Difference sets and Hadamard matrices

Padraig Ó Catháin

National University of Ireland, Galway

17 May 2012

Outline

1. 2-designs and difference sets

2. Skew difference sets

Designs

Definition

Let (V, B) be an incidence structure in which $|V| = v$ and $|b| = k$ for all $b \in B$. Then $\Delta = (V, B)$ is a (v, k, λ) ***design*** if and only if any pair of elements of V occurs in exactly λ blocks.

Definition

The design Δ is ***symmetric*** if $|V| = |B|$.

We give an example of a symmetric $(16, 6, 2)$ design, Δ.

Example

Let $V = C_4^2$, i.e. the points of Δ are the elements of the group $C_4 \times C_4$. The blocks of Δ are also labelled by the elements of C_4^2, with $b_{(x,y)} = \{(w, z) \mid w = x \text{ or } z = y \text{ but not both}\}$.
Every block contains 6 points. Every pair of points are contained in precisely 2 blocks. (Requires checking a number of cases, e.g. that $(x, y), (x, z)$ occur together in the two blocks indexed by $(x, *)$, $* \neq y, z$.)

A projective plane is an example of a symmetric design with $\lambda = 1$.

Example

Let $\mathbb{F}$ be any field. Then there exists a projective plane over $\mathbb{F}$ derived from a 3-dimensional $\mathbb{F}$-vector space. In the case that $\mathbb{F}$ is a finite field of order q we obtain a geometry with

- $q^2 + q + 1$ points and $q^2 + q + 1$ lines.
- $q + 1$ points on every line and $q + 1$ lines through every point.
- Every pair of lines intersecting in a unique point.

Applications of designs

- Design of experiments: designs derived from Hadamard matrices provide constructions of Orthogonal Arrays of strengths 2 and 3.
- Signal Processing: sequences with low autocorrelation are provided by designs with circulant incidence matrices.
- Coding Theory: A class of binary codes derived from the rows of a Hadamard matrix are optimal with respect to the Plotkin bound. A particular family of examples (derived from the $(16, 6, 2)$ design given) are linear, and were used in the Mariner 9 missions. Such codes enjoy simple (and extremely fast) encryption and decryption algorithms.
- Quantum Computing: Hadamard matrices arise as unitary operators used for entanglement.

Incidence matrices

Definition

Define a function $\phi : V \times B \to \{0, 1\}$ given by $\phi(v, b) = 1$ if and only if $v \in b$. An ***incidence matrix*** for Δ is a matrix

$$M = [\phi(v, b)]_{v \in V, b \in B} .$$

Lemma

The $v \times v$ $(0, 1)$-matrix M is the incidence matrix of a 2-(v, k, λ) *symmetric design if and only if*

$$MM^{\top} = (k - \lambda)I + \lambda J$$

Proof.

Entry (i, j) in $MM^{\top}$ is the inner product of the i^{th} and j^{th} rows of M. This is $|b_i \cap b_j|$. □

Automorphisms of 2-designs

Definition

An ***automorphism*** of a symmetric 2-design Δ is a permutation $\sigma \in \mathrm{Sym}(V)$ which preserves B setwise.

Example

The group $C_4 \times C_4$ is a group of automorphisms of the design Δ, acting regularly on points and on blocks.

The automorphisms of Δ form a **group**, $\mathrm{Aut}(\Delta)$. **Difference sets** correspond to regular subgroups of $\mathrm{Aut}(\Delta)$.

Difference sets

- Suppose that G acts regularly on V.
- Labelling one point with 1_G induces a labelling of the remaining points in V with elements of G.
- So blocks of Δ are subsets of G, and G also acts regularly on the blocks.
- So all the blocks are translates of one another: every block is of the form bg relative to some fixed base block b.
- So $|b \cap bg| = \lambda$ for any $g \neq 1$. This can be interpreted in light of the multiplicative structure of the group.
- Identifying b with the $\mathbb{Z}G$ element $\hat{b} = \sum_{g \in b} g$, and doing a little algebra we find that $\hat{b}$ satisfies the identity $\hat{b}\hat{b}^{(-1)} = (k - \lambda) + \lambda G$.

Difference sets

Definition

Let G be a group of order v, and $\mathcal{D}$ a k-subset of G. Suppose that every non-identity element of G has λ representations of the form $d_i d_j^{-1}$ where $d_i, d_j \in \mathcal{D}$. Then $\mathcal{D}$ is a (v, k, λ)-difference set in G.

Theorem

If G contains a (v, k, λ)-difference set then there exists a symmetric 2-(v, k, λ) design on which G acts regularly. Conversely, a 2-(v, k, λ) design on which G acts regularly corresponds to a (v, k, λ)-difference set in G.

Example

The difference set $\mathcal{D} = \{1, 2, 4\}$ in $\mathbb{Z}_7$ gives rise to a 2-$(7, 3, 1)$ design as follows: we take the group elements as points, and the translates $\mathcal{D} + k$ for $0 \leq k \leq 6$ as blocks.

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

- $MM^\top = (3 - 1)I + J$: M is the incidence matrix of a 2-$(7, 3, 1)$ design.
- In fact this is an incidence matrix for the Fano plane.

Summary (of difference sets and symmetric designs)

- Design theory studies finite set systems with rigid intersection properties.
- Applications are to problems involving **correlation**.
- The main open problems in design theory concern existence of designs.
- Abstract algebra provides constructions and non-existence results.
- Difference sets are particularly useful algebraic analogues of symmetric designs.

- Many families of difference sets are known: classification seems impossible.
- Some parameter sets are better understood then others, e.g. difference sets with $\lambda = 1$ correspond to finite projective planes, and difference sets with parameters $(4t-1, 2t-1, t-1)$ correspond to Hadamard matrices (which have their own existence theory).
- In this talk we study difference sets satisfying the following **skewness** condition:

Definition

Let $D \subseteq G$, where G is a group of odd order. We say that D is **skew** if for every $g \in G$, $|D \cap \{g, g^{-1}\}| = 1$.

Existence of skew difference sets

- Let $\mathbb{F}_q$ be a finite field, $q = 4t - 1$.
- There are $2t - 1$ quadratic residues in $\mathbb{F}_q$.
- The quadratic residues of $\mathbb{F}_q$ form a difference set in $(\mathbb{F}_q, +)$, this is Paley's Theorem.
- The element x is a quadratic residue mod q if and only if $-x$ is **not** (quadratic reciprocity).
- So the Paley difference sets are skew.
- So there exists a skew difference set with parameters $(4t - 1, 2t - 1, t - 1)$ whenever $4t - 1$ is a prime power.

- It is easily seen that **every** skew difference set has parameters $(4t-1, 2t-1, t-1)$. (It is enough to observe that k determine λ, and that these numbers must be integers.)
- Suppose that D is a skew difference set in an **abelian** group. Then $4t-1$ is a prime power.
- If $4t-1$ is cyclic, then D is equivalent to a Paley difference set.
- In the general abelian case, $\exp(G)^2 \mid |G|$.

On the strength of this evidence, it was conjectured that all skew difference sets were Paley.

Then in 2006, Ding and Yuan produced a counterexample...

Theorem

Let $\mathbb{F}_q$ be a field of order $3^{2n+1} = 4t - 1$. The set of images of the polynomial $g(x) = x^{10} + x^6 - x^2$ has size $2t - 1$ and is a skew difference set in $(\mathbb{F}_q, +)$. For $q = 3^5$ and 3^7, these difference sets are inequivalent to the Paley difference sets.

They conjecture that these difference sets are never equivalent to the Paley difference sets. But no sufficiently fine invariants have been found to verify this conjecture...

Once others began to look for skew Hadamard difference sets, they found them.

- Wend and Hu: there are 5 inequivalent skew difference sets in each of C_3^5 and C_3^7 and at least 4 in each C_3^{2n+1}. (2006)
- Ding, Wang and Xiang: another construction in characteristic 3, via symplectic geometry (2007).
- Weng, Qiu, Wang and Xiang: yet another construction from semifields generalising Ding-Yuan. (2007)
- Feng: a construction of skew difference sets in nonabelian groups of order p^3 and exponent p for all primes $p \equiv 3 \mod 4$, a proof that this family is inequivalent to the Paley family. (2009)
- Muzychuk: There are exponentially many (in q) equivalence classes of skew-Hadamard difference sets in elementary abelian groups of order q^3. (2011)
- Momihara: A new construction generalising some sporadic cyclotomic difference sets. (2012)

But:

- There are still no general inequivalence results; it is unlikely that all of these constructions are pairwise inequivalent.
- There are no unified constructions, or signs of a classification - results are isolated and methods ad hoc.
- All these results occur either in characteristic 3 or in groups of (moral) rank 3.

- The Hadamard matrices associated with the Paley difference sets are characterized among all Hadamard matrices by having non-affine doubly transitive automorphism groups.
- This group can be interpreted as a ‘transitive extension’ of the automorphism group of the Paley 2-design. We say that the Paley difference sets have the *transitive extension* property.
- We produced a classification of $(4t-1, 2t-1, t-1)$ difference sets with the transitive extension property. (The affine case is work in progress.)

Theorem (Ó C., 2012, JCTA)

Let p be a prime, and $n = kp^{\alpha} \in \mathbb{N}$.

- *Define*

$$G_{p,k,\alpha} = \left\langle a_1, \ldots, a_n, b \mid a_i^p = 1, \left[a_i, a_j\right] = 1, b^{p^{\alpha}} = 1, a_i^b = a_{i+k} \right\rangle .$$

- *The subgroups*

$$R_e = \left\langle a_1 b^{p^e}, a_2 b^{p^e}, \ldots, a_n b^{p^e} \right\rangle$$

  for $0 \leq e \leq \alpha$ contain skew Hadamard difference sets.
- *Each difference set gives rise to a Paley Hadamard matrix.*
- *These are the only non-affine difference sets which give rise to Hadamard matrices in which $\mathcal{A}_H$ is transitive.*
- *These are the only skew difference sets which give rise to Hadamard matrices in which $\mathcal{A}_H$ is transitive.*