Mutually Unbiased Bases and Covers of Complete Bipartite Graphs

Chris Godsil and Aidan Roy

November 19, 2004

with thanks

to Martin Rötteler for his help

Outline

Outline

Flat Matrices

Definition

A complex matrix M is flat if all its entries have the same absolute value.

Unbiased Bases

Definition

Two orthogonal bases in $\mathbb{C}^d$ are unbiased if the corresponding change of basis matrix is flat.

Unbiasedness is a Symmetric Relation

- If M is flat, so are $\overline{M}$, M^T and M^*.

Unbiasedness is a Symmetric Relation

- If M is flat, so are $\overline{M}$, M^T and M^*.
- The change of basis matrix between orthogonal bases is unitary.

Unbiased Unitary Matrices

An ordered orthogonal basis in $\mathbb{C}^d$ corresponds to a $d \times d$ unitary matrix. If U and V are unitary $d \times d$ matrices, the corresponding orthogonal bases are unbiased if and only if U^*V is flat (and unitary).

Unbiased Unitary Matrices

An ordered orthogonal basis in $\mathbb{C}^d$ corresponds to a $d \times d$ unitary matrix. If U and V are unitary $d \times d$ matrices, the corresponding orthogonal bases are unbiased if and only if U^*V is flat (and unitary).

In which case, the columns of I and U^*V form an unbiased pair of bases.

Entries of Flat Unitary Matrices

- If M is flat and $d \times d$ and $|M_{i,j}| = \alpha$ for all i and j, then $(MM^*)_{i,i} = d\alpha^2$ for all i.

Entries of Flat Unitary Matrices

- If M is flat and $d \times d$ and $|M_{i,j}| = \alpha$ for all i and j, then $(MM^*)_{i,i} = d\alpha^2$ for all i.
- If M is unitary, $MM^* = I$, and therefore

Entries of Flat Unitary Matrices

- If M is flat and $d \times d$ and $|M_{i,j}| = \alpha$ for all i and j, then $(MM^*)_{i,i} = d\alpha^2$ for all i.
- If M is unitary, $MM^* = I$, and therefore
- If M is flat and unitary, $|M_{i,j}| = d^{-1/2}$.

Hadamard Matrices

Definition

A Hadamard matrix H is a $d \times d$ matrix with entries ± 1 such that $H^T H = dI$.

Hadamard Matrices

Definition

A Hadamard matrix H is a $d \times d$ matrix with entries ± 1 such that $H^T H = dI$.

Example

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Hadamard Bases

Example

If H is Hadamard with order $d \times d$, then

$$d^{-1/2}H$$

is flat and unitary and the orthogonal bases given by I_d and $d^{-1/2}H$ are unbiased.

Example: Vandermonde

Example

Let θ be a primitive d-th root of unity, and let V be the $d \times d$ matrix given by

$$V_{i,j} := \theta^{(i-1)(j-1)}.$$

Then $d^{-1/2}V$ is flat and unitary.

Outline

A Definition

Definition

A set of orthogonal bases of $\mathbb{C}^d$ is mutually unbiased if each pair of bases in it is unbiased.

Why?

Why do we want mutually unbiased sets of bases?

Applications

- Quantum key exchange.
- Determining the state of a quantum system.
- Constructing discrete Wigner functions.

Upper Bounds

The maximum size of a set of mutually unbiased bases is at most:

- $d + 1$ in $\mathbb{C}^d$,

and

- $\frac{1}{2}d + 1$ in $\mathbb{R}^d$.

The Main Problem

For which integers d is it possible to construct a set of $d + 1$ mutually unbiased bases in $\mathbb{C}^d$?

Example

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ i & -i\end{pmatrix}$$

Outline

Hermitian Matrices

A set of m mutually unbiased bases in $\mathbb{C}^d$ gives a set of md unit vectors

$$x_1, \ldots, x_{md}.$$

If $X_i := x_i x_i^*$, we then have md matrices

$$X_1, \ldots, X_{md}$$

each lying in $\mathcal{H}(d)$, the real vector space of Hermitian $d \times d$ matrices.

A Gram Matrix

Define an inner product on the space of Hermitian matrices by

$$\langle H|K\rangle := \operatorname{tr}(HK).$$

Let G be the $md \times md$ matrix with

$$G_{i,j} = \langle X_i|X_j\rangle.$$

The Complete Multipartite Graph

Then

$$G = I + d^{-1}A,$$

where A is the adjacency matrix of the complete multipartite graph, with m parts of size d. We know that

$$\mathrm{rk}(G) = md - m + 1$$

and therefore—

The Complete Multipartite Graph, ctd.

$$\begin{aligned} md - m + 1 &= \mathrm{rk}(G) \\ &= \dim(\mathrm{span}(\{X_i\}_{i=1}^{md})) \\ &\leq \dim(\mathcal{H}(d)) \\ &= d^2. \end{aligned}$$

The Bound

Theorem

The maximum size of a set of mutually unbiased bases in $\mathbb{C}^d$ *is* $d+1$.

Is the Bound Good?

Sets of $d+1$ mutually unbiased bases in $\mathbb{C}^d$ are known to exist if d is a prime power :-)

Is the Bound Good?

Sets of $d+1$ mutually unbiased bases in $\mathbb{C}^d$ are known to exist if d is a prime power :-)

If $d = 2e$, where e is odd, a product-type construction due to Klappenecker and Rötteler yields triples, but no larger sets are known :-(

Links

Or we can construct triples from spin models.

Links

Or we can construct triples from spin models. But that is. . . .

circus?

…another kettle of fish:

Real Pairs

- If a pair of mutually unbiased bases exists in $\mathbb{R}^d$, then $d = 2$ or $4 \mid d$ and a Hadamard matrix of order $d \times d$ exists.

Real Mutually Unbiased Triples

Suppose we have a triple of mutually unbiased bases in $\mathbb{R}^d$. Then there must be Hadamard matrices H and K of order $d \times d$, so that our mutually unbiased bases are the columns of

$$I, \quad \frac{1}{\sqrt{d}}H, \quad \frac{1}{\sqrt{d}}K,$$

and the product

$$\frac{1}{d}H^T K$$

must be flat and unitary.

Real Triples are Scarce. . .

Consequently

- each entry of $H^T K$ must be equal to $\pm\sqrt{d}$, and
- since H and K are integer matrices, d is the square of an integer.

…But Do Exist

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{pmatrix}, \quad K = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Outline

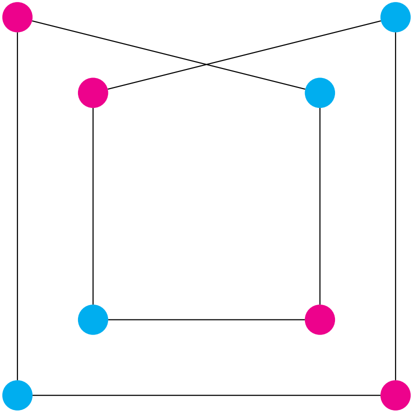
Covers of Complete Bipartite Graphs

Let X be a graph with d vertices. We construct a cover of X with *index* r as follows.
The vertex set of the cover is

$$V(X) \times \{1, \dots, d\}.$$

So we have d *fibres* of size, each fibre corresponds to a vertex of X.
If two fibres of the correspond to adjacent vertices in G we join the vertices in the first fibre to the vertices in the second by a matching with size r.

An Example



ctd.

- If $X = K_{d,d}$, then a cover of X with index r is a bipartite graph on $rd + rd$ vertices, regular of degree d.

Outline

Distance-Regular Covers

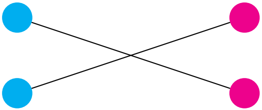
We want more! We want covers Y of $K_{d,d}$ such that

- Y has diameter four.
- Two distinct vertices in the same fibre are at distance four, and two vertices in different fibres are at distance less than four.
- There is a constant, traditionally c_2, such that if u and v are at distance two in Y, then they have exactly c_2 common neighbours.
- If the above conditions hold, then $rc_2 = d$.

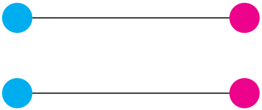
Hadamard

2-fold antipodal distance-regular covers of $K_{d,d}$ correspond to Hadamard matrices.

$H_{i,j} = -1$:



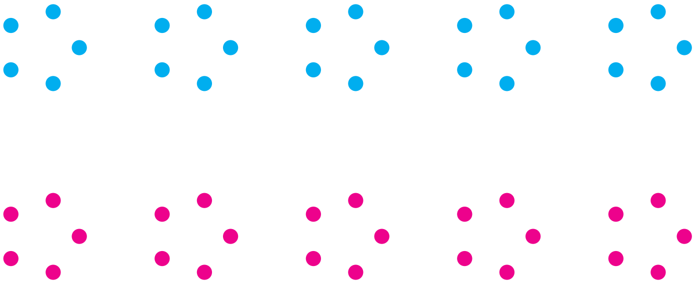
$H_{i,j} = 1$:



Affine Planes

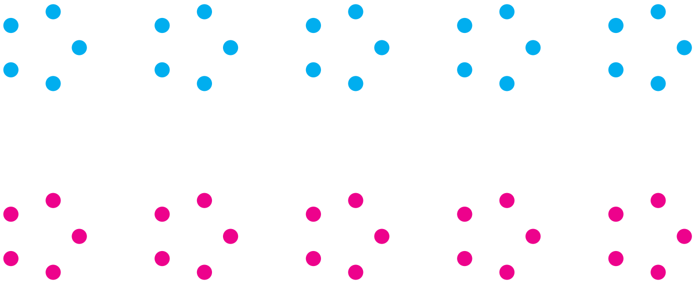
d-fold covers of $K_{d,d}$ correspond to affine planes with one parallel class of lines deleted.

AG(2,5)



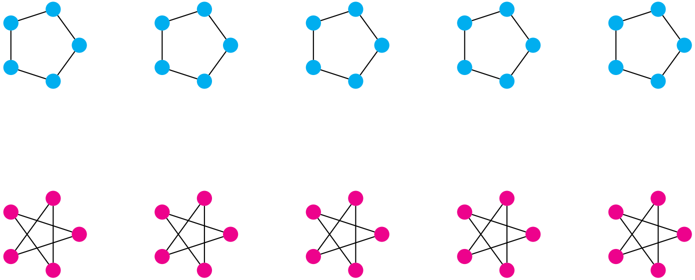
Adjacency: $(x, y) \sim [a, y - ax]$.

Hoffman-Singleton, Robertson



Adjacency: $(x, y) \sim [a, y - ax]$.

Hoffman-Singleton, Robertson



Adjacency: $(x, y) \sim [a, y - ax]$.

Abelian Groups

If we have an r-fold cover of $K_{d,d}$ and an abelian group of automorphisms acting transitively on each colour class, the eigenvectors of the cover give rise to a set of r mutually unbiased bases in $\mathbb{C}^d$.

Semifields

Each commutative semifield of order q gives a q-fold cover of $K_{q,q}$ with an abelian group acting as required.

Semifields

Each commutative semifield of order q gives a q-fold cover of $K_{q,q}$ with an abelian group acting as required.

Q: wth is a semifield?

Semifields

Each commutative semifield of order q gives a q-fold cover of $K_{q,q}$ with an abelian group acting as required.

Q: wth is a semifield?
A: drop associativity

History

- The first examples of maximal sets of mutually unbiased bases were found by Ivanovic (1981), in the case where d is prime.

History

- The first examples of maximal sets of mutually unbiased bases were found by Ivanovic (1981), in the case where d is prime.
- Wootters and Fields (1989) found constructions for all prime-power values of d.

History

- The first examples of maximal sets of mutually unbiased bases were found by Ivanovic (1981), in the case where d is prime.
- Wootters and Fields (1989) found constructions for all prime-power values of d.
- Calderbank, Cameron, Kantor and Seidel (1997) show how to construct maximal sets in prime-power dimensions, using symplectic spreads. This construction yields the same examples as our semifield construction. :-(

Future

- Can we use covers to find sets of four mutually unbiased bases in dimension $2e$, where e is odd?

Future

- Can we use covers to find sets of four mutually unbiased bases in dimension $2e$, where e is odd?
- We have observed connections with the theory of spin models, introduced by Vaughan Jones in his work on link invariants. These provide a generalization of our construction, which we have not yet investigated in any depth.

Future

- Can we use covers to find sets of four mutually unbiased bases in dimension $2e$, where e is odd?
- We have observed connections with the theory of spin models, introduced by Vaughan Jones in his work on link invariants. These provide a generalization of our construction, which we have not yet investigated in any depth.
- A mutually unbiased set of bases determines a set of lines in $\mathbb{C}^d$. If we replace the distance-regular covers of complete graphs by other classes of distance-regular graphs, we can use our technology to construct other interesting sets of complex lines. This needs further investigation.