Quantum Geometry: MUB's and SIC-POVM's

Chris Godsil

Perth, December 2009

Outline

Some Physics

- One thing to remember is that “the axioms of quantum physics are not so strict as in mathematics”. (Dénes Peres, Quantum Information Theory, p. 22)
- Hydrogen is a colorless odorless gas which, given sufficient time, turns into human beings. (Henry Hiebert)

Outline

Lines and Things

A simple system in quantum physics is described by a complex vector space, and the states of the system correspond to the lines in this space. (So a state is a point in a complex projective space.)

Lines

Our general problem is to find large sets of lines in $\mathbb{C}^d$, subject to restrictions on the "angles" between the lines.

If we specify two lines by giving unit vectors x and y that span them, then the angle between them is given by

$$\langle x|y\rangle\langle y|x\rangle.$$

Lines

Our general problem is to find large sets of lines in $\mathbb{C}^d$, subject to restrictions on the "angles" between the lines.

If we specify two lines by giving unit vectors x and y that span them, then the angle between them is given by

$$\langle x|y\rangle\langle y|x\rangle.$$

(Well, strictly the angle should be $\arccos(\sqrt{\langle x|y\rangle\langle y|x\rangle})$, but let's not get lost in notation.)

Too Many Unit Vectors

Each 1-dimensional subspace of $\mathbb{C}^d$ contains infinitely many unit vectors; this gives too many choices. But if x and y are unit vectors that span the same line, then the matrices:

$$xx^*, \quad yy^*$$

are equal—because $y = cx$ where $|c| = 1$ and so $cc^* = 1$ and

$$yy^* = (cx)(cx)^* = cc^*xx^* = xx^*.$$

(The $d \times d$ matrix xx^* represents orthogonal projection onto the line spanned by x; its form does not depend on which basis we choose for the line.)

Outline

Equiangular Lines

A set of lines in $\mathbb{C}^d$ is equiangular if the angle between any two distinct lines is the same.

What is the maximum size of a set of equiangular lines in $\mathbb{C}^d$?

An Unusual Way to Count

We will get our bound as follows:

1. Assign a vector in a space of dimension m to each line.

An Unusual Way to Count

We will get our bound as follows:

1. Assign a vector in a space of dimension m to each line.
2. Show that the vectors we get are linearly independent.

An Unusual Way to Count

We will get our bound as follows:

1. Assign a vector in a space of dimension m to each line.
2. Show that the vectors we get are linearly independent.
3. Conclude that we have at most m lines.

Assigning Vectors

We have already seen that a line is determined by a projection, which we now view as a vector in the space of $d \times d$ complex matrices.
Since

$$(xx^*)^* = xx^*,$$

our projections are Hermitian matrices. The set of $d \times d$ Hermitian matrices is a real vector space with dimension d^2.

Independence

Assume that $\mathrm{tr}(X_i) = 1$ and $\mathrm{tr}(X_i X_j) = a^2 < 1$. To prove that the X_i's are linearly independent, we show that there is a dual basis. Define

$$Y_i := X_i - a^2 I$$

and observe that

$$\mathrm{tr}(Y_i X_i) = \begin{cases} 1 - a^2, & i = j; \\ 0, & i \neq j. \end{cases}$$

Independence ctd.

If

$$0 = \sum_r c_r X_r$$

then

$$0 = \sum_r c_r \operatorname{tr}(Y_i X_r) = c_i(1 - a^2)$$

It follows that $c_i = 0$ for all i. Therefore $X_1, \ldots, X_n$ are linearly independent elements of the real vector space of Hermitian matrices, which has dimension d^2.

Theorem

A set of equiangular lines in $\mathbb{C}^d$ has size at most d^2.

The Angle

If $\mathcal{L}$ is a set of n equiangular lines in $\mathbb{C}^d$ and $n = d^2$, then I is a linear combination of the associated projections X_r. So

$$I = \sum_r c_r X_r$$

and consequently

$$1 = \operatorname{tr}(Y_i I) = \sum_r c_r \operatorname{tr}(Y_i X_r) = (1 - a^2) c_r.$$

This implies that $c_1 = \cdots = c_n$; as $\operatorname{tr}(I) = d$ it follows easily that $c_r = d^{-1}$ and $a^2 = (d+1)^{-1}$.

Fiducial Vectors

All known constructions of sets of d^2 equiangular lines in $\mathbb{C}^d$ start with a unit vector f and a group $\mathcal{G}$ of matrices. The group is fixed and the idea is to choose f so that the distinct vectors

$$Mf, \quad M \in \mathcal{G}$$

span a set of equiangular lines. (Physicists call f a fiducial vector.)

The Group

The group usually used is defined as follows. Let $e_1, \ldots, e_d$ be the standard basis for $\mathbb{C}^d$.

- Let P be the permutation matrix that maps e_r to e_{r+1} (with subscripts computed modulo d).

The Group

The group usually used is defined as follows. Let $e_1, \ldots, e_d$ be the standard basis for $\mathbb{C}^d$.

- Let P be the permutation matrix that maps e_r to e_{r+1} (with subscripts computed modulo d).
- Let $\theta = \exp(2\pi i/d)$ and assume D is the diagonal matrix such that $De_r = \theta^{r-1} e_r$.

The Group

The group usually used is defined as follows. Let $e_1, \ldots, e_d$ be the standard basis for $\mathbb{C}^d$.

- Let P be the permutation matrix that maps e_r to e_{r+1} (with subscripts computed modulo d).
- Let $\theta = \exp(2\pi i/d)$ and assume D is the diagonal matrix such that $De_r = \theta^{r-1} e_r$.

The Group

The group usually used is defined as follows. Let $e_1, \ldots, e_d$ be the standard basis for $\mathbb{C}^d$.

- Let P be the permutation matrix that maps e_r to e_{r+1} (with subscripts computed modulo d).
- Let $\theta = \exp(2\pi i/d)$ and assume D is the diagonal matrix such that $De_r = \theta^{r-1} e_r$.

Then P and D generate a (non-abelian) group of order d^3, where each element can be written as

$$\theta^r P^s D^t, \qquad 0 \leq r, s, t < d.$$

The Construction

The trick is now to choose f so that

$$|\langle f|Mf\rangle|^2 = \frac{1}{d+1}$$

for each element M in our group.

The Construction

The trick is now to choose f so that

$$|\langle f|Mf\rangle|^2 = \frac{1}{d+1}$$

for each element M in our group.

How do we make such a choice?

The Construction

The trick is now to choose f so that

$$|\langle f|Mf\rangle|^2 = \frac{1}{d+1}$$

for each element M in our group.

How do we make such a choice?

Very carefully.

Part of an Example

Renes et al give a fiducial vector in $\mathbb{C}^4$ in terms of the numbers

1. $$\frac{1 - 1/\sqrt{5}}{2\sqrt{2 - \sqrt{2}}}$$

Part of an Example

Renes et al give a fiducial vector in $\mathbb{C}^4$ in terms of the numbers

1. $$\frac{1 - 1/\sqrt{5}}{2\sqrt{2 - \sqrt{2}}}$$
2. $$\frac{1}{2}\sqrt{1 + 1/\sqrt{5} \pm \sqrt{1/5 + 1/\sqrt{5}}}$$

Part of an Example

Renes et al give a fiducial vector in $\mathbb{C}^4$ in terms of the numbers

1. $$\frac{1-1/\sqrt{5}}{2\sqrt{2-\sqrt{2}}}$$

2. $$\frac{1}{2}\sqrt{1+1/\sqrt{5}\pm\sqrt{1/5+1/\sqrt{5}}}$$

3. $$\arccos\frac{2}{\sqrt{5+\sqrt{5}}},\quad \arcsin\frac{2}{\sqrt{5}}$$

Data

Equiangular line sets in $\mathbb{C}^d$ of size d^2 have been constructed for d in $\{2, \ldots, 15, 19, 24, 35, 48\}$.

Sets that are equiangular to machine precision have constructed up to dimension 66.

If d is a prime power, we can construct sets of size $d^2 - d + 1$.

Outline

Flat Matrices

Definition

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

Flat Matrices

Definition

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

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

Unbiased Bases

An ordered orthogonal basis in $\mathbb{C}^d$ corresponds to a $d \times d$ unitary matrix.

Definition

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.
Note that $U^* V$ is flat if and only if $V^* U$ is, so unbiasedness is a symmetric relation.

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

Theorem

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

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

Acknowledgement

From now on, this is joint work with Aidan Roy.

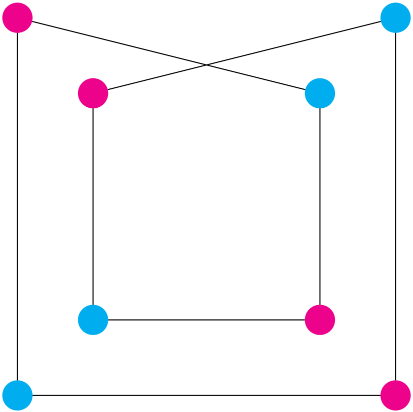
Covers of Complete Bipartite Graphs

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

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

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

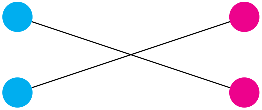
We want more! We want covers Y of $K_{d,d}$ such that

- 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 $rc_2 = d$.

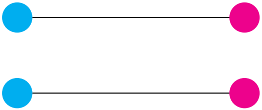
Hadamard

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

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



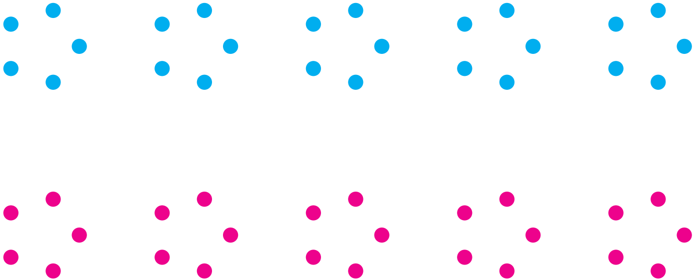
$H_{i,j} = 1$:



Affine Planes

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

AG(2,5)



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

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 correspond to the characters of the abelian group.

The restriction of the rd characters to the neighborhood of a fixed vertex are vectors in $\mathbb{C}^d$, and these form 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 from the axioms for a field.

History

- The first examples of sets of $d+1$ 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) showed how to construct maximal sets in prime-power dimensions, using symplectic spreads. This construction yields the same examples as our semifield construction.

A Problem

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