Title: Complex Lines

Date: Apr 28, 2008 09:50 AM

URL: http://pirsa.org/08040071

Abstract: Certain structures arising in Physics (mub\'s and sic-povm\'s) can be viewed as sets of lines in complex space that are as large as possible, given some simple constraints on the angles between distinct lines. The analogous problems in real space have long been of interest in Combinatorics, because of their relation to classical combinatorial structures. In the complex case there seems no reason for any combinatorial connection to exist. will discuss some of the history of the real problems, and describe some recent work that relates the complex problems to some very interesting classes of graphs.

Complex Lines

Chris Godsil

April 2008

OUTLINE

1. EQUIANGULAR LINES
   - Geometry
   - Bounds
   - Constructions
2. MUB'S
   - Introduction
   - Graphs
3. SPIN MODELS
   - Type-II Matrices
   - Spin Models and MUB's

Outline

Inner Products

We use $\langle x|y\rangle$ to denote the usual inner product. So if we work in $\mathbb{C}^d$, then

$$\langle x|y\rangle = x^* y = \bar{x}^T y$$

while in $\mathbb{R}^d$,

$$\langle x|y\rangle = x^T y.$$

ANGLES

It seems natural to represent a line by a unit vector that spans it. We define the angle between lines spanned by unit vectors x and y to be

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

(We should perhaps use $\arccos(|\langle x|y\rangle|)$, but it will not be worth the effort.)

DEFINITION

A set of lines in $\mathbb{C}^d$ (or $\mathbb{R}^d$) is equiangular if the angle between and two distinct lines is the same.

PROJECTIONS

Although it may be natural to represent a line by a unit vector that spans it, there is an alternative that is often more convenient. If a line ℓ is spanned by a unit vector x then the matrix

$$P = xx^*$$

is a projection ($P^2 = P$ and $P^* = P$); in fact P represents orthogonal projection onto ℓ.

Another Inner Product

The space of Hermitian operators on $\mathbb{C}^d$ is a vector space over $\mathbb{R}^d$ with an inner product given by

$$\langle P|Q\rangle := \operatorname{tr}(PQ)$$

If $P = xx^*$ and $Q = yy^*$, then

$$PQ = xx^* yy^* = (x^* y)xy^*$$

and hence

$$\operatorname{tr}(PQ) = (x^* y) \operatorname{tr}(xy^*) = (x^* y)(y * x) = |\langle x|y\rangle|^2.$$

Summary

If P and Q are the orthogonal projections onto lines in $\mathbb{F}^d$, then the angle between the two lines is determined by $\mathrm{tr}(PQ)$. These projections are elements of the vector space of Hermitian operators on $\mathbb{F}^n$. ($\mathbb{F}$ is $\mathbb{C}$ or $\mathbb{R}$.)

OUTLINE

1. EQUIANGULAR LINES
   - Geometry
   - Bounds
   - Constructions
2. MUB'S
   - Introduction
   - Graphs
3. SPIN MODELS
   - Type-II Matrices
   - Spin Models and MUB's

LINEARLY INDEPENDENT OPERATORS

Suppose we have a set of m equiangular lines in $\mathbb{C}^d$, given by projections $P_1, \ldots, P_m$.

LEMMA

The operators $P_1, \ldots, P_m$ are linearly independent.

THE PROOF

PROOF.

There is a non-negative real number γ such that $\langle P_i | P_j \rangle = \gamma$. Suppose there are scalars $c_1, \ldots, c_m$ such that

$$c_1 P_1 + \cdots + c_m P_m = 0.$$

Then multiply both sides of this by P_1 and take the trace to get

$$0 = c_1 + \gamma(c_2 + \cdots + c_m) = (1 - \gamma)c_1 + \gamma \sum_i c_i.$$

This shows that c_1 is determined by γ and $\sum c_i$, and it follows that $c_1 = \cdots = c_m$. We conclude that all the c_i's are zero. $\square$

THE ABSOLUTE BOUND

THEOREM

The size of a set of equiangular lines in $\mathbb{C}^d$ is at most d^2. The size of a set of equiangular lines in $\mathbb{R}^d$ is at most $\binom{d+1}{2}$.

PROOF.

The size of a set of equiangular lines is bounded by the size of a basis in the space spanned by the projections corresponding to the lines.
The Hermitian operators on $\mathbb{C}^d$ form a vector space of dimension d^2.
Real symmetric operators on $\mathbb{R}^d$ form a vector space of dimension $\binom{d+1}{2}$. □

SIC-POVM's

DEFINITION

A set of d^2 equiangular lines in $\mathbb{C}^d$ is known, to physicists, as a SIC-POVM.

The paper at arXiv:quant-ph/0310075 by Renes, Blume-Kohout, Scott and Caves is a convenient starting point to the physical literature.
The first work was carried out in 1975 by Delsarte, Goethals and Seidel, who derived the basic bounds and constructed examples in $\mathbb{C}^2$ and $\mathbb{C}^3$. (See Seidel's "Selected Works".)

EQUALITY

If equality holds in the absolute bound, then I lies in the span of the line projections P_i. Hence there are scalars c_i such that

$$\sum_i c_i P_i = I.$$

If we multiply both sides by P_j and then take traces, we get

$$c_j(1-\gamma) + \gamma \sum_i c_i = 1,$$

from which it follows that the c_i's are all equal, and hence that all are equal to d/m. Consequently

$$m = \frac{d - d\gamma}{1 - d\gamma}.$$

In the complex case we deduce that $\gamma = \frac{1}{d+1}$; in the real case we find that $\gamma = \frac{1}{d+2}$.

OUTLINE

1. EQUIANGULAR LINES
   - Geometry
   - Bounds
   - Constructions
2. MUB'S
   - Introduction
   - Graphs
3. SPIN MODELS
   - Type-II Matrices
   - Spin Models and MUB's

Equality

If equality holds in the absolute bound, then I lies in the span of the line projections P_i. Hence there are scalars c_i such that

$$\sum_i c_i P_i = I.$$

If we multiply both sides by P_j and then take traces, we get

$$c_j(1-\gamma) + \gamma \sum_i c_i = 1,$$

from which it follows that the c_i's are all equal, and hence that all are equal to d/m. Consequently

$$m = \frac{d - d\gamma}{1 - d\gamma}.$$

In the complex case we deduce that $\gamma = \frac{1}{d+1}$; in the real case we find that $\gamma = \frac{1}{d+2}$.

OUTLINE

1. EQUIANGULAR LINES
   - Geometry
   - Bounds
   - Constructions
2. MUB'S
   - Introduction
   - Graphs
3. SPIN MODELS
   - Type-II Matrices
   - Spin Models and MUB's

Complex Constructions

Examples of sets of d^2 equiangular complex lines in $\mathbb{C}^d$ are known for the following values of d:

$$2, 3, 4, 5, 6, 7, 8, 19.$$

In all cases where these bounds can be realised, examples can be constructed using generalised Pauli matrices.

GENERALISED PAULI MATRICES

Let $e_0, \dots, e_{d-1}$ denote the standard basis for $\mathbb{C}^d$, where the indices are taken modulo d, and let ω be a primitive d-th root of unity. For $j = 0, \dots, d-1$, define operators $X(i)$ and $Y(j)$ on $\mathbb{C}^d$ by

$$X(j) : e_k \mapsto e_{k+j}, \quad Y(j) : e_k \mapsto \omega^{jk} e_j.$$

The group

$$\Gamma = \langle X(j)Y(k) : j,k \in \mathbb{Z}_d \rangle$$

has order d^3. Its centre has order d and is generated by ωI; the quotient group modulo the centre is isomorphic to $\mathbb{Z}_d^2$.

FIDUCIAL VECTORS

DEFINITION

If v is a non-zero vector in $\mathbb{C}^d$, then the vectors

$$\gamma v, \quad \gamma \in \Gamma$$

span at most d^2 distinct complex lines. If we obtain exactly d^2 lines and these lines are equiangular, we say that v is a fiducial vector.

All known examples of maximal sets of equiangular lines have been found by making a suitable choice of fiducial vector.

GENERALISED PAULI MATRICES

Let $e_0, \dots, e_{d-1}$ denote the standard basis for $\mathbb{C}^d$, where the indices are taken modulo d, and let ω be a primitive d-th root of unity. For $j = 0, \dots, d-1$, define operators $X(i)$ and $Y(j)$ on $\mathbb{C}^d$ by

$$X(j) : e_k \mapsto e_{k+j}, \quad Y(j) : e_k \mapsto \omega^{jk} e_j.$$

The group

$$\Gamma = \langle X(j)Y(k) : j, k \in \mathbb{Z}_d \rangle$$

has order d^3. Its centre has order d and is generated by ωI; the quotient group modulo the centre is isomorphic to $\mathbb{Z}_d^2$.

APPROXIMATELY FIDUCIAL VECTORS

Renes et al have found vectors in $\mathbb{C}^d$ for $5 \leq d \leq 45$ that are fiducial to machine precision. (What this means is not clear.)

The Real Case

- An equiangular set of lines in $\mathbb{R}^d$ has size at most $\binom{d+1}{2}$. Examples of maximal size are known when $d \in \{2, 3, 7, 23\}$. It seems unlikely that other examples exist (but we do not really have a clue).
- These examples are not constructed using anything like the fiducial-vector method.

APPROXIMATELY FIDUCIAL VECTORS

Renes et al have found vectors in $\mathbb{C}^d$ for $5 \leq d \leq 45$ that are fiducial to machine precision. (What this means is not clear.)

Fiducial Vectors

Definition

If v is a non-zero vector in $\mathbb{C}^d$, then the vectors

$$\gamma v, \quad \gamma \in \Gamma$$

span at most d^2 distinct complex lines. If we obtain exactly d^2 lines and these lines are equiangular, we say that v is a fiducial vector.

All known examples of maximal sets of equiangular lines have been found by making a suitable choice of fiducial vector.

APPROXIMATELY FIDUCIAL VECTORS

Renes et al have found vectors in $\mathbb{C}^d$ for $5 \leq d \leq 45$ that are fiducial to machine precision. (What this means is not clear.)

FIDUCIAL VECTORS

DEFINITION

If v is a non-zero vector in $\mathbb{C}^d$, then the vectors

$$\gamma v, \quad \gamma \in \Gamma$$

span at most d^2 distinct complex lines. If we obtain exactly d^2 lines and these lines are equiangular, we say that v is a fiducial vector.

All known examples of maximal sets of equiangular lines have been found by making a suitable choice of fiducial vector.

APPROXIMATELY FIDUCIAL VECTORS

Renes et al have found vectors in $\mathbb{C}^d$ for $5 \leq d \leq 45$ that are fiducial to machine precision. (What this means is not clear.)

The Real Case

- An equiangular set of lines in $\mathbb{R}^d$ has size at most $\binom{d+1}{2}$. Examples of maximal size are known when $d \in \{2, 3, 7, 23\}$. It seems unlikely that other examples exist (but we do not really have a clue).

THE REAL CASE

- An equiangular set of lines in $\mathbb{R}^d$ has size at most $\binom{d+1}{2}$. Examples of maximal size are known when $d \in \{2, 3, 7, 23\}$. It seems unlikely that other examples exist (but we do not really have a clue).
- These examples are not constructed using anything like the fiducial-vector method.

OUTLINE

MUTUALLY UNBIASED BASES

DEFINITION

Two orthonormal bases $x_1, \ldots, x_d$ and $y_1, \ldots, y_d$ in $\mathbb{C}^d$ are unbiased if the angles

$$|\langle x_i | y_j \rangle|$$

are the same for all choices of i and j. A set of orthonormal bases is mutually unbiased if each pair of distinct bases is unbiased.

If two bases are unbiased, the angle must be $\frac{1}{\sqrt{d}}$.

AN EXAMPLE

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

MATRICES

We can represent orthonormal bases in $\mathbb{C}^d$ by $d \times d$ matrices.

DEFINITION

A matrix over $\mathbb{C}$ is flat if all its entries have the same absolute value.

If U and V are unitary matrices, then the corresponding bases are unbiased if and only if U^*V is flat. (And if U^*V is flat, then the basis formed by its columns is unbiased relative to the standard basis.)

HADAMARD MATRICES

DEFINITION

A $d \times d$ matrix H is a Hadamard matrix if each entry is ± 1 and

$$H^T H = dI$$

If $d > 2$ and a Hadamard matrix exists, then $4|d$. If H is Hadamard then

$$\frac{1}{\sqrt{d}} H$$

is flat and unitary.
(Physicists refer to flat unitary matrices as generalised Hadamard matrices.)

BOUNDS

THEOREM

A set of mutually unbiased bases in $\mathbb{C}^d$ *has size at most* $d+1$.

The Problem

For which values of d does there exist a mutually unbiased set of orthogonal bases of size $d+1$?

Lower Bounds

It follows from work of Klappenecker and Rötteler that if $d \geq 2$, then there is at least a triple of mutually unbiased bases. (If a triple exists in $\mathbb{R}^d$, then $4|d$ and d is a square.)

Outline

1. Equiangular Lines
   - Geometry
   - Bounds
   - Constructions
2. MUB's
   - Introduction
   - Graphs
3. Spin Models
   - Type-II Matrices
   - Spin Models and MUB's

(What follows is joint work with Aidan Roy.)

AFFINE PLANES

Let $\mathbb{F}$ be a finite field, e.g., $\mathbb{Z}_p$. The points of the affine plane are represented by ordered pairs (x, y) from $\mathbb{F} \times \mathbb{F}$. The lines of finite slope (not parallel to the y-axis) can be represented by ordered pairs $[a, b]$ from $\mathbb{F} \times \mathbb{F}$.

The point (x, y) is on the line $[a, b]$ if $y = ax + b$ (just as in high school). The lines with the same slope form a parallel class.

A GRAPH

Given $\mathbb{F}$ with order q, we construct a graph X as follows.

A GRAPH

Given $\mathbb{F}$ with order q, we construct a graph X as follows.

- The vertices of X are the q^2 points (x, y) and the q^2 lines $[a, b]$.

A GRAPH

Given $\mathbb{F}$ with order q, we construct a graph X as follows.

- The vertices of X are the q^2 points (x, y) and the q^2 lines $[a, b]$.
- The vertex (x, y) is adjacent with the line $[a, b]$ if the point is on the line.

PROPERTIES

The graph just constructed is:

BIPARTITE: point vertices are adjacent only to line vertices, and vice versa.

REGULAR: each vertex has exactly q neighbors.

DIAMETER 4: two points with the same x-coordinate are at distance four, two lines in the same parallel class are at distance four; any other pair of vertices are at distance at most three.

SYMMETRIES

Our graph has two abelian groups of symmetries of order q^2, each with $q+1$ orbits.

- $T_{u,v}$: maps (x,y) to $(x+u,y+v)$ and $[a,b]$ to $[a,b+v-au]$.
- $S_{w,z}$: maps (x,y) to $(x,y+z+wx)$ and $[a,b]$ to $[a+y,b+z]$.

An Abelian group

If we define

$$H_{x,y} := T_{x,y} S_{y,0}.$$

then the set

$$H := \{H_{x,y} : x, y \in \mathbb{F}\}$$

is an abelian group of order q^2 that acts transitively on the points and on the lines.

MUB's

Let $\mathbb{F}$ be a finite field and let H be the group just defined. Let H_0 be the subset of H defined by

$$H_0 = \{H_{u,0} : u \in \mathbb{F}\}.$$

Each character of H is a function on H, its restriction to H_0 is a vector in $\mathbb{C}^q$.

MUB's

Let $\mathbb{F}$ be a finite field and let H be the group just defined. Let H_0 be the subset of H defined by

$$H_0 = \{H_{u,0} : u \in \mathbb{F}\}.$$

Each character of H is a function on H, its restriction to H_0 is a vector in $\mathbb{C}^q$.

Theorem

These q^2 vectors, together with the standard basis vectors, form a set of $q+1$ mutually unbiased bases in $\mathbb{C}^q$.

Semifields

Definition

A semifield is an algebraic structure that satisfies the axioms for a field, except that we do not require multiplication to be associative.

A finite semifield has order p^n, where p is a prime.

Semifields and MUB's

- In the construction just presented, everything still works if we use a commutative semifield in place of field.

SEMIFIELDS AND MUB'S

- In the construction just presented, everything still works if we use a commutative semifield in place of field.
- All known MUB's can be obtained from this construction using suitable commutative semifields.

SEMIFIELDS AND MUB'S

- In the construction just presented, everything still works if we use a commutative semifield in place of field.
- All known MUB's can be obtained from this construction using suitable commutative semifields.
- An equivalent construction was found by Calderbank, Cameron, Kantor and Seidel.

SEMIFIELDS AND MUB'S

- In the construction just presented, everything still works if we use a commutative semifield in place of field.
- All known MUB's can be obtained from this construction using suitable commutative semifields.
- An equivalent construction was found by Calderbank, Cameron, Kantor and Seidel.
- Each commutative semifield gives rise to an affine plane. If the semifield is not a field, the plane is not Desarguesian.

Outline

1. Equiangular Lines
   - Geometry
   - Bounds
   - Constructions
2. MUB's
   - Introduction
   - Graphs
3. Spin Models
   - Type-II Matrices
   - Spin Models and MUB's

SCHUR PRODUCT

DEFINITION

If A and B are $m \times n$ matrices, their Schur product $A \circ B$ is the $m \times n$ matrix given by

$$(A \circ B)_{i,j} = A_{i,j} B_{i,j}.$$

INVERSES

- The matrix J with all entries equal to 1 is the identity for Schur multiplication.

INVERSES

- The matrix J with all entries equal to 1 is the identity for Schur multiplication.
- If no entry of A is zero, there is a unique matrix $A^{(-)}$ such that
$$A \circ A^{(-)} = J;$$
we call $A^{(-)}$ the Schur inverse of A.

Type II

Definition

A $v \times v$ complex matrix W is a type-II matrix if

$$WW^{(-)T} = vI.$$

TYPE II

DEFINITION

A $v \times v$ complex matrix W is a type-II matrix if

$$WW^{(-)T} = vI.$$

So if W is a type-II matrix then

$$W^{-1} = \frac{1}{v} W^{(-)T}.$$

FLAT UNITARY MATRICES

THEOREM

Let W be a $d \times d$ matrix over $\mathbb{C}$. Then any two of the following imply the third:

1. *W is a type-II matrix.*
2. *W is flat.*
3. *Some scalar multiple of W is unitary.*

Spin Models

Definition

If no entry of W is invertible, define

$$W_{i/j} := We_i \circ (We_j)^{(-)}.$$

We say that W is a spin model if each of the vectors $W_{i/j}$ is an eigenvector for W.

The Cyclic Spin Model

Example

Choose θ so that θ^2 is a primitive complex v-th root of 1, and let W be the $v \times v$ matrix given by

$$W_{i,j} := \theta^{(i-j)^2}, \qquad 0 \le i,j < v.$$

SUMMARY

- Spin models were introduced by Vaughan Jones in his work on operator theory and link invariants.

Summary

- Spin models were introduced by Vaughan Jones in his work on operator theory and link invariants.
- They provide representations of the Braid group(s).

SUMMARY

- Spin models were introduced by Vaughan Jones in his work on operator theory and link invariants.
- They provide representations of the Braid group(s).
- There are very few examples.

Outline

1. Equiangular Lines
   - Geometry
   - Bounds
   - Constructions
2. MUB's
   - Introduction
   - Graphs
3. Spin Models
   - Type-II Matrices
   - Spin Models and MUB's

Lemma

Let A be a type-II matrix of order $n \times n$ and let D_j be the diagonal matrix with r-th diagonal entry equal to the r-th entry of the j-th column of $\sqrt{n}A^{(-)}$. If A is a spin model, then for $j = 1, \dots, n$,

$$D_j A D_j^{-1} = A^{-1} D_j A.$$

(Chan, Godsil, Munemasa.)

COROLLARY

Suppose A is a unitary type-II matrix. If A is a spin model, the column sets of the matrices I, A and D_jA form a set of three mutually unbiased bases.

PROOF.

By the previous lemma, $A^{-1}D_jA = D_jAD_j^{-1}$. The diagonal entries of D_j have norm 1, and so D_j is unitary. Hence $D_jAD_j^{-1}$ is a flat unitary matrix and therefore $A^{-1}D_jA$ is flat and unitary. $\square$

Corollary

Suppose A is a unitary type-II matrix. If A is a spin model, the column sets of the matrices I, A and $D_j A$ form a set of three mutually unbiased bases.

Proof.

By the previous lemma, $A^{-1}D_j A = D_j A D_j^{-1}$. The diagonal entries of D_j have norm 1, and so D_j is unitary. Hence $D_j A D_j^{-1}$ is a flat unitary matrix and therefore $A^{-1}D_j A$ is flat and unitary. $\square$


Adobe Reader
File
Edit
View
Document
Tools
Window
Help
Mon 10:42 AM
0803.3553v1.pdf
distorting.pdf
Macintosh HD
ps-quasi-3des.pdf
0604088v2.pdf
projects
v15i1r55.pdf
0803.3781.pdf
notes
C.pdf
cliquer-1.2
0804.2576v1
r6rs
Bento_UG
PythonDocs
0804.2956v1.pdf
photo_notes
europe08
anyons.pdf


Finder
File
Edit
View
Go
Window
Help
(Charged)
Mon 10:42 AM
0803.3553v1.pdf
distorting.pdf
Macintosh HD
ps-quasi-3des.pdf
0604088v2.pdf
projects
v15i1r55.pdf
0803.3781.pdf
notes
C.pdf
cliquer-1.2
0804.2576v1
r6rs
Bento_UG
PythonDocs
0804.2956v1.pdf
photo_notes
europe08
anyons.pdf