 \mod 4$*,* $p^k \neq 3, 11$*.*
- $\Gamma \cong Sp_6(2)$*, and* H *is of order* 36*.*

- Now, to answer Horadam's question, we observed that a Hadamard matrix developed from a twin prime power difference set necessarily has order $n^2 = p^a q^b + 1$ where $\left|p^a - q^b\right| = 2$.
- We then show that these orders coincide with Ito's list only finitely many times, and check that the matrices at each of these orders do not have transitive automorphism groups. Hence the matrices are not cocyclic.

Future work:
From Ito's list, establish all difference sets with 2-transitive automorphism groups.

Bibliography:

- 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*
- www.maths.nuigalway.ie/~padraig