Quantum Physics and Algebraic Graph Theory

Chris Godsil

Combinatorics & Optimization
University of Waterloo

Binghampton, May 2009

Outline

1. Colouring
   - Gleason's Theorem
   - Frankl & Rödl
2. MUB's
   - Bounds
   - A Construction
3. Graphs
   - State Transfer
   - Eigenvalues and Periodicity

Henry Hiebert

Hydrogen is an odourless, colourless gas which, given enough time, turns into people.

Outline

Cliques & Cocliques

Definition

We define a graph $\Sigma(d)$ on the unit sphere in $\mathbb{R}^d$ by defining two unit vectors to be adjacent if they are orthogonal.

Although this graph is infinite, its maximal cliques are finite: the cliques of maximal size are the orthonormal bases of $\mathbb{R}^d$, which have size d.

A COLOURING PROBLEM

PROBLEM

Can we colour the vertices of $\Sigma(d)$ with exactly d colours?

If we can, the vertices with a given colour form a coclique which contains a vertex from each clique of size d.

Gleason's Theorem

Theorem

Assume $d \geq 3$ and let f be a function on the unit sphere in $\mathbb{R}^d$. Suppose:

(A) *f is non-negative.*

(B) *For each orthonormal basis $x_1, \ldots, x_d$, we have $f_1 + \cdots + f_d = 1$.*

Then there is a positive definite $d \times d$ matrix A such that $\operatorname{tr}(A) = 1$ and, for all unit vectors x

$$f(x) = x^T Ax.$$

Continuity

Corollary

Assume $d \geq 3$. If f is a non-negative function on the unit sphere in $\mathbb{R}^d$ such that the sum of the values of f on any orthonormal basis is 1, then f is continuous.

No d-Colouring

Corollary

If $d \geq 3$, the graph $\Sigma(d)$ does not have a d-colouring.

No d-Colouring

Corollary

If $d \geq 3$, the graph $\Sigma(d)$ does not have a d-colouring.

Proof.

Assume there is a d-colouring and let S be one of the colour classes. Define a real function f on unit vectors by

$$f(x) = \begin{cases} 1, & x \in S; \\ 0, & x \notin S. \end{cases}$$

Then f is non-negative and sums to 1 on each orthonormal basis, but is not continuous. □

Outline

1 Colouring
- Gleason's Theorem
- Frankl & Rödl

2 MUB's
- Bounds
- A Construction

3 Graphs
- State Transfer
- Eigenvalues and Periodicity

Another Orthogonality Graph

Definition

Define $\Omega(d)$ to be the graph with the ± 1-vectors of length d as vertices, where two vectors are adjacent if they are orthogonal.

Colouring $\Omega(d)$

- If d is odd, $\Omega(d)$ has no edges.

Colouring $\Omega(d)$

- If d is odd, $\Omega(d)$ has no edges.
- If $d \equiv 2$ modulo 4, then $\Omega(d)$ is bipartite.

COLOURING $\Omega(d)$

- If d is odd, $\Omega(d)$ has no edges.
- If $d \equiv 2$ modulo 4, then $\Omega(d)$ is bipartite.
- If $4|d$, then the rows of any $d \times d$ Hadamard matrix form a d-clique in $\Omega(d)$.

COLOURING $\Omega(d)$

- If d is odd, $\Omega(d)$ has no edges.
- If $d \equiv 2$ modulo 4, then $\Omega(d)$ is bipartite.
- If $4|d$, then the rows of any $d \times d$ Hadamard matrix form a d-clique in $\Omega(d)$.
- If $4|d$ and d is not a power of 2, then $\chi(\Omega(d)) > d$.

A THEOREM OF FRANKL & RÖDL

THEOREM

There is a real constant ϵ such that if $4|d$ and d is large enough, then

$$\alpha(\Omega(d)) \le (2-\epsilon)^d.$$

A Question

. . . but exactly when is $\chi(\Omega(2^d)) > 2^d$?

A Question

…but exactly when is $\chi(\Omega(2^d)) > 2^d$?

- $\chi(\Omega(4)) = 4$ and $\chi(\Omega(8)) = 8$.

A Question

…but exactly when is $\chi(\Omega(2^d)) > 2^d$?

- $\chi(\Omega(4)) = 4$ and $\chi(\Omega(8)) = 8$.
- $\chi(\Omega(16)) > 16$.
  (Galliard, Tappe and Wolf: `arXiv:quant-ph/0211011`; De Klerck and Pasechnik: `arXiv:math/0505038`)

A QUESTION

...but exactly when is $\chi(\Omega(2^d)) > 2^d$?

- $\chi(\Omega(4)) = 4$ and $\chi(\Omega(8)) = 8$.
- $\chi(\Omega(16)) > 16$.
  (Galliard, Tappe and Wolf: `arXiv:quant-ph/0211011`;
  De Klerck and Pasechnik: `arXiv:math/0505038`)
- If $d \geq 4$, then $\chi(\Omega(2^d)) > 2^d$.
  (Godsil and Newman: `arXiv:math/0509151`)

Why Should We Care?

We play a game with Alice and Bob. We separately offer Alice and Bob ± 1-vectors v_A and v_B of length 2^m. Without any further communication Alice and Bob must generate vectors x_A and x_B respectively, such that:

Why Should We Care?

We play a game with Alice and Bob. We separately offer Alice and Bob ± 1-vectors v_A and v_B of length 2^m. Without any further communication Alice and Bob must generate vectors x_A and x_B respectively, such that:

- x_A and x_B have length m
- If $v_A = v_B$, then $x_A = x_B$.
- If v_A and v_B are orthogonal, then $x_A \neq x_B$.

A Classical Solution?

Graph View the ± 1 vectors as vertices of $\Omega(2^m)$.

A Classical Solution?

Graph View the ± 1 vectors as vertices of $\Omega(2^m)$.

Coloring Alice and Bob construct a proper coloring of $\Omega(2^m)$ with 2^m colors; in other words a map from its vertices to $\{1, \ldots, 2^m\}$ such that adjacent vertices are assigned different integers.

A Classical Solution?

Graph View the ± 1 vectors as vertices of $\Omega(2^m)$.

Coloring Alice and Bob construct a proper coloring of $\Omega(2^m)$ with 2^m colors; in other words a map from its vertices to $\{1, \dots, 2^m\}$ such that adjacent vertices are assigned different integers.

Solution Alice and Bob determine the color of the vertex they are given, and return this.

A Quantum Solution

Buhrmann, Cleve and Tapp described an algorithm that will solve the problem on $\Omega(2^m)$ for any m, provided that Alice and Bob share 2^m Bell pairs of qubits.

Brassard, Cleve and Widgerson showed that if no 2^m-coloring of $\Omega(2^m)$ exists, no classical algorithm will work without some communication between Alice and Bob.

A QUANTUM SOLUTION

Buhrmann, Cleve and Tapp described an algorithm that will solve the problem on $\Omega(2^m)$ for any m, provided that Alice and Bob share 2^m Bell pairs of qubits.

Brassard, Cleve and Widgerson showed that if no 2^m-coloring of $\Omega(2^m)$ exists, no classical algorithm will work without some communication between Alice and Bob.

In a sense, the quantum chromatic number of $\Omega(2^m)$ is 2^m, even though the chromatic number is actually much larger.

References

- Peter Frankl and Vojtěch Rödl.
  Forbidden intersections.
  Trans. Amer. Math. Soc., 300(1):259–286, 1987.

- Andrew M. Gleason.
  Measures on the closed subspaces of a Hilbert space.
  J. Math. Mech., 6:885–893, 1957.

- C. D. Godsil and M. W. Newman.
  Colouring an orthogonality graph, 2005.
  http://arxiv.org/abs/math/0509151

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 orthonormal 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.)

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.

Outline

Acknowledgement

(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.

Symmetries

Our graph has two abelian groups of automorphisms, each of order q^2 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.

PROBLEM

What is the maximum size of a set of mutually unbiased bases in $\mathbb{C}^6$?

References

- A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel.
  Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets.
  Proc. London Math. Soc. (3), 75(2):436–480, 1997.
- Chris Godsil and Aidan Roy.
  Equiangular lines, mutually unbiased bases, and spin models.
  `arXiv:quant-ph/0511004`, page 23 pp., 2005.
- William K. Wootters and Brian D. Fields.
  Optimal state-determination by mutually unbiased measurements.
  Ann. Physics, 191(2):363–381, 1989.

Outline

A Hamiltonian

Definition

Let X be a graph with adjacency matrix A. We define the Hamiltonian $H_X(t)$ by

$$H_X(t) = \exp(iAt).$$

Properties

- $H_X(t)$ is a unitary matrix, and symmetric.

PROPERTIES

- $H_X(t)$ is a unitary matrix, and symmetric.
- It determines a continuous time quantum walk on X. (This a sequence of probability distributions, where the distributions at time t are the rows of $H(t) \circ \overline{H(t)}$.)

Perfect State Transfer

Definition

Suppose u and v are distinct vertices of X. We say perfect state transfer from u to v occurs at time τ if

$$|H(\tau)_{u,v}| = 1.$$

An Example

Suppose $X = K_2$. Then $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $A^2 = I_2$. So

$$\exp(iAt) = \cos(t)I + i\sin(t)A$$

and hence $H(\pi/2) = iA$. Thus we have perfect state transfer at time $\pi/2$.

An Example

Suppose $X = K_2$. Then $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $A^2 = I_2$. So

$$\exp(iAt) = \cos(t)I + i\sin(t)A$$

and hence $H(\pi/2) = iA$. Thus we have perfect state transfer at time $\pi/2$.

As homework, you should verify that perfect state transfer can occur between the end vertices of a path on three vertices.

The Problem

In which cases is perfect state transfer possible?

The Problem

In which cases is perfect state transfer possible?

- Christandl, Datta, Dorlas, Ekert, Kay, and Landahl showed that it does occur on P_2 and P_3, and on the Cartesian powers of these graphs.

The Problem

In which cases is perfect state transfer possible?

- Christandl, Datta, Dorlas, Ekert, Kay, and Landahl showed that it does occur on P_2 and P_3, and on the Cartesian powers of these graphs.
- Saxena, Shparlinski and Severini have investigated circulants.

Periodicity

Definition

Suppose $u \in V(X)$. If there is a time τ such that

$$|H(\tau)_{u,u}| = 1,$$

we say that X is periodic relative to u, with period τ. If X is periodic with period τ relative to each vertex, we say that X is periodic.

If X has no isolated vertices and is periodic with period τ, then $H(\tau)$ is a scalar matrix.

State Transfer and Periodicity

Lemma

If perfect state transfer from u to v occurs at time τ, then X is periodic relative to both u and v with period 2τ.

Proof.

- If $H(\tau)_{u,v}$ has norm 1, then the uv-entry of $H(\tau)$ is the only entry in its row or column that is not zero.
- $H(\tau)$ is symmetric.

□

Vertex-Transitive Graphs

Lemma

If X is vertex transitive and X is periodic relative to u at time τ, then $H(\tau)$ is a scalar matrix.

Vertex-Transitive Graphs

Lemma

If X is vertex transitive and X is periodic relative to u at time τ, then $H(\tau)$ is a scalar matrix.

Proof.

- $H(t)$ is a polynomial in A.

□

Vertex-Transitive Graphs

Lemma

If X is vertex transitive and X is periodic relative to u at time τ, then $H(\tau)$ is a scalar matrix.

Proof.

- $H(t)$ is a polynomial in A.
- All polynomials in A have constant diagonal.

□

Outline

Spectral Decomposition

Definition

For each eigenvalue θ of A, there a corresponding projection E_θ such that $E_\theta E_\sigma = 0$ if $\theta \neq \sigma$ and, for any complex-valued function f defined on the eigenvalues of A,

$$f(A) = \sum_\theta f(\theta)\, E_\theta.$$

Hence

$$H_X(t) = \sum_\theta \exp(i\theta t)\, E_\theta$$

and the eigenvalues of A are the complex numbers $\exp(i\theta t)$, where θ runs over the eigenvalues of A.

Integer Eigenvalues

If each eigenvalue of A is an integer, then

$$H(2\pi) = \sum_{\theta} E_{\theta} = I$$

and so X is certainly periodic. For a large class of graphs, the converse is true.

Theorem

If X is a regular graph with at least four distinct eigenvalues and X is periodic with respect to some vertex, then its eigenvalues are all integers.

Perfect State Transfer

Theorem

If X is vertex transitive and perfect state transfer takes place at time τ, then $H(\tau)$ is a scalar multiple of a permutation matrix of order two with no fixed points.

Problems

- Is there a graph with no rational eigenvalues on which perfect state transfer occurs?

Problems

- Is there a graph with no rational eigenvalues on which perfect state transfer occurs?
- If perfect state transfer takes place from u to v, what properties must u and v share?

References

Matthias Christandl, Nilanjana Datta, Tony C. Dorlas, Artur Ekert, Alastair Kay, and Andrew J. Landahl.
Perfect transfer of arbitrary states in quantum spin networks.
Physical Review A, 71:032312, 2005.

Chris Godsil.
Periodic graphs, 2008.
arxiv

Nitin Saxena, Simone Severini, and Igor Shparlinski.
Parameters of integral circulant graphs and periodic quantum dynamics.
Int. J. Quant. Inf., 5:417–430, 2007.