Title: Quantum computing and algebraic graph theory

Date: May 24, 2006 04:00 PM

URL: http://pirsa.org/06050011

Abstract: It is somewhat surprising, but problems in quantum computing lead to problems in algebraic graph theory. I will discuss some instances that I am familiar with, and note a commmon thread.

A Bound

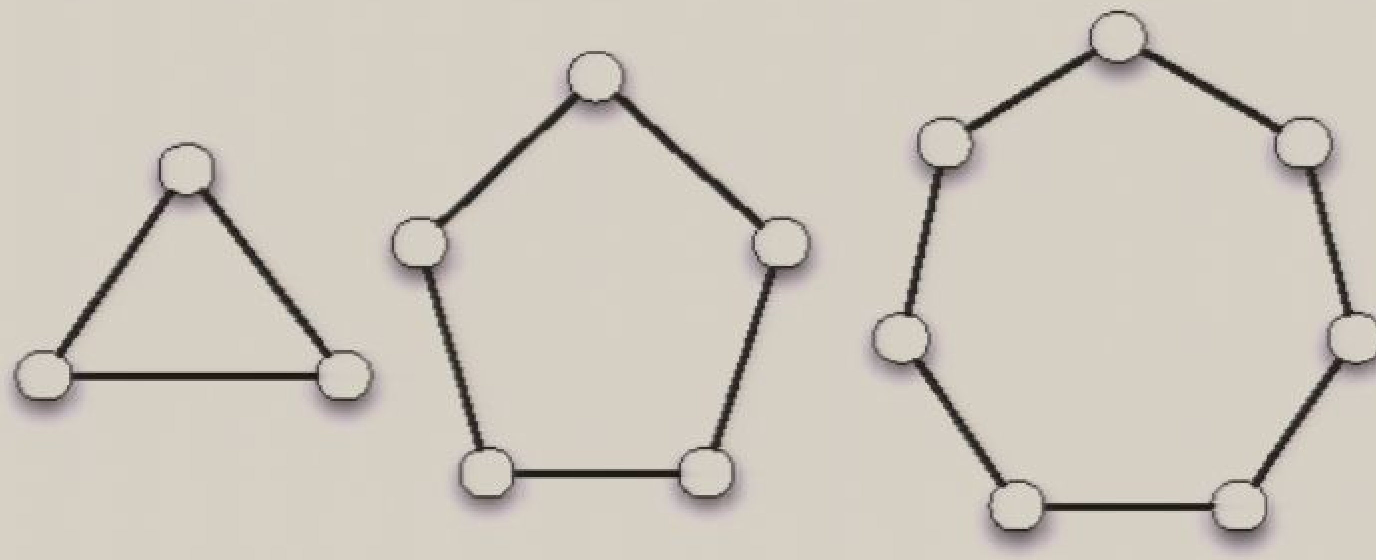
If a graph X has diameter d and maximum valency k, then the number of vertices of X is at most

$$1 + k + k(k-1) + \cdots + k(k-1)^{d-1}.$$

If equality holds, we call X a Moore graph.

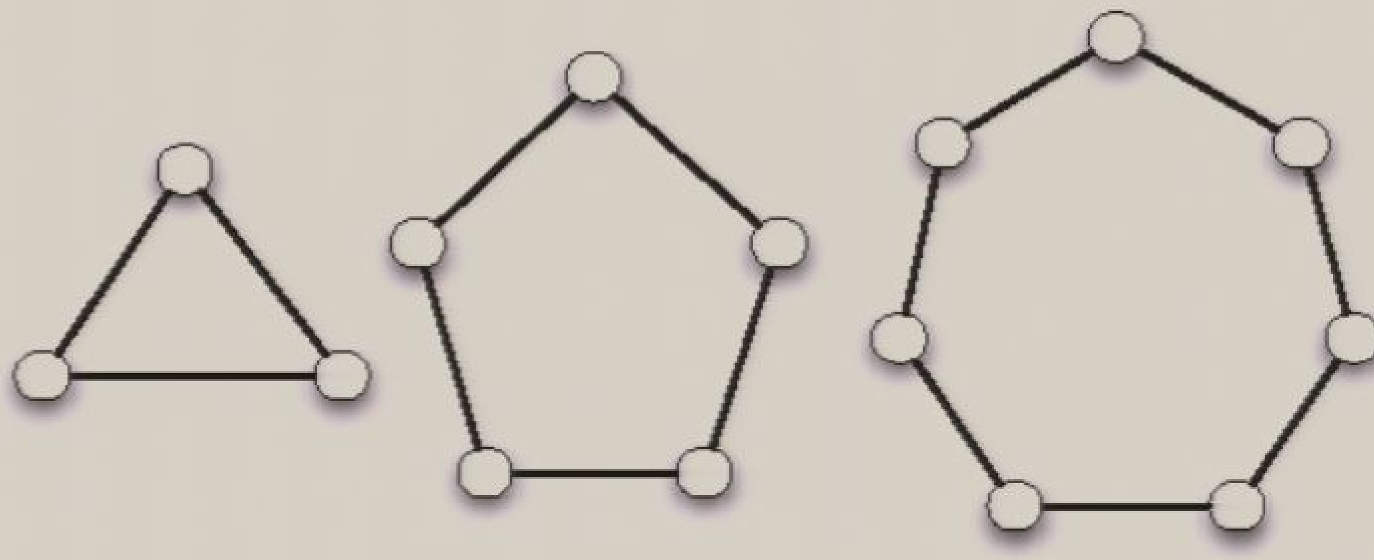
Examples

- Complete graphs, with $d = 1$.
- Odd cycles, with $k = 2$.

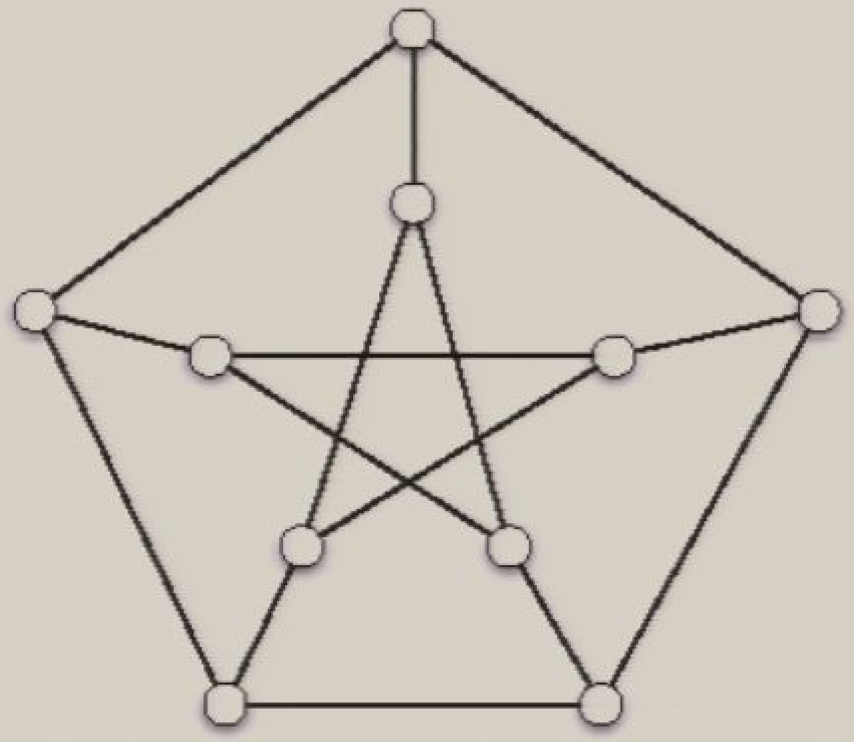


Examples

- Complete graphs, with $d = 1$.
- Odd cycles, with $k = 2$.



Petersen



Outline

Adjacency matrices

Definition

If X is a graph, its adjacency matrix $A(X)$ is the 01-matrix with rows and columns indexed by the vertices of X, and its ij-entry is 1 if vertex i and j are adjacent.

Example

Example

If $X = C_5$, then

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

A Quadratic

Suppose X is a Moore graph with diameter two and valency k. If $A = A(X)$, then

$$A^2 + A - (k-1)I = J.$$

Eigenvalues

A Moore graph with diameter two and valency k has eigenvalues k and

$$\theta = \frac{1}{2}(-1 + \sqrt{4k-3}), \qquad \tau = \frac{1}{2}(-1 - \sqrt{4k-3}).$$

If $k > 2$, then θ and τ must be integers and the multiplicity of τ is

$$\frac{(\theta^2+\theta+1)(\theta^2+1)(\theta+1)}{2\theta+1}.$$

The Consequence

Theorem (Hoffman and Singleton)

If a Moore graph with diameter two and valency k exists, then $k \in \{2, 3, 7, 57\}$.

Valency 57

Problem

Is there a Moore graph with diameter two and valency 57?

Outline

Degree

Suppose $\mathcal{L}$ is a set of lines in complex space $\mathbb{C}^d$. We can specify the lines by unit vectors $z_1, \ldots, z_n$ such that z_i spans the i-th line. The angle between the i-th and j-th lines is determined by $|\langle z_i | z_j \rangle|$. We are concerned with large sets of lines with specified angles.

One Angle

If we have n lines in $\mathbb{C}^d$ with any two distinct lines at the same angle, then $n \leq d^2$. If we have d^2 such lines then:

- A physicist has a SIC-POVM.

One Angle

If we have n lines in $\mathbb{C}^d$ with any two distinct lines at the same angle, then $n \leq d^2$. If we have d^2 such lines then:

- A physicist has a SIC-POVM.
- A mathematician has a set of d^2 equiangular lines in $\mathbb{C}^d$.

Problem

Both physicist and mathematician have the same

Problem

Is it true that for all positive integers d, there is a set of d^2 equiangular lines in $\mathbb{C}^d$?

Mutually Unbiased Bases

Definition

Two orthonormal bases of $\mathbb{C}^d$ are mutually unbiased if the angle between two unit vectors from distinct bases is always the same.

Mutually Unbiased Bases

Definition

Two orthonormal bases of $\mathbb{C}^d$ are mutually unbiased if the angle between two unit vectors from distinct bases is always the same.

So a set of m pairwise mutually unbiased bases is a set of md lines in m classes, such that distinct lines in the same class are orthogonal and lines in different classes are at the same angle.

How Many Bases?

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

Problem

Is it true that there is always a set of $d + 1$ mutually unbiased bases in $\mathbb{C}^d$?

Outline

1. Algebraic Graph Theory
   - Moore Graphs
   - Not Many Moore Graphs
2. Mutually Unbiased Bases
   - Lines in Complex Space
   - An Incidence Graph
3. Coloring
   - A Game
   - Coloring Spheres
4. Graph Isomorphism
   - Isomorphism and Spectra
   - Symmetric Powers
5. Association Schemes

(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 at 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.

More MUB's

- We can use commutative semifields rather than fields. All known MUB's can be obtained from this construction using suitable commutative semifields.

More MUB's

- We can use commutative semifields rather than fields. 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.

More MUB's

- We can use commutative semifields rather than fields. 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.
- There are more graphs than MUB's: we can construct graphs of the same form which lack the abelian group of symmetries.

Outline

The Rules

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 communication Alice and Bob must generate vectors x_A and x_B respectively of length m such that:

The Rules

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 communication Alice and Bob must generate vectors x_A and x_B respectively of length m such that:

- 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 Define $\Omega(n)$ to be the graph with the ± 1-vectors of length n as its vertices; two vertices are adjacent if and only if the corresponding vectors are orthogonal.

A Classical Solution?

Graph Define $\Omega(n)$ to be the graph with the ± 1-vectors of length n as its vertices; two vertices are adjacent if and only if the corresponding vectors are orthogonal.

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 Define $\Omega(n)$ to be the graph with the ± 1-vectors of length n as its vertices; two vertices are adjacent if and only if the corresponding vectors are orthogonal.

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.

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.

Classical Failures

- The vertices of $\Omega(2^m)$ contain an orthogonal basis of $\mathbb{R}^{2^m}$, and so we cannot use fewer than 2^m colors.

Classical Failures

- The vertices of $\Omega(2^m)$ contain an orthogonal basis of $\mathbb{R}^{2^m}$, and so we cannot use fewer than 2^m colors.
- If $m = 1$, 2 or 3, then $\Omega(2^m)$ admits a 2^m-coloring.

Classical Failures

- The vertices of $\Omega(2^m)$ contain an orthogonal basis of $\mathbb{R}^{2^m}$, and so we cannot use fewer than 2^m colors.
- If $m = 1$, 2 or 3, then $\Omega(2^m)$ admits a 2^m-coloring.
- If m is large enough, there is no proper 2^m-coloring (Frankl and Rödl).

Classical Failures

- The vertices of $\Omega(2^m)$ contain an orthogonal basis of $\mathbb{R}^{2^m}$, and so we cannot use fewer than 2^m colors.
- If $m = 1$, 2 or 3, then $\Omega(2^m)$ admits a 2^m-coloring.
- If m is large enough, there is no proper 2^m-coloring (Frankl and Rödl).
- $\Omega(16)$ does not have a 16-coloring (Galliard, Tapp and Wolf).

Classical Failures

- The vertices of $\Omega(2^m)$ contain an orthogonal basis of $\mathbb{R}^{2^m}$, and so we cannot use fewer than 2^m colors.
- If $m = 1$, 2 or 3, then $\Omega(2^m)$ admits a 2^m-coloring.
- If m is large enough, there is no proper 2^m-coloring (Frankl and Rödl).
- $\Omega(16)$ does not have a 16-coloring (Galliard, Tapp and Wolf).
- If $m \geq 4$ there is no 2^m-coloring of $\Omega(2^m)$ (Godsil and Newman).

Outline

The Sphere

We construct an infinite graph X with the points of the unit sphere in $\mathbb{R}^3$ as its vertices, where two unit vectors are adjacent if and only if they are orthogonal.

Problem

Can we properly color the vertices of X using three colors?

Some Physics

Theorem (Gleason)

If f is a non-negative real function on the vertices of X that sums to 1 on each orthonormal basis, then f is continuous.

Some Physics

Theorem (Gleason)

If f is a non-negative real function on the vertices of X that sums to 1 on each orthonormal basis, then f is continuous.

Corollary

We cannot color X with three colors.

Rationality

Theorem (Godsil and Zaks)

The subgraph of the orthogonality graph on the unit sphere in $\mathbb{R}^3$ *formed by the rational vectors is 3-colorable.*

Outline

Isomorphism

If A_1 and A_2 are adjacency matrices of graphs X_1 and X_2 then X_1 and X_2 are isomorphic if and only if there is a permutation matrix P such that

$$P^T A_1 P = A_2.$$

Since a permutation matrix is orthogonal, this implies that A_1 and A_2 are similar and hence they have the same spectrum. (That is, the same characteristic polynomial.)

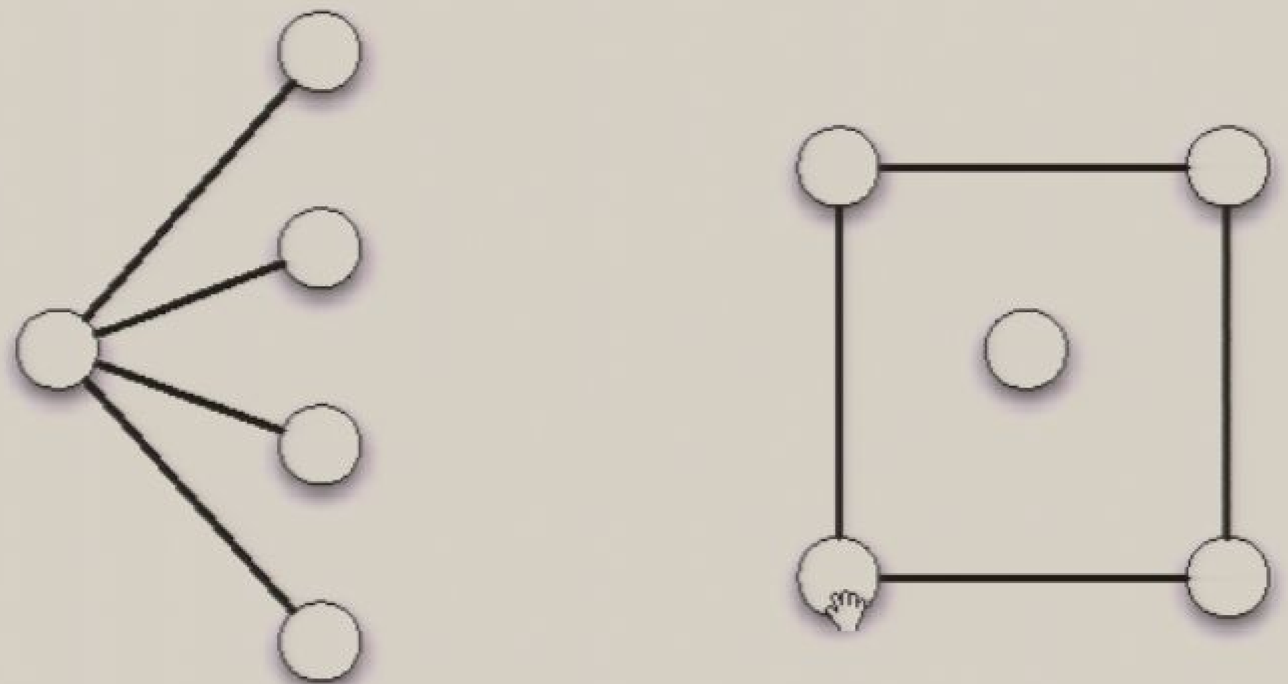
Complexity

The problem of graph isomorphism is in the class NP, but is not known to be NP-complete.
Since we can compute the characteristic polynomial in polynomial time, the idea that we might be able to verify that graphs are not isomorphic by computing characteristic polynomials is very attractive. . .

Salvage?

We can attempt to save the situation by using weighted adjacency matrices, thus replacing $A(X)$ by a symmetric matrix of the same size, but all such attempts fail on strongly regular graphs.

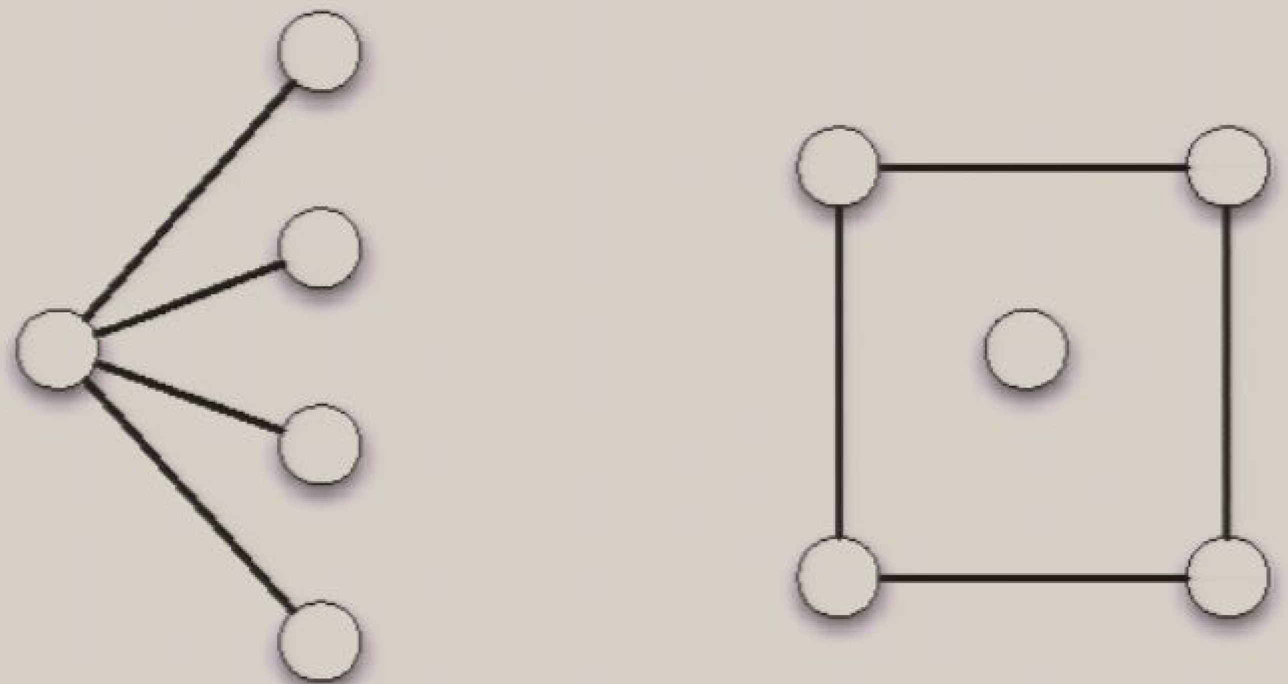
A Counterexample



Complexity

The problem of graph isomorphism is in the class NP, but is not known to be NP-complete.
Since we can compute the characteristic polynomial in polynomial time, the idea that we might be able to verify that graphs are not isomorphic by computing characteristic polynomials is very attractive. . .

A Counterexample



Salvage?

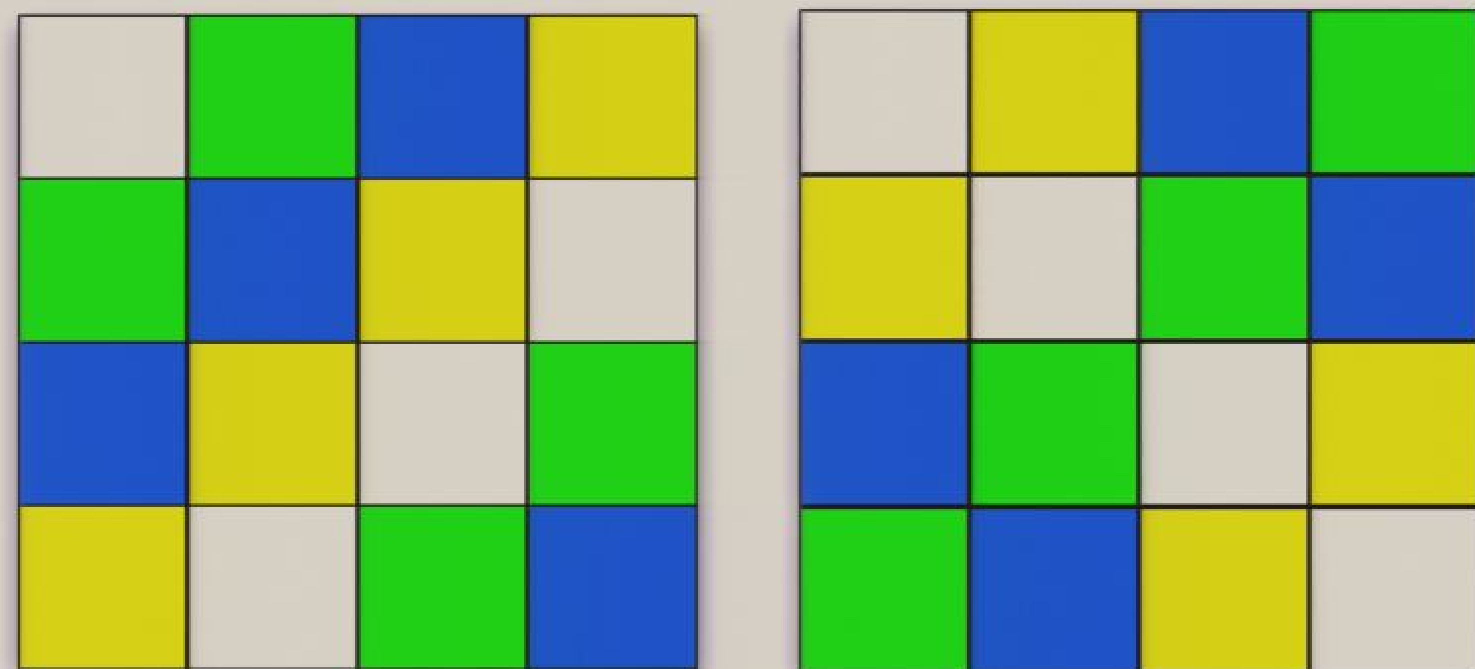
We can attempt to save the situation by using weighted adjacency matrices, thus replacing $A(X)$ by a symmetric matrix of the same size, but all such attempts fail on strongly regular graphs.

Latin Square Graphs

Definition

Let L be an $n \times n$ Latin square. The vertices of the Latin square graph $X(L)$ are the n^2 positions in the matrix L, two positions are adjacent if they are in the same row of L, or the same column, or have the same entry.

Two Latin Squares



Regularity

If X is the graph of a Latin square of order n, then X has $v = n^2$ vertices and:

Regularity

If X is the graph of a Latin square of order n, then X has $v = n^2$ vertices and:

(a) Each vertex has valency $k = 3n - 3$.

Regularity

If X is the graph of a Latin square of order n, then X has $v = n^2$ vertices and:

(a) Each vertex has valency $k = 3n - 3$.

(b) Two adjacent vertices have exactly $a = n$ common neighbours.

Regularity

If X is the graph of a Latin square of order n, then X has $v = n^2$ vertices and:

(a) Each vertex has valency $k = 3n - 3$.

(b) Two adjacent vertices have exactly $a = n$ common neighbours.

(c) Two distinct non-adjacent vertices have exactly $c = 6$ common neighbours.

A Matrix Equation

If X is a Latin square graph with parameters $(v, k; a, c)$, then

$$AJ = JA = kJ$$
$$A^2 - (a-c)A - (k-c)I = cJ$$

and A^r is a linear combination of J, I and A whose coefficients are determined by r and the parameters of X.

The Bad News

If L and M are inequivalent Latin squares of the same order, then $X(L)$ and $X(M)$ are cospectral, but not isomorphic. And there are lots of inequivalent Latin squares.

Outline

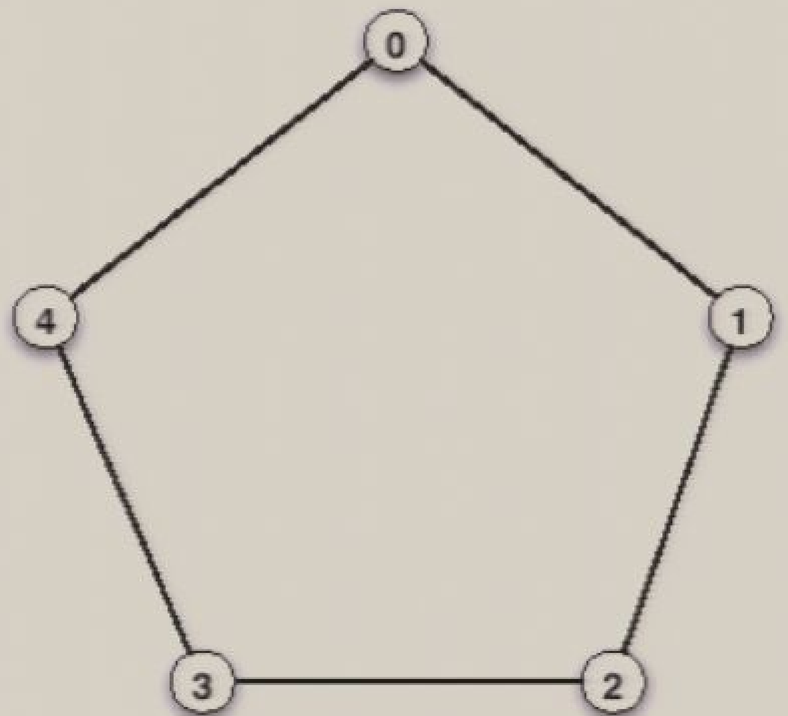
A Construction

We describe a construction due to Terry Rudolph.

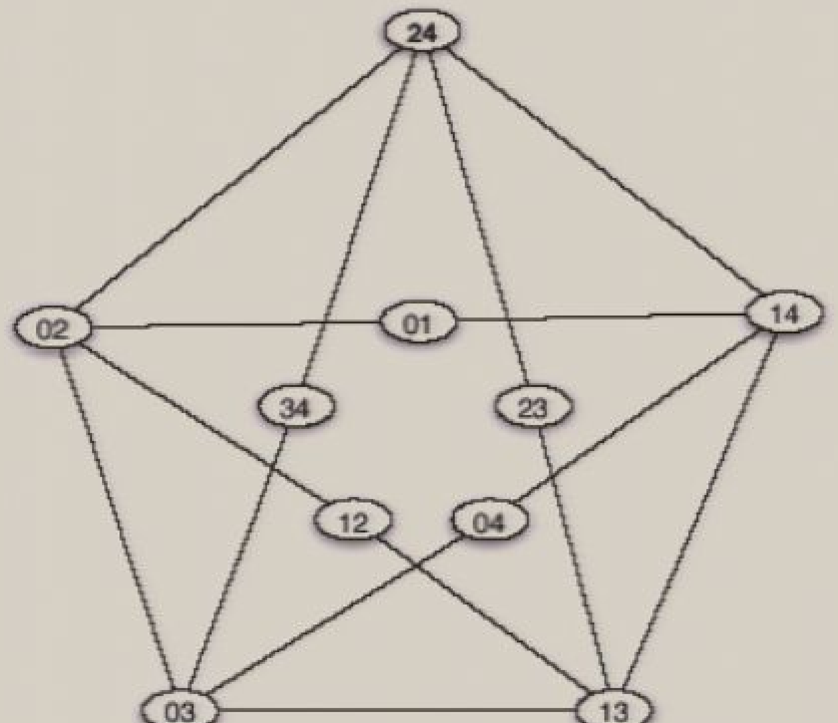
Definition

Let k be a positive integer and let X be a graph. The vertices of the k-th symmetric power $X^{\{k\}}$ of X are the subsets of $V(X)$ with size k, and two k-subsets are adjacent if their symmetric difference is an edge of X.

Example: C_5



$C_5^{\{2\}}$



Walks

Consider k particles undergoing a random walk on a graph X, such the particles occupy distinct vertices. At each time interval, one particle is chosen to move (at random) and it moves (at random) to an unoccupied adjacent vertex.
These random walks correspond to random walks with one particle on $X^{\{k\}}$.

Strongly Regular Graphs

Rudolph observed that

Strongly Regular Graphs

Rudolph observed that

- the spectrum of $X^{\{2\}}$ was better at distinguishing graphs than the spectrum of X but

Strongly Regular Graphs

Rudolph observed that

- the spectrum of $X^{\{2\}}$ was better at distinguishing graphs than the spectrum of X but
- it did not distinguish pairs of strongly regular graphs with the same parameters (for graphs with up to 36 vertices).

The Spectrum of $X^{\{2\}}$

Theorem

The spectrum of $X^{\{2\}}$ is determined by the spectrum of X and the determinant of the series

$$\sum_r \left(\sum_i \binom{r}{i} A^i \circ A^{r-i} \right) t^r.$$

Here $M \circ N$ denotes the Schur product of M and N, defined by

$$(M \circ N)_{i,j} = M_{i,j} N_{i,j}.$$

Another Failure

Theorem

If X and Y are strongly regular graphs with the same parameters, then $X^{\{2\}}$ and $Y^{\{2\}}$ are cospectral.

(See Audenaert, Godsil, Royle and Rudolph: math.CO/0507251.)

But. . .

In all cases tested, the spectrum of $X^{\{3\}}$ determines X. (The cases tested include all strongly regular graphs on 35 and 36 vertices, and there are 32,548 strongly regular graphs on 36 vertices having the same parameter set as the graph of a 6×6 Latin square.)

But. . .

In all cases tested, the spectrum of $X^{\{3\}}$ determines X. (The cases tested include all strongly regular graphs on 35 and 36 vertices, and there are 32,548 strongly regular graphs on 36 vertices having the same parameter set as the graph of a 6×6 Latin square.)

The Spectrum of $X^{\{2\}}$

Theorem

The spectrum of $X^{\{2\}}$ is determined by the spectrum of X and the determinant of the series

$$\sum_r \left(\sum_i \binom{r}{i} A^i \circ A^{r-i} \right) t^r.$$

Here $M \circ N$ denotes the Schur product of M and N, defined by

$$(M \circ N)_{i,j} = M_{i,j} N_{i,j}.$$

But. . .

In all cases tested, the spectrum of $X^{\{3\}}$ determines X. (The cases tested include all strongly regular graphs on 35 and 36 vertices, and there are 32,548 strongly regular graphs on 36 vertices having the same parameter set as the graph of a 6×6 Latin square.)

A Common Thread

The incidence graphs in Section 2, the finite orthogonality graphs in Section 3 and the strongly regular graphs from Section 4 each give rise in a natural way to an association scheme. For our immediate purposes, this is a commutative algebra of symmetric matrices which is also closed under Schur multiplication and contains J, the all-ones matrix.