CASA
Cyber Security in the Age of Large-Scale Adversaries

Quantum isomorphic strongly regular graphs from the E_8 root system

Algebraic Graph Theory Seminar, May 6, 2024

Simon Schmidt
Ruhr-Universität Bochum

Ruhr Universität Bochum RUB

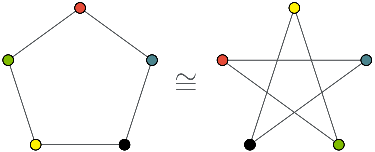
Gefördert durch DFG Deutsche Forschungsgemeinschaft

Horst Görtz Institut

Graph isomorphism

Two graphs G and H are *isomorphic* if there exists a bijection σ such that

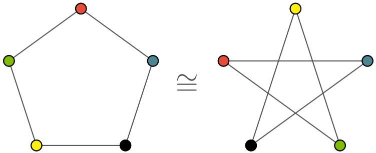
$$i \sim j \qquad \text{if and only if} \qquad \sigma(i) \sim \sigma(j)$$



Graph isomorphism

Two graphs G and H are *isomorphic* if there exists a bijection σ such that

$$i \sim j \qquad \text{if and only if} \qquad \sigma(i) \sim \sigma(j)$$



Theorem (Lovász)

It holds $G \cong H$ if and only if $|\mathrm{hom}(F, G)| = |\mathrm{hom}(F, H)|$ for all graphs F.

Quantum isomorphism

Two graphs G and H are called *quantum isomorphic* if

$$|\mathrm{hom}(F, G)| = |\mathrm{hom}(F, H)| \quad \text{for all } \textit{planar} \text{ graphs } F.$$

Quantum isomorphism

Two graphs G and H are called *quantum isomorphic* if

$$|\mathrm{hom}(F,G)| = |\mathrm{hom}(F,H)| \quad \text{for all } \textit{planar} \text{ graphs } F.$$

Note

- G and H fractionally isomorphic $\iff$ $|\mathrm{hom}(T,G)| = |\mathrm{hom}(T,H)|$ for all trees T
- G and H cospectral $\iff$ $|\mathrm{hom}(C,G)| = |\mathrm{hom}(C,H)|$ for all cycles C

Quantum isomorphism

Two graphs G and H are called *quantum isomorphic* if

$$|\hom(F, G)| = |\hom(F, H)| \quad \text{for all } \textit{planar} \text{ graphs } F.$$

Note

- G and H fractionally isomorphic $\iff |\hom(T, G)| = |\hom(T, H)|$ for all trees T
- G and H cospectral $\iff |\hom(C, G)| = |\hom(C, H)|$ for all cycles C

Theorem (Atserias et al.)

There exist pairs of quantum isomorpic, but non-isomorphic graphs.

Quantum permutation matrices

A *quantum permutation matrix* $u = (u_{ij})_{i,j \in [m]}$ consists of $n \times n$ matrices u_{ij} fulfilling

$$u_{ij} = u_{ij}^* = u_{ij}^2 \quad \text{and} \quad \sum_k u_{ik} = \sum_k u_{ki} = \mathrm{Id}.$$

Quantum permutation matrices

A *quantum permutation matrix* $u = (u_{ij})_{i,j\in[m]}$ consists of $n \times n$ matrices u_{ij} fulfilling

$$u_{ij} = u_{ij}^* = u_{ij}^2 \quad \text{and} \quad \sum_k u_{ik} = \sum_k u_{ki} = \mathrm{Id}.$$

$$m = 2 : \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix} \qquad m = 4 : \begin{pmatrix} p & 1-p & 0 & 0 \\ 1-p & p & 0 & 0 \\ 0 & 0 & q & 1-q \\ 0 & 0 & 1-q & q \end{pmatrix}$$

Quantum permutation matrices

A *quantum permutation matrix* $u = (u_{ij})_{i,j\in[m]}$ consists of C^*-algebra elements u_{ij} fulfilling

$$u_{ij} = u_{ij}^* = u_{ij}^2 \quad \text{and} \quad \sum_k u_{ik} = \sum_k u_{ki} = \mathrm{Id}.$$

$$m = 2 : \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix} \qquad m = 4 : \begin{pmatrix} p & 1-p & 0 & 0 \\ 1-p & p & 0 & 0 \\ 0 & 0 & q & 1-q \\ 0 & 0 & 1-q & q \end{pmatrix}$$

Theorem (Mančinska, Roberson)

Graphs G and H are quantum isomorphic if and only if there exists a quantum permutation matrix $u = (u_{ij})_{i\in V(G), j\in V(H)}$ such that $u_{ik}u_{jl} = 0$ if $i \sim j$ and $k \nsim l$ or vice versa.

Strongly regular graphs

A k-regular graph G is called *strongly regular* if there exists $\lambda, \mu \in \mathbb{N}_0$ such that

- adjacent vertices have λ common neighbors
- non-adjacent vertices have μ common neighbors

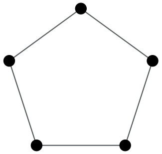
We then say that G is strongly regular with parameters (n, k, λ, μ).

Strongly regular graphs

A k-regular graph G is called *strongly regular* if there exists $\lambda, \mu \in \mathbb{N}_0$ such that

- adjacent vertices have λ common neighbors
- non-adjacent vertices have μ common neighbors

We then say that G is strongly regular with parameters (n, k, λ, μ).



The 5-cycle is strongly regular with parameters $(5, 2, 0, 1)$

A strongly regular graph from the E_8 root system

The E_8 root system consists of the following 240 vectors in $\mathbb{R}^8$:

$$\pm e_i \pm e_j \text{ for } 1 \leq i < j \leq 8, \quad x = \frac{1}{2}(x_1, \ldots, x_8) \text{ for } x_i \in \{\pm 1\} \text{ and } \prod_{i=1}^{8} x_i = 1.$$

Let $G(E_8)$ be the orthogonality graph of the 120 lines spanned by the E_8 root system.

A strongly regular graph from the E_8 root system

The E_8 root system consists of the following 240 vectors in $\mathbb{R}^8$:

$$\pm e_i \pm e_j \text{ for } 1 \leq i < j \leq 8, \quad x = \frac{1}{2}(x_1, \dots, x_8) \text{ for } x_i \in \{\pm 1\} \text{ and } \prod_{i=1}^{8} x_i = 1.$$

Let $G(E_8)$ be the orthogonality graph of the 120 lines spanned by the E_8 root system.

- $G(E_8)$ is strongly regular with parameters $(120, 63, 30, 36)$
- It has independence number 8

A subgroup of the automorphism group of this graph

Define

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and } Y = XZ.$$

Lemma

For each $M := M_1 \otimes M_2 \otimes M_3$ with $M_i \in \{I, X, Y, Z\}$ the maps $\sigma_M : V(G(E_8)) \to V(G(E_8)),\ x \mapsto Mx$ are automorphisms of $G(E_8)$.

A subgroup of the automorphism group of this graph

Define

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and } Y = XZ.$$

Lemma

For each $M := M_1 \otimes M_2 \otimes M_3$ with $M_i \in \{I, X, Y, Z\}$ the maps $\sigma_M : V(G(E_8)) \to V(G(E_8)),\ x \mapsto Mx$ are automorphisms of $G(E_8)$.

We obtain a subgroup $L \cong \mathbb{Z}_2^6$ of $\mathrm{Aut}(G(E_8))$. The action of L on $V(G(E_8))$ has 15 orbits, partitioning the vertex set in 15 cliques of size 8.

$$\begin{aligned}
V_1 &: \quad e_1 \pm e_2, e_3 \pm e_4, e_5 \pm e_6, e_7 \pm e_8,\\
V_2 &: \quad e_1 \pm e_3, e_2 \pm e_4, e_5 \pm e_7, e_6 \pm e_8,\\
V_3 &: \quad e_1 \pm e_4, e_2 \pm e_3, e_5 \pm e_8, e_6 \pm e_7,\\
V_4 &: \quad e_1 \pm e_5, e_2 \pm e_6, e_3 \pm e_7, e_4 \pm e_8,\\
V_5 &: \quad e_1 \pm e_6, e_2 \pm e_5, e_3 \pm e_8, e_4 \pm e_7,\\
V_6 &: \quad e_1 \pm e_7, e_2 \pm e_8, e_3 \pm e_5, e_4 \pm e_6,\\
V_7 &: \quad e_1 \pm e_8, e_2 \pm e_7, e_3 \pm e_6, e_4 \pm e_5,
\end{aligned}$$

$$\begin{aligned}
V_8 &: \quad x_{\{1,2\}}, x_{\{3,4\}}, x_{\{5,6\}}, x_{\{7,8\}}, x_{\{1,4,6,8\}}, x_{\{2,3,6,8\}}, x_{\{2,4,5,8\}}, x_{\{2,4,6,7\}},\\
V_9 &: \quad x_{\{1,3\}}, x_{\{2,4\}}, x_{\{5,7\}}, x_{\{6,8\}}, x_{\{1,4,7,8\}}, x_{\{1,4,5,6\}}, x_{\{1,2,6,7\}}, x_{\{1,2,5,8\}},\\
V_{10} &: \quad x_{\{1,4\}}, x_{\{2,3\}}, x_{\{5,8\}}, x_{\{6,7\}}, x_{\{1,3,7,8\}}, x_{\{1,3,5,6\}}, x_{\{1,2,5,7\}}, x_{\{1,2,6,8\}},\\
V_{11} &: \quad x_{\{1,5\}}, x_{\{2,6\}}, x_{\{3,7\}}, x_{\{4,8\}}, x_{\{1,6,7,8\}}, x_{\{2,5,7,8\}}, x_{\{4,5,6,7\}}, x_{\{1,2,4,7\}},\\
V_{12} &: \quad x_{\{1,6\}}, x_{\{2,5\}}, x_{\{3,8\}}, x_{\{4,7\}}, x_{\{1,5,7,8\}}, x_{\{2,6,7,8\}}, x_{\{3,5,6,7\}}, x_{\{4,5,6,8\}},\\
V_{13} &: \quad x_{\{1,7\}}, x_{\{2,8\}}, x_{\{3,5\}}, x_{\{4,6\}}, x_{\{1,5,6,8\}}, x_{\{3,6,7,8\}}, x_{\{2,5,6,7\}}, x_{\{4,5,7,8\}},\\
V_{14} &: \quad x_{\{1,8\}}, x_{\{2,7\}}, x_{\{3,6\}}, x_{\{4,5\}}, x_{\{1,5,6,7\}}, x_{\{4,6,7,8\}}, x_{\{2,5,6,8\}}, x_{\{3,5,7,8\}},\\
V_{15} &: \quad x_{\varnothing}, x_{\{5,6,7,8\}}, x_{\{3,4,7,8\}}, x_{\{2,4,6,8\}}, x_{\{3,4,5,6\}}, x_{\{2,4,5,7\}}, x_{\{2,3,6,7\}}, x_{\{2,3,5,8\}}.
\end{aligned}$$

Construction of quantum permutation matrices

Denote by $P_x := \frac{1}{\|x\|^2} x x^*$ the rank-one projection associated to x.

Quantum permutation matrix

For every $i \in [15]$, choose $w_i \in V_i$. For $x, y \in V_i$, define

$$u^{(i)}_{x,y} = M_{xy} P_{w_i} M^*_{xy},$$

where $M_{xy} = M_1 \otimes M_2 \otimes M_3$ with $M_k \in \{I, X, Y, Z\}$ such that $M_{xy} x = y$.

Construction of quantum permutation matrices

Denote by $P_x := \frac{1}{\|x\|^2} xx^*$ the rank-one projection associated to x.

Quantum permutation matrix

For every $i \in [15]$, choose $w_i \in V_i$. For $x, y \in V_i$, define

$$u^{(i)}_{x,y} = M_{xy} P_{w_i} M^*_{xy},$$

where $M_{xy} = M_1 \otimes M_2 \otimes M_3$ with $M_k \in \{I, X, Y, Z\}$ such that $M_{xy} x = y$.

$$\begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 & u_8 \\ u_2 & u_1 & u_4 & u_3 & u_6 & u_5 & u_8 & u_7 \\ u_3 & u_4 & u_1 & u_2 & u_7 & u_8 & u_5 & u_6 \\ u_4 & u_3 & u_2 & u_1 & u_8 & u_7 & u_6 & u_5 \\ u_5 & u_6 & u_7 & u_8 & u_1 & u_2 & u_3 & u_4 \\ u_6 & u_5 & u_8 & u_7 & u_2 & u_1 & u_4 & u_3 \\ u_7 & u_8 & u_5 & u_6 & u_3 & u_4 & u_1 & u_2 \\ u_8 & u_7 & u_6 & u_5 & u_4 & u_3 & u_2 & u_1 \end{pmatrix}$$

Construction of quantum permutation matrices

Denote by $P_x := \frac{1}{\|x\|^2} xx^*$ the rank-one projection associated to x.

Quantum permutation matrix

For every $i \in [15]$, choose $w_i \in V_i$. For $x, y \in V_i$, define

$$u^{(i)}_{x,y} = M_{xy} P_{w_i} M^*_{xy},$$

where $M_{xy} = M_1 \otimes M_2 \otimes M_3$ with $M_k \in \{I, X, Y, Z\}$ such that $M_{xy} x = y$.

$$\begin{pmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 & u_8 \\ u_2 & u_1 & u_4 & u_3 & u_6 & u_5 & u_8 & u_7 \\ u_3 & u_4 & u_1 & u_2 & u_7 & u_8 & u_5 & u_6 \\ u_4 & u_3 & u_2 & u_1 & u_8 & u_7 & u_6 & u_5 \\ u_5 & u_6 & u_7 & u_8 & u_1 & u_2 & u_3 & u_4 \\ u_6 & u_5 & u_8 & u_7 & u_2 & u_1 & u_4 & u_3 \\ u_7 & u_8 & u_5 & u_6 & u_3 & u_4 & u_1 & u_2 \\ u_8 & u_7 & u_6 & u_5 & u_4 & u_3 & u_2 & u_1 \end{pmatrix}$$

$$\begin{array}{c} \\ V_1 \\ V_2 \\ \vdots \\ \vdots \\ V_{15} \end{array} \begin{array}{c} \begin{array}{ccccc} V_1 & V_2 & \cdots & \cdots & V_{15} \end{array} \\ \begin{pmatrix} u^{(1)} & 0 & 0 & \cdots & 0 \\ 0 & u^{(2)} & 0 & \cdots & 0 \\ 0 & 0 & u^{(3)} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & u^{(15)} \end{pmatrix} \end{array}$$

The quantum isomorphism

Lemma

Let $k, s \in V_i$ and $l, t \in V_j$, $i \neq j$.

(i) For $k \sim l, s \sim t$, we have $u_{ks}^{(i)} u_{lt}^{(j)} = 0$ if and only if $\langle w_i, w_j \rangle = 0$.

(ii) For $k \sim l, s \nsim t$ or vice versa, we have $u_{ks}^{(i)} u_{lt}^{(j)} = 0$ if and only if $\langle w_i, w_j \rangle \neq 0$.

The quantum isomorphism

Lemma

Let $k, s \in V_i$ and $l, t \in V_j$, $i \neq j$.

(i) For $k \sim l, s \sim t$, we have $u^{(i)}_{ks} u^{(j)}_{lt} = 0$ if and only if $\langle w_i, w_j \rangle = 0$.

(ii) For $k \sim l, s \nsim t$ or vice versa, we have $u^{(i)}_{ks} u^{(j)}_{lt} = 0$ if and only if $\langle w_i, w_j \rangle \neq 0$.

Recall: $G \cong_q H \iff$ there exists a quantum permutation matrix $u = (u_{ij})_{i \in V(G), j \in V(H)}$ such that $u_{ik} u_{jl} = 0$ if $i \sim_G j$ and $k \nsim_H l$ or vice versa.

Quantum isomorphic graph

Let $\boldsymbol{w} = \{w_1, \ldots, w_{15}\}$ and define the graph $G^{\boldsymbol{w}}$ as follows. We let $V(G^{\boldsymbol{w}}) = V(G(E_8))$.

- If $s \in V_i$, $t \in V_j$, $\langle w_i, w_j \rangle \neq 0$, let $s \sim_{G^{\boldsymbol{w}}} t$ if and only if $s \sim_{G(E_8)} t$
- If $s \in V_i$, $t \in V_j$, $\langle w_i, w_j \rangle = 0$, let $s \sim_{G^{\boldsymbol{w}}} t$ if and only if $s \nsim_{G(E_8)} t$

Quantum isomorphic graphs

Theorem (S.)

The graphs $G(E_8)$ and $G^{\boldsymbol{w}}$ are quantum isomorphic, non-isomorphic strongly regular graphs.

Quantum isomorphic graphs

Theorem (S.)

The graphs $G(E_8)$ and $G^{\mathbf{w}}$ are quantum isomorphic, non-isomorphic strongly regular graphs.

- It holds $G(E_8) \cong_q G^{\mathbf{w}}$, since the quantum permutation matrix we constructed fulfills $u_{ik}u_{jl} = 0$ if $i \sim_{G(E_8)} j$ and $k \nsim_{G^{\mathbf{w}}} l$ or vice versa.

Quantum isomorphic graphs

Theorem (S.)

The graphs $G(E_8)$ and $G^{\mathbf{w}}$ are quantum isomorphic, non-isomorphic strongly regular graphs.

- It holds $G(E_8) \cong_q G^{\mathbf{w}}$, since the quantum permutation matrix we constructed fulfills $u_{ik}u_{jl} = 0$ if $i \sim_{G(E_8)} j$ and $k \nsim_{G^{\mathbf{w}}} l$ or vice versa.
- It holds $G(E_8) \ncong G^{\mathbf{w}}$ since $\{w_1, \dots, w_{15}\}$ is an independent set of size 15 in $G^{\mathbf{w}}$. $G(E_8)$ has independence number 8.

Quantum isomorphic graphs

Theorem (S.)

The graphs $G(E_8)$ and $G^{\boldsymbol{w}}$ are quantum isomorphic, non-isomorphic strongly regular graphs.

- It holds $G(E_8) \cong_q G^{\boldsymbol{w}}$, since the quantum permutation matrix we constructed fulfills $u_{ik}u_{jl} = 0$ if $i \sim_{G(E_8)} j$ and $k \nsim_{G^{\boldsymbol{w}}} l$ or vice versa.
- It holds $G(E_8) \ncong G^{\boldsymbol{w}}$ since $\{w_1, \dots, w_{15}\}$ is an independent set of size 15 in $G^{\boldsymbol{w}}$. $G(E_8)$ has independence number 8.

Lemma

The graphs $G^{\boldsymbol{w}_{(1)}}$ and $G^{\boldsymbol{w}_{(2)}}$ are isomorphic for any choice of $\boldsymbol{w}_{(1)}$, $\boldsymbol{w}_{(2)}$.

Another strongly regular graph with parameters $(120, 63, 30, 36)$

The graph $VO_6^+(2)$:

- Vertex set: $\mathbb{F}_2^6$
- Vertices x, y are adjacent if $Q(x+y) = 0$, where $Q(z) = z_1z_2 + z_3z_4 + z_5z_6$

Another strongly regular graph with parameters $(120, 63, 30, 36)$

The graph $VO_6^+(2)$:

- Vertex set: $\mathbb{F}_2^6$
- Vertices x, y are adjacent if $Q(x+y) = 0$, where $Q(z) = z_1z_2 + z_3z_4 + z_5z_6$

Another strongly regular graph

Define G_1 as follows.

- Vertex set: One orbit of the cliques of size 8 under $\mathbb{Z}_2^6 \times A_8$ in $VO_6^+(2)$
- Vertices are adjacent if the associated cliques have two points in common.

Another strongly regular graph with parameters $(120, 63, 30, 36)$

The graph $VO_6^+(2)$:

- Vertex set: $\mathbb{F}_2^6$
- Vertices x, y are adjacent if $Q(x+y) = 0$, where $Q(z) = z_1z_2 + z_3z_4 + z_5z_6$

Another strongly regular graph

Define G_1 as follows.

- Vertex set: One orbit of the cliques of size 8 under $\mathbb{Z}_2^6 \times A_8$ in $VO_6^+(2)$
- Vertices are adjacent if the associated cliques have two points in common.

Theorem (S.)

The complement of G_1 is isomorphic to $G^{\boldsymbol{w}}$.

Properties of the graphs

- $G(E_8)$ is distance-transitive, $\bar{G}_1$ is not
- We have $|\text{Aut}\, G(E_8)| = 348364800$, $\text{Aut}\, \bar{G}_1 = 1290240$
- $\bar{G}_1$ has independence number 15, the graph $G(E_8)$ has independence number 8

Godsil-McKay switching

Take a graph G, a partition $\pi = \{C_1, \ldots, C_k, D\}$ of $V(G)$. Suppose for $i, j \in [k]$, $v \in D$:

(i) any two vertices in C_i have the same number of neighbors in C_j,

(ii) the vertex v has either 0, $\frac{n_i}{2}$ or n_i neighbors in C_i, where $n_i := |C_i|$.

Define graph $G^{\pi,D}$: For each $v \in D$ and $i \in [k]$ such that v has $\frac{n_i}{2}$ neighbors in C_i, delete these $\frac{n_i}{2}$ edges and join v instead to the other $\frac{n_i}{2}$ vertices in C_i.

Theorem (Godsil, McKay)

The graphs G and $G^{\pi,D}$ are cospectral.

Godsil-McKay switching

Theorem (S.)

Assume $G_1 \cong_q G_2$ with quantum permutation matrix u of the form

$$\begin{array}{c} \\ V_1 \\ V_2 \\ \vdots \\ \vdots \\ V_m \end{array} \begin{array}{c} \begin{array}{ccccc} V_1 & V_2 & \dots & \dots & V_m \end{array} \\ \begin{pmatrix} u^{(1)} & 0 & 0 & \dots & 0 \\ 0 & u^{(2)} & 0 & \dots & 0 \\ 0 & 0 & u^{(3)} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & u^{(m)} \end{pmatrix} \end{array}$$

Let $\{S_1, \dots, S_{k+1}\}$ be a partition of $[m]$ and define a partition $\pi = \{C_1, \dots, C_k, D\}$ of the vertex set by $C_i := \cup_{s \in S_i} V_s$, $D := \cup_{s \in S_{k+1}} V_s$. If G_1 and G_2 fulfill the properties (i) and (ii) with respect to π, the graphs $G_1^{\pi,D}$ and $G_2^{\pi,D}$ are quantum isomorphic.

Summary

- We constructed two non-isomorphic strongly regular graphs whose homomorphism counts from all planar graphs coincide
- The quantum permutation matrix was constructed from a subgroup of $\mathrm{Aut}(G(E_8))$, related to Pauli matrices
- Using Godsil-McKay switching, one obtains more such pairs of quantum isomorphic strongly regular graphs

Summary

- We constructed two non-isomorphic strongly regular graphs whose homomorphism counts from all planar graphs coincide
- The quantum permutation matrix was constructed from a subgroup of $\mathrm{Aut}\,(G(E_8))$, related to Pauli matrices
- Using Godsil-McKay switching, one obtains more such pairs of quantum isomorphic strongly regular graphs

Thank you for your attention!

Summary

- We constructed two non-isomorphic strongly regular graphs whose homomorphism counts from all planar graphs coincide
- The quantum permutation matrix was constructed from a subgroup of $\mathrm{Aut}(G(E_8))$, related to Pauli matrices
- Using Godsil-McKay switching, one obtains more such pairs of quantum isomorphic strongly regular graphs

Thank you for your attention!

S. Schmidt, Quantum isomorphic strongly regular graphs from the E8 root system, Algebraic Combinatorics, Volume 7 (2024) no. 2