

Real Mutually Unbiased Bases and Association Schemes

Nicholas LeCompte
William J. Martin
William Owens

Department of Mathematical Sciences
WPI

SIAM DM08



Outline

Real Mutually Unbiased Bases



Outline

Real Mutually Unbiased Bases

Association Schemes

Outline

Real Mutually Unbiased Bases

Association Schemes

Two Observations

The 24-cell

- ▶ 24 unit vectors in \mathbb{R}^4 :
- ▶ $\pm \mathbf{e}_i, \quad \pm \mathbf{e}_1 \pm \mathbf{e}_2 \pm \mathbf{e}_3 \pm \mathbf{e}_4$
- ▶ angles $60^\circ, 90^\circ, 120^\circ, 180^\circ$
- ▶ take one from each antipodal pair \Rightarrow three orthonormal bases
- ▶ mutually unbiased: $\langle \mathbf{b}, \mathbf{b}' \rangle = 1/\sqrt{4}$ whenever \mathbf{b} and \mathbf{b}' are chosen from different bases

Real MUBs

k orthonormal bases in \mathbb{R}^d :

- ▶ $\mathcal{B}_i = \{\mathbf{b}_{i,1}, \dots, \mathbf{b}_{i,d}\}$
- ▶ mutually unbiased: $\langle \mathbf{b}, \mathbf{b}' \rangle = 1/\sqrt{d}$ whenever \mathbf{b} and \mathbf{b}' are chosen from different bases

Question: What is the maximum number, $k(d)$, of mutually unbiased bases (“MUBs”) in \mathbb{R}^d ?

What's Known

dim. d	bounds on $k(d)$
any d	$\leq \frac{d}{2} + 1$ (DGS)
4^i	$= \frac{d}{2} + 1$ (CHKSS) “maximal”
$d \neq 4n, d > 2$	= one
$4n$ (n non-sq.)	\leq two, (equality iff $\exists d \times d$ HM)
$4s^2$ (s odd)	\leq three (BSTW)
$4^i s^2$ (s odd)	$\geq 2 + \#MOLS(2^i s)$, if $\exists \sqrt{d} \times \sqrt{d}$ HM (WB)

Delsarte, Goethals, Seidel / Calderbank, et al. / Boykin, et al. /
 Wocjan and Beth

Bannai and Bannai

Kerdock-like code: binary code of length N where the only non-zero weights are

$$\frac{1}{2}(N \pm \sqrt{N}), \quad \frac{1}{2}N, \quad N$$

Question: Are all Kerdock-like codes Kerdock?

Question: Does existence imply $N = 4^i$?

Schemes from MUBs from Codes

Bannai and Bannai proved

maximal MUBs \Leftrightarrow Kerdock-like code
maximal MUBs \Rightarrow 4-class association scheme (and more)

The vertices of the scheme can be viewed as $\pm \mathbf{b}_{i,j}$.

Definition

A finite set X of points on the unit sphere in \mathbb{R}^m is an *association scheme* if there exists integers $p_{i,j}^k$ such that

$$|\{\mathbf{c} : \mathbf{a} \sim_i \mathbf{c} \sim_j \mathbf{b}\}| = p_{i,j}^k$$

whenever $\mathbf{a} \sim_k \mathbf{b}$ in X

where $\mathbf{a} \sim_k \mathbf{b}$ means $\langle \mathbf{a}, \mathbf{b} \rangle = \sigma_k$ for some sequence $\sigma_0 = 1 > \sigma_1 > \dots > \sigma_e$ of scalars.

24-cell

For example, the 24-cell has inner products

$$\sigma_0 = 1, \sigma_1 = \frac{1}{2}, \sigma_2 = 0, \sigma_3 = -\frac{1}{2}, \sigma_4 = -1$$

and, for example,

$$[p_{1,j}^k]_{k,j} = \begin{bmatrix} 0 & 8 & 0 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 0 & 4 & 0 & 4 & 0 \\ 0 & 1 & 3 & 3 & 1 \\ 0 & 0 & 0 & 8 & 0 \end{bmatrix}$$

First Observation

The schemes constructed by Abdukhalikov, Bannai and Suda are all Q -polynomial, Q -bipartite, and Q -antipodal. So by the Dismantling Theorem, any subcollection of a maximal collection of MUBs also forms a Q -polynomial scheme.

Second Observation

Every 4-class scheme which is both Q -antipodal and Q -bipartite gives rise to a set of real MUBs.

In other words

real MUBs \Leftrightarrow 4-class Q -antip. Q -bip. assoc. schemes

Eigenvalues of a SRG

We have a Q -bipartite double cover of a $SRG(v, k, \lambda, \mu)$

$$\tilde{P} = \begin{bmatrix} 1 & k & v-1-k \\ 1 & r & -r-1 \\ 1 & s & -s-1 \end{bmatrix}, \quad \tilde{Q} = \begin{bmatrix} 1 & f & g \\ 1 & fr/k & gs/k \\ 1 & -\frac{f(r+1)}{v-1-k} & -\frac{g(s+1)}{v-1-k} \end{bmatrix}$$

Dual Eigenvalues of our 4-Class Scheme

Assume first non-trivial column in decreasing order.

$$Q = \begin{bmatrix} 1 & f & g \\ 1 & fr/k & gs/k \\ 1 & -\frac{f(r+1)}{v-1-k} & -\frac{g(s+1)}{v-1-k} \\ 1 & fr/k & gs/k \\ 1 & f & g \end{bmatrix}$$

Q -antipodal

Since our scheme is Q -antipodal, the last column must read
 $k - 1, -1, k - 1, -1, k - 1$
for some integer k

Imprimitive SRG

So we must have a complete multipartite quotient:

$\text{compl}(kK_d)$

$$\tilde{P} = \begin{bmatrix} 1 & d(k-1) & d-1 \\ 1 & 0 & -1 \\ 1 & -d & d-1 \end{bmatrix}, \tilde{Q} = \begin{bmatrix} 1 & k(d-1) & k-1 \\ 1 & 0 & -1 \\ 1 & -k & k-1 \end{bmatrix}$$

Dual Eigenvalues of our 4-Class Scheme

So we start with

$$Q = \begin{bmatrix} 1 & k(d-1) & k-1 \\ 1 & 0 & -1 \\ 1 & -k & k-1 \\ 1 & 0 & -1 \\ 1 & k(d-1) & k-1 \end{bmatrix}$$

Dual Eigenvalues of our 4-Class Scheme

Q -bipartite condition:

$$Q = \begin{bmatrix} 1 & m_1 & k(d-1) & k-1 \\ 1 & \frac{m_1}{t} & 0 & -1 \\ 1 & 0 & -k & k-1 \\ 1 & -\frac{m_1}{t} & 0 & -1 \\ 1 & -m_1 & k(d-1) & k-1 \end{bmatrix}$$

Dual Eigenvalues of our 4-Class Scheme

Row sums must be zero (except row zero):

$$Q = \begin{bmatrix} 1 & m_1 & k(d-1) & kd - m_1 & k-1 \\ 1 & \frac{m_1}{t} & 0 & -\frac{m_1}{t} & -1 \\ 1 & 0 & -k & 0 & k-1 \\ 1 & -\frac{m_1}{t} & 0 & \frac{m_1}{t} & -1 \\ 1 & -m_1 & k(d-1) & m_1 - kd & k-1 \end{bmatrix}$$

Three-Term Recurrence

For some number c_2^* , we have

$$Q_{i,1}^2 = b_0^* Q_{i,0} + c_2^* Q_{i,2}$$

$$Q_{i,1}^2 = m_1 + c_2^* Q_{i,2}$$

$$m_1^2 = m_1 + c_2^* k(d-1)$$

$$\frac{m_1^2}{t^2} = m_1$$

$$0 = m_1 - kc_2^*$$

Three-Term Recurrence

For some number c_2^* , we have

$$\begin{aligned}m_1(m_1 - 1) &= c_2^* k(d - 1) \\ t &= \sqrt{m_1} \\ c_2^* &= m_1/k\end{aligned}$$

This gives $m_1 = d$ and $t = \sqrt{d}$.

Dual Eigenvalues of our 4-Class Scheme

So our second eigenmatrix becomes

$$Q = \begin{bmatrix} 1 & d & k(d-1) & d(k-1) & k-1 \\ 1 & \sqrt{d} & 0 & -\sqrt{d} & -1 \\ 1 & 0 & -k & 0 & k-1 \\ 1 & -\sqrt{d} & 0 & \sqrt{d} & -1 \\ 1 & -d & k(d-1) & -d(k-1) & k-1 \end{bmatrix}$$

This Gives Mutually Unbiased Bases!

Looking at the first column of Q , we have

- ▶ $2kd$ vectors in \mathbb{R}^d (scale to unit vectors)
- ▶ partitioned into k classes of size $2d$
- ▶ vectors in same class either parallel or orthogonal
- ▶ vectors in different classes have inner product $\pm 1/\sqrt{d}$

Implications

Krein conditions are vacuous, but other conditions for schemes may be useful.

Duality: symmetric (m, μ) -nets give diameter 4 distance-regular graphs which are both bipartite and antipodal. If any of these admits a transitive abelian group of automorphisms, then the characters of a related group are guaranteed to give mutually unbiased bases.

Thank You!

Association Scheme: Usual Definition

A (symmetric) *association scheme* consists of a set $\{A_0, \dots, A_d\}$ of symmetric 01-matrices with

- ▶ $A_0 = I$
- ▶ $\sum_i A_i = J$ (the all-ones matrix)
- ▶ $A_i A_j$ is a linear combination of A_0, \dots, A_d

Rows and columns are indexed by base set X of size v .

Bose-Mesner algebra

$$\mathcal{A} = \text{span}\{A_0, \dots, A_d\}$$

is a commutative semisimple matrix algebra containing I .
It is also closed under entrywise multiplication \circ (also called “Schur mult.” or “Hadamard mult.”) and contains the identity J for this multiplication.

$$\mathcal{A} = \text{span}\{E_0, \dots, E_d\}$$

(basis of minimal idempotents)

Orthogonality relations

$$A_i = \sum_{j=0}^d P_{ji} E_j \quad E_j = \frac{1}{v} \sum_{i=0}^d Q_{ij} A_i$$

The change-of-basis matrices P and Q are called the “first and second eigenmatrices” of the scheme. A scaled version of P is called the “character table”:

$$PQ = vI$$

$$MP = Q^T K$$

where M is a diagonal matrix of multiplicities $m_j = \text{rank } E_j$ and K is a diagonal matrix of valencies $v_i = \text{rowsum } A_i$.

Metric and Cometric Schemes

The scheme is *metric* (or *P-polynomial*) if there is an ordering of the A_i for which

- ▶ $p_{ij}^k = 0$ whenever $k > i + j$
- ▶ $p_{ij}^{i+j} > 0$ whenever $i + j \leq d$

The scheme is *cometric* (or *Q-polynomial*) if there is an ordering of the E_j for which

- ▶ $q_{ij}^k = 0$ whenever $k > i + j$
- ▶ $q_{ij}^{i+j} > 0$ whenever $i + j \leq d$

Imprimitivity

An association scheme is *imprimitive* if there is a subset $A_{i_0}, A_{i_1}, \dots, A_{i_e}$ of the associate matrices A_i satisfying $\sum_h A_{i_h} = I_w \otimes J_r$ for some $1 < w, r < v$.

Any imprimitive distance-regular graph is either bipartite or antipodal or both.

Imprimitivity

Theorem (Suzuki, 1998)

Any imprimitive cometric association scheme is either Q -bipartite or Q -antipodal or both, with possible exceptions if the number of classes is four or six.

Theorem (Cerzo and Suzuki, 2006)

The exception with $d = 4$ does not occur.

Q-bipartite Schemes

If we view a cometric association scheme as the polytope which is the convex hull of the columns of E_1 , then the scheme is

Q-bipartite

if and only if

this polytope is “antipodal”: $x \in X \Rightarrow -x \in X$

So these correspond to very symmetric sets of lines through the origin in \mathbb{R}^m .

Question: What restriction on a system of lines ensures that it represents a Q-bipartite cometric scheme?

Q-antipodal Schemes

Again, view a cometric association scheme as the polytope which is the convex hull of the columns of E_1 .

The scheme is Q-antipodal
 if and only if

Natural ordering of relations:

$$Q_{01} = m_1 > Q_{11} > \cdots > Q_{d1}$$

Then

$$Q_{0d} = Q_{2d} = \cdots = m_d \text{ and } Q_{1d} = Q_{3d} = \cdots = -1$$

and

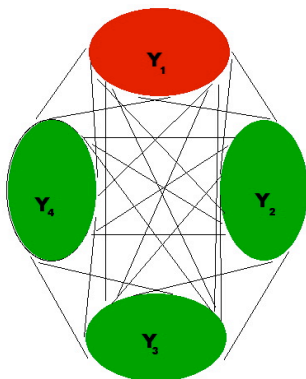
$$p_{ij}^k = 0 \text{ unless } i + j + k \text{ is even or } i, j, k \text{ all odd.}$$

Dismantling

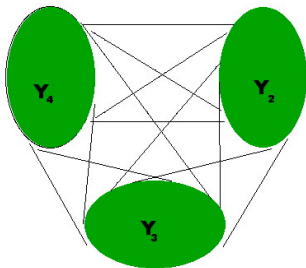
Theorem (Muzychuk, Williford, WJM (2007))

*Every Q -antipodal scheme is dismantlable:
the subscheme induced on any non-trivial collection of w'
 Q -antipodal classes is cometric for $w' \geq 1$ and Q -antipodal with d
classes for $w' > 1$.*

Dismantlability



Dismantlability



Thank You!