LINKED SYSTEMS OF DESIGNS

Bill Martin
Dept. of Mathematical Sciences
and
Dept. of Computer Science

Worcester Polytechnic Institute
(WPI)

AMS Special Session on Codes & Designs
Richmond VA Sun. Nov. 7, 2010

MY CO-AUTHORS

This talk will be based mainly on the preprint

Uniformity in association schemes and coherent configurations: cometric Q-antipodal schemes and linked systems

written along with Edwin van Dam and Misha Muzychuk

But it also involves ongoing joint work with Jason Williford.

ASSOCIATION SCHEMES

Finite set X of size v
Symmetric relations $R_0, R_1, \ldots, R_d$ on X satisfying

- $R_0 = id_X = \{(a,a) : a \in X\}$
- $X \times X = R_0 \dot\cup R_1 \dot\cup \cdots \dot\cup R_d$
- there exist integers p_{ij}^k such that $|\{c \in X : (a,c) \in R_i \text{ and } (c,b) \in R_j\}| = p_{ij}^k$ whenever $(a,b) \in R_k$

BOSE-MESNER ALGEBRA

Let A_i denote the adjacency matrix of the (undirected) graph (X, R_i). Then

$$\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$$

satisfy

- $A_0 = I$
- $A_0 + A_1 + \cdots + A_d = J$ (all ones matrix)
- $A_i A_j = \sum_{k=0}^{d} p_{ij}^{k} A_k$

So the linear span

$$\mathbb{A} = \mathrm{span}_{\mathbb{R}}(A_0, A_1, \ldots, A_d)$$

is a commutative algebra of symmetric matrices also closed under entrywise (Schur, or Hadamard) multiplication. (This is the Bose-Mesner algebra.)

Q-POLYNOMIAL SCHEMES

The Bose-Mesner algebra $\mathbb{A}$ has a basis

$$\{E_0, E_1, \ldots, E_d\}$$

of primitive idempotents ($E_i E_j = \delta_{ij} E_i$) and is closed under entrywise multiplication. So there exist scalars q_{ij}^k satisfying

$$E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^{d} q_{ij}^k E_k$$

We say the scheme is Q-polynomial (or cometric) if there is an ordering $E_0, E_1, \ldots, E_d$ for which

$$q_{ij}^k = 0 \quad \text{when } k > i+j$$

$$q_{ij}^k \neq 0 \quad \text{when } k = i+j$$

IMPRIMITIVE Q-POLY. SCHEMES

An association scheme

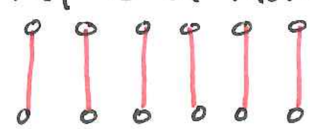
$$(X, \{R_0, R_1, \ldots, R_d\})$$

is imprimitive if some graph $G_i = (X, R_i)$ with $1 \le i \le d$ is disconnected.

THEOREM: (Suzuki '98, Cerzo/Suzuki '06, Tanaka/Tanaka '10)

An imprimitive Q-polynomial association scheme is either

* Q-bipartite (some R_i is a matching)



* Q-antipodal
* both

TODAY'S TOPIC ($d = 3, 4$ ONLY)

COHERENT CONFIGURATIONS

These are a generalization of association schemes. Change as follows

- ~~id_X is a relation~~

replaced by

- id_X is a <u>union</u> of relations

and

- ~~each R_i is a symmetric relation~~

replaced by

- for each R_i, R_i^T is also a relation

Now the matrix algebra $\mathbb{A}$ is a coherent algebra.

EXAMPLE: If group G acts on finite set X, then the orbits on pairs

$$R_i = \{ (x^g, y^g) : g \in G \}$$

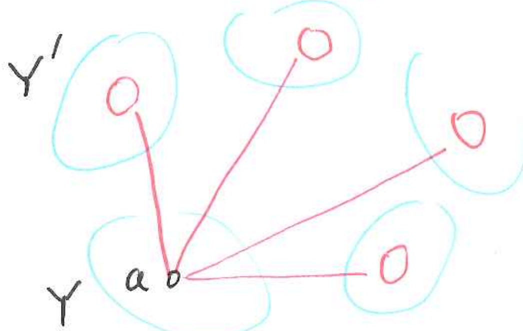
form a coherent configuration.

UNIFORM SCHEMES

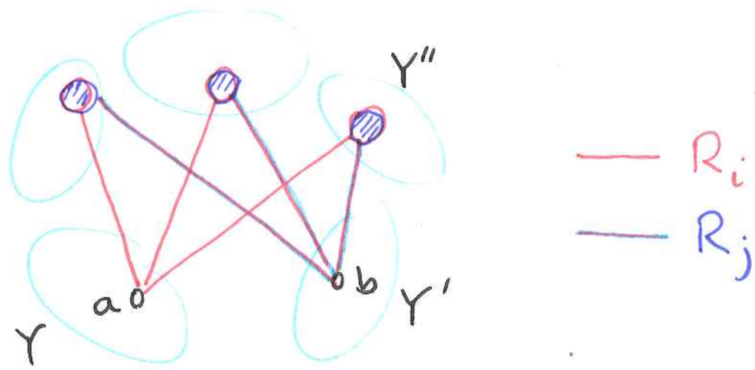
Vertex set X is partitioned into fibres

$$X = Y_1 \,\dot\cup\, Y_2 \,\dot\cup \cdots \dot\cup\, Y_w$$

relation "between" fibres



In relation R_i, $a \in Y$ has $p_{ii}^0/(w-1)$ i-neighbors in each fibre $Y' \neq Y$



a,b in distinct fibres have

$$\left|\{c \in Y'' : (a,c) \in R_i \text{ and } (c,b) \in R_j\}\right| = \frac{p_{ij}^k}{w-2}$$

when $a \in Y$, $b \in Y' \neq Y$ are k-related.

THEOREM – UNIFORM SCHEMES

A scheme is uniform if and only if it is dismantlable.

A cometric scheme is uniform if and only if it is Q-antipodal.

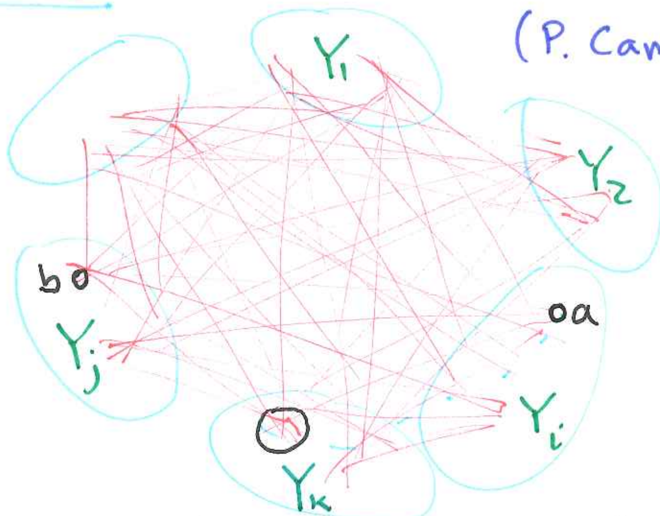
Every uniform scheme is contained in a coherent configuration which has

$$id_Y = \{(a,a) : a \in Y\}$$

as a basis relation for each fibre in the scheme.

LINKED SYSTEMS OF SYMMETRIC DESIGNS

(P. Cameron)



Vertex set X is partitioned into w fibres of size v (homogeneous case)

$$X = Y_1 \dot\cup Y_2 \dot\cup \cdots \dot\cup Y_w$$

Relation R_1 has no edges with both ends in same fibre,

Between any two distinct fibres, R_1 induces the incidence graph of a symmetric (v, k, λ) design

For any three distinct fibres Y_i, Y_j, Y_k if $a \in Y_i$ and $b \in Y_j$ then the number of common neighbors of a and b in Y_k is λ if a and b are incident and μ otherwise.

VAN DAM'S THEOREM

Q-antipodal cometric association schemes with $d=3$ are in one-to-one correspondence with linked systems of symmetric designs.

EXAMPLES?

One infinite family due to Cameron and Seidel coming from Kerdock codes (1974)

Mathon (1981): Computer search to link $(16,6,2)$ designs

$128 = 16 + 16 + \cdots + 16$ (above example)

$48 = 16 + 16 + 16$

$32 = 16 + 16$

REAL MUTUALLY UNBIASED BASES

A set of k real MUBs in dimension d is a collection

$$\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k\}$$

of orthonormal bases for $\mathbb{R}^d$ satisfying

$$b \cdot b' = \pm \frac{1}{\sqrt{d}} \qquad b \in \mathcal{B}_i \quad b' \in \mathcal{B}_j \quad (i \neq j)$$

Known Results: M_d = max # bases in dim. d

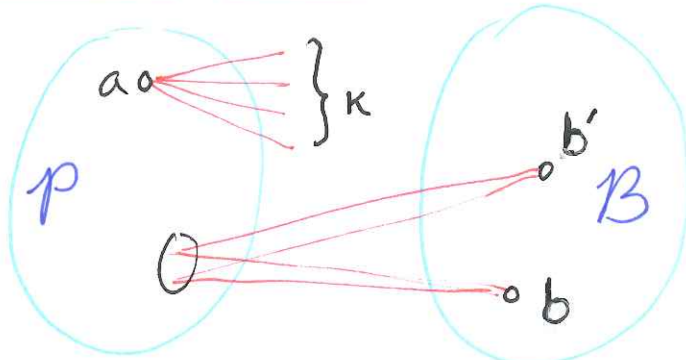
- $M_d \geq 2$ iff $\exists$ $d \times d$ Hadamard matrix
- $M_d \geq 3$ iff. $\exists$ $d \times d$ HMs H_1, H_2, H_3 satisfying
  $$H_1 H_2 = \sqrt{d}\, H_3$$
- $M_d \leq \frac{d}{2} + 1$
- If $\exists$ HM of side $\sqrt{d}$ then
  $$M_d \geq 2 + \#\mathrm{MOLS}(\sqrt{d})$$

THEOREM (LeCompte, Owens, WJM)

Q-bipartite Q-antipodal cometric association schemes with $d=4$ are in one-to-one correspondence with sets of real MUBs.

Linked systems of Hadamard symmetric nets

STRONGLY REGULAR DESIGN



Incidence structure $(\mathcal{P}, \mathcal{B}, \mathcal{I})$
semiregular
Any two points lie in α or β common blocks

$\Rightarrow$ Strongly reg. graph on $\mathcal{P}$

Any two blocks contain λ or μ common points

$\Rightarrow$ strongly reg. graph on $\mathcal{B}$

Our case: these two graphs must have same parameters.

Connection to Association Schemes: Linking these up, we obtain all 4-class association schemes which are Q-antipodal (and, hence, Q-polynomial/cometric)

EXAMPLES — LINKED SYSTEMS OF STRONGLY REGULAR DESIGNS

- $168 = 56 + 56 + 56$
  Hyperovals in $PG(2,4)$
- $150 = 50 + 50 + 50$
  Cocliques in Hoffman-Singleton graph
- $729 = 243 + 243 + 243$
  dual of ternary Golay code
- Hemisystems in generalized quadrangles
- real mutually unbiased bases
- $4224 = 1408 + 1408 + 1408$
  Higman's Leech lattice example
- Higman triality schemes
  $D_4(q)$ extends via $O_8^+(q)$

DIFFERENCE SETS

So I have a problem for you:

For which triples (v, k, λ) can you find three (v, k, λ) difference sets D_1, D_2, D_3 satisfying

$$|D_1 \cap (g + D_2)| = \begin{cases} \lambda', & g \in D_3 \\ \mu', & g \notin D_3 \end{cases}$$

for all $g \in G$?

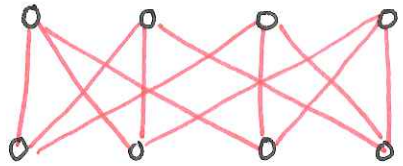
(NOTE: I am assuming here that D_1, D_2, D_3 all live in the same group, but this can be relaxed.)

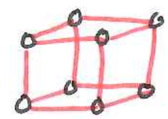
Connection to Association Schemes:

If you can achieve this not only for triple (D_1, D_2, D_3) but also for triples $(D_3, -D_2, D_1)$ and $(-D_3, -D_1, D_2)$, then you have a linked system of symmetric designs with three fibres.

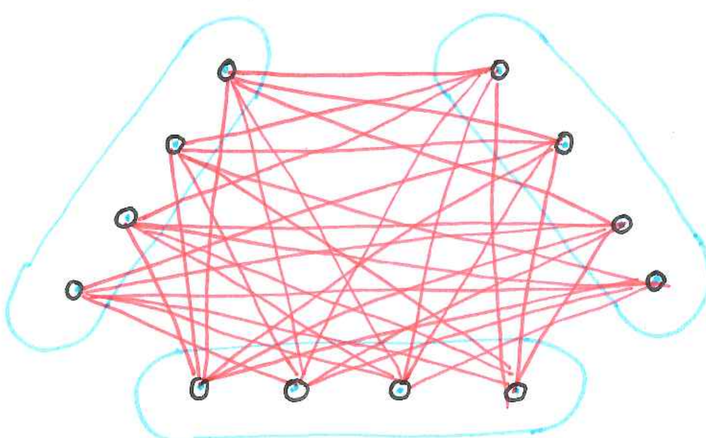
ONE LAST SMALL EXAMPLE

$(4,3,2)$ symmetric design

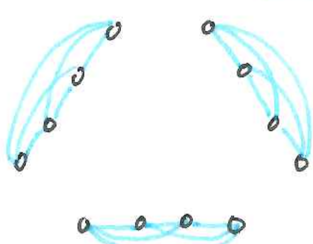


(or just )

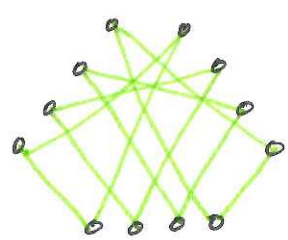
can be linked up to give a 3-class association scheme



R_1



R_2



R_3

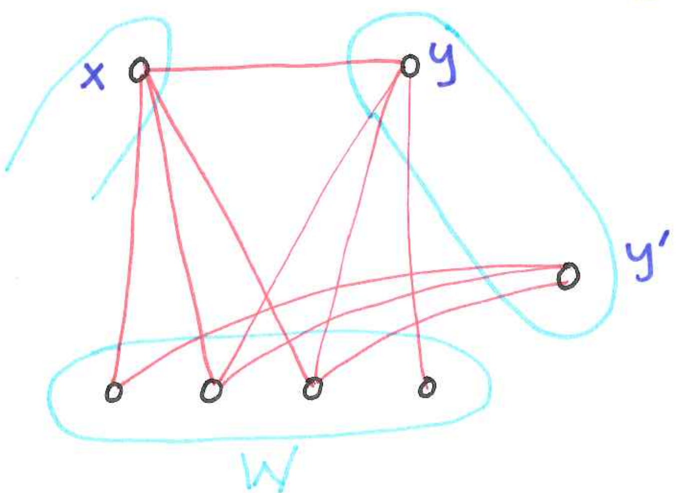
(degenerate: two imprimitivity systems in this case)

THE "LINKED" PROPERTY

As you see here (as in the general case), given any three distinct fibres

$$U, V, W$$

and vertices $x \in U$ and $y \in V$ the number of $z \in W$ incident to both x and y depends <u>only</u> on whether x and y are incident



In this example $\lambda = 2$

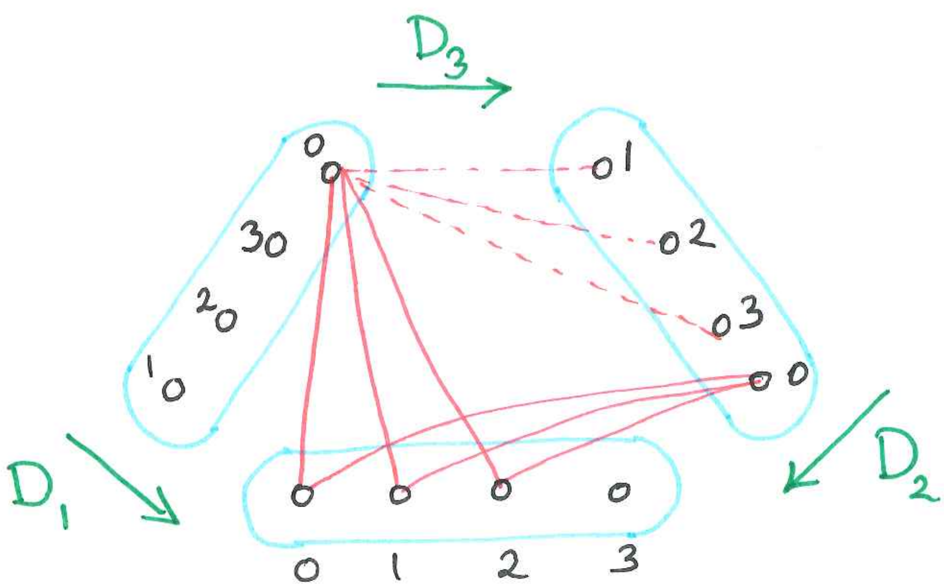
$\mu = 3$

THIS IS A DIFFERENCE SET CONSTRUCTION!

Note that this trivial example is one solution to the above open problem.

$$G = \mathbb{Z}_4$$

$$D_1 = D_2 = \{0, 1, 2\} \qquad D_3 = \{1, 2, 3\}$$



QUESTIONS?

THANK YOU

And, on behalf of all the participants, thanks to the organizers

Jim and Qing