Quantum Symmetries of Graphs and Nonlocal Games

Michael Brannan
Department of Pure Mathematics
Institute for Quantum Computing
University of Waterloo

University at Buffalo, March 31, 2022

What is this talk about?

Some intriguing connections that have recently emerged between

- **"Pure" Mathematics** – noncommutative algebra, representation theory, operator algebras, combinatorics, ...
- **Quantum Information Theory (QIT)** – nonlocal games, interactive proof systems, quantum entanglement, complexity theory, ...

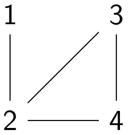
E.g., the Connes Embedding Problem in operator algebras, capacity problems for noisy quantum channels, ...
Today I will illustrate these connection by considering graphs, their (quantum) symmetries, and some related nonlocal games of interest in QIT.

Graphs

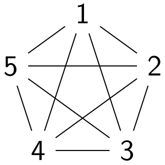
A (finite, simple) graph is a pair $X = (V, E)$ where

- V is a finite set (the vertices of X) and
- $E \subset V \times V$ (the edges of X) satisfying $(x, x) \notin E$ for all $x \in V$ and $(x, y) \in E \iff (y, x) \in E$.

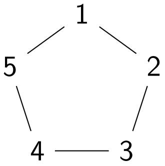
$X =$



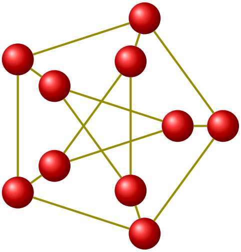
$K_5 =$



$C_5 =$



$P =$



Symmetries of Graphs

Let $X = (V(X), E(X))$ and $Y = (E(Y), V(Y))$ be graphs.

- An graph isomorphism from X to Y is a **bijection** $\varphi : V(X) \to V(Y)$ that preserves edges:

$$(x, y) \in E(X) \iff (\varphi(x), \varphi(y)) \in E(Y).$$

- If $X = Y$, then graph isomorphisms $X \to X$ form a group under composition, called the symmetry group $G(X)$ of X.

Examples: (From previous slide)

$$G(X) = S_2,\ G(K_5) = S_5,\ G(C_5) = D_5,\ G(P) = S_5.$$

$$\mathrm{Z} = \quad \begin{array}{ccc} 1 & — & 3 \\ | & / & | \\ 2 & — & 4 \\ | & & | \\ 5 & & 6 \end{array} \implies \mathrm{G(Z)} = \{\mathrm{e}\} \text{ (i.e., } Z \text{ is rigid)}$$

$G(X)$ as a Matrix Group

- Given a graph $X = (V, E)$ with $|V| = n$ vertices, its symmetry group $G(X)$ is a subgroup of the symmetric group S_n.
- Therefore automorphisms of X can be identified with permutation matrices

  $$\sigma = [\sigma_{xy}]_{x,y \in V} \in M_n(\mathbb{C})$$

  that respect the edge structure of X. That is,

  $$\boxed{\sigma A_X = A_X \sigma,}$$

  where $A_X = [A_X(x, y)]_{x,y \in V} = [\chi_E(x, y)]_{x,y \in V}$ is the adjacency matrix of X.
- So
  $$G(X) = \{\sigma \in S_n \mid A_X \sigma = \sigma A_X\} \subset M_n(\mathbb{C}).$$
- In general, $G(X)$ is difficult to compute!

Quantum Symmetries of Graphs

Let's make life more complicated and generalize the notion of symmetries of graphs, using ideas from noncommutative algebra

Definition

Let $X = (V, E, A_X)$ be a graph with $n = |V|$. Let B be a unital associative $\mathbb{C}$-algebra. A matrix $p = [p_{xy}]_{x,y \in V} \in M_n(B)$ is called a quantum automorphism of X if its entries satisfy the relations

$$(1) \quad p_{xy}p_{xz} = \delta_{\{y=z\}}p_{xy}, \quad p_{xy}p_{zy} = \delta_{\{x=z\}}p_{xy}$$

$$(2) \quad \sum_x p_{xy} = 1, \quad \sum_y p_{xy} = 1$$

$$(3) \quad pA_X = A_X p.$$

- Think of a quantum automorphisms $p \in M_n(B)$ of X as "B-valued permutation matrices". We regard these as quantum symmetries of the graph X.
- **Do they form a group?** No.

The Quantum Symmetry Group of a Graph

Although quantum automorphisms of X don't form a group, they can be assembled into a quantum group, denoted by $G^+(X)$.

Definition (Banica, Bichon)

Let $\mathcal{C}(G^+(X))$ be the universal unital algebra with **generators** $\{q_{xy}\}_{x,y\in V}$ and **relations** making $q = [q_{xy}]$ a quantum automorphism of X. $\in M_n(\mathcal{C}(G^+(X)))$

- $\mathcal{C}(G^+(X))$ captures "all" quantum symmetries of X via its representation theory: Quantum automorphisms $p = [p_{xy}] \in M_n(B)$ of X correspond to **representations**

$$\pi : \mathcal{C}(G^+(X)) \to B; \qquad \pi(q_{xy}) = p_{xy}.$$

- In particular, the **algebra of coordinate functions** $\mathcal{C}(G(X))$ on the symmetry group $G(X)$ is the **abelianization** of $\mathcal{C}(G^+(X))$:

$$q_{xy} \mapsto \text{ the } (x,y) \text{ coordinate function on } G(X) \subset S_n \subset M_n.$$

The Quantum Symmetry Group of a Graph

$$\mathcal{C}(G^+(X)) = \left\langle q_{xy},\ x, y \in V \;\middle|\; q = [q_{xy}] \text{ is a quantum aut. of } X \right\rangle.$$

$$\mathcal{C}(G(X)) = \mathcal{C}(G^+(X))/\langle \text{commutators} \rangle$$

- We say that a graph X has quantum symmetry if $\mathcal{C}(G^+(X))$ is non-abelian. I.e., if $\mathcal{C}(G^+(X)) \neq \mathcal{C}(G(X))$.
- If $\mathcal{C}(G^+(X))$ is non-abelian, it is not an algebra of functions on a group. But it still has many "group-like" properties.
- $\mathcal{C}(G^+(X))$ is actually a Hopf-$*$-algebra with structure maps:

$$\Delta(q_{xy}) = \sum_z q_{xz} \otimes q_{zy},\ S(q_{xy}) = q_{yx},\ \epsilon(q_{xy}) = \delta_{x,y},\ q_{xy}^* = q_{xy}.$$

- Get a **quantum group** $G^+(X) = (\mathcal{C}(G^+(X)), \Delta, S, \epsilon)$ – the quantum symmetry group of X.

Graphs with Quantum Symmetry

Do some graphs actually admit quantum symmetries?

- Yes! Take $X = K_n$. Know $G(K_n) = S_n$.
- $\mathcal{C}(G^+(K_n))$ has generators q_{xy} with relations $q_{xy}q_{xz} = \delta_{y,z}q_{xy}$, $q_{yx}q_{zx} = \delta_{y,z}q_{yx}$, $\sum_x q_{xy} = 1 = \sum_y q_{xy}$
- We write $G^+(K_n) = S_n^+$. (Wang's Q. Permutation gp '98)
- Take $n = 4$, a, b self-adjoint idempotents in a $*$-algebra B. Put

$$p = \begin{pmatrix} a & 1-a & 0 & 0 \\ 1-a & a & 0 & 0 \\ 0 & 0 & b & 1-b \\ 0 & 0 & 1-b & b \end{pmatrix} \quad (4 \times 4 \text{ q. permutation})$$

- Get a quotient map $\mathcal{C}(S_4^+) \to \mathbb{C}\langle a, b\rangle \subseteq B$; $q_{xy} \mapsto p_{xy}$.
- In particular, we have $\mathcal{C}(S_4^+) \to \mathbb{C}[\mathbb{Z}_2 \star \mathbb{Z}_2]$.
- In general $\mathcal{C}(G^+(X))$ can be ∞-dimensional and very noncommutative!

Why study $G^+(X)$?

- Determining $G^+(X)$ for a given graph X is an interesting (and difficult) algebraic problem.
- $G^+(X)$ defines new classes quantum algebraic invariants for graphs (quantum vertex transitivity, quantum rigidity, etc...)
- $G^+(X)$ is known for most small graphs ($|V| \leq 11$) and certain families of graphs [Banica-Bichon, Ren, Schmidt].
- For **operator algebraists**, $\mathcal{C}(G^+(X))$ can be viewed as a quantum version of the a group algebra $\mathbb{C}\Gamma$ for some discrete group Γ.
- In fact, one can complete $\mathcal{C}(G^+(X))$ into a Hilbert spaace $L^2(G^+(X))$, and form the quantum group von Neumann algebra

$$\underbrace{L^\infty(G^+(X)) = \mathcal{C}(G^+(X))''}_{\text{an analogue of the group von Neumann algebra } \mathcal{L}(\Gamma)=\mathbb{C}\Gamma''} \subset B(L^2(G^+(X))).$$

Some operator algebraic results

For complete graphs, we a have a fairly good handle on the operator algebraic structure of $G^+(K_n) = S_n^+$:

Theorem (B-Chirvasitu-Freslon)

For each n, $\mathcal{C}(S_n^+)$ is a residually finite-dimensional (RFD) $*$-algebra. Moreover, $L^\infty(S_n^+)$ is a full II_1-factor with the Connes Embedding Property (CEP).

- Informally: a von Neumann algebra M has the CEP if it can be "well-approximated" by matrices. (Not all von Neumann algebras have the CEP! **[Ji-Natarajan-Vidick-Wright-Yuen]**

Question: What about general $G^+(X)$? How big/complicated can we make $\mathcal{C}(G^+(X)), L^\infty(G^+(X))$?

Theorem (B.-Chirvasitu-Roberson)

Let Γ be a finitely generated, finitely presented group. Then there exists a finite graph X and a Hopf $*$-algebra embedding

$$\mathbb{C}\Gamma \hookrightarrow \mathcal{C}(G^+(X)).$$

- The preceding theorems say that you can make $G^+(X)$ very complicated from an algebraic/operator algebraic perspective.
- Most interestingly, these results arise from studying the quantum groups $G^+(X)$ from the perspectives of quantum information theory and representation theory.

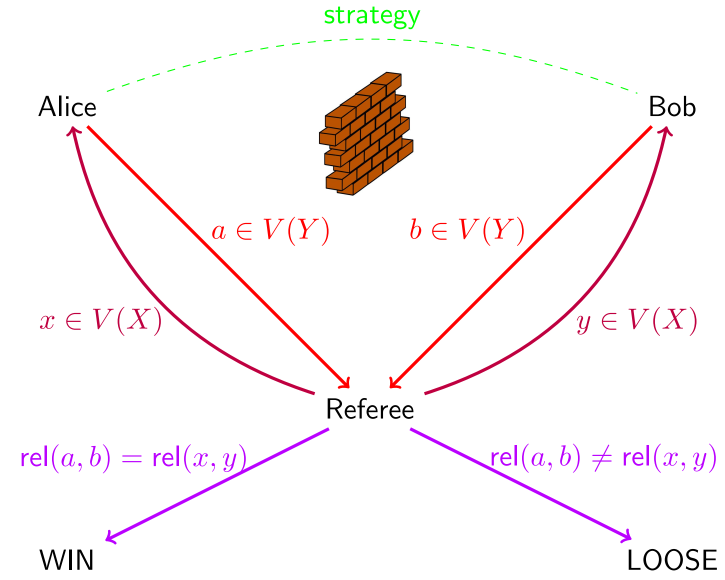
Quantum Symmetries via Quantum Information

- Suppose your friends, Alice and Bob, hand you two graphs X, Y, and claim that they are isomorphic. You'd like to verify their claim.
- One way to accomplish this is to play a **nonlocal game**, called the Graph Isomorphism Game, $\mathsf{Iso}(X, Y)$.
  1. You are the referee, Alice and Bob are the players, and they cooperate to win each round of the game.
  2. During each round, the referee randomly samples a pair of vertices $(x, y) \in V(X) \times V(X)$, and sends x to Alice and y to Bob. Alice and Bob then return vertices $a \in V(Y)$ and $b \in V(Y)$, respectively.
  3. Alice and Bob win the round if $\mathsf{rel}_X(x, y) = \mathsf{rel}_Y(a, b)$, where

$$\mathsf{rel}_X(x,y) = \begin{cases} 1, & (x,y) \in E(X) \\ 0, & x = y \\ -1, & (x,y) \notin E(X) \end{cases}.$$

  4. **Nonlocality Assumption**: During play, Alice and Bob are spatially separated and can't communicate with each other!

Schematic for a round of $\mathsf{Iso}(X, Y)$



Winning Strategies for Iso(X, Y)

- As the referee, you observe Alice and Bob's behavior via their joint input-output correlations:

$$p(a, b|x, y) = \text{“}\mathbb{P}(\text{Alice and Bob return } (a, b) \text{ given } (x, y))\text{”}$$

- You'd be confident that X and Y are isomorphic if Alice and Bob win every round of the game with probability 1:

$$p(a, b|x, y) = 0 \quad \text{whenever} \quad \mathrm{rel}_X(x, y) \neq \mathrm{rel}_Y(a, b).$$

- Such a correlation $[p(a, b|x, y)]_{a,b,x,y}$ is called a winning strategy for Iso(X, Y).
- **Example**: Alice and Bob can fix an isomorphism $\varphi : X \to Y$, and agree to use φ each round to supply answers to the referee:

$$p(a, b|x, y) = \delta_{a,\varphi(x)}\delta_{b,\varphi(y)}.$$

  This is a deterministic winning strategy.

Winning Strategies for Iso(X, Y)

- **Example**: More generally, before each round, Alice and Bob could jointly sample an isomorphism $\varphi : X \to Y$ according to some probability distribution $\mathbb{P}$:

$$p(a, b|x, y) = \sum_{\varphi} \mathbb{P}(\varphi)\delta_{a,\varphi(x)}\delta_{b,\varphi(y)} = \mathbb{P}(\varphi|\varphi(x) = a,\ \varphi(y) = b).$$

- The above strategies are often referred to as "classical strategies."
- **Questions**: What is the most general form of a winning strategy for Iso(X, Y)? Does a winning strategy for Iso(X, Y) *really* imply that the graphs are isomorphic?

Using Quantum Mechanics to Win

- Our physical world is described by the laws of quantum mechanics!
- This means that Alice and Bob can play the game $\mathrm{Iso}(X, Y)$ by performing measurements on quantum systems.
- Mathematically, a quantum system is given by a Hilbert space H. The state of the quantum system H is described by a unit vector $|\psi\rangle \in H$. Measurements of the state $|\psi\rangle \in H$ are described by operators on H: A (projective) measurement with n outcomes is given by a family of self-adjoint projections

$$(P_a)_{a=1}^n \subset B(H) \quad \text{such that} \quad \sum_a P_a = 1.$$

The probability of measuring the state $|\psi\rangle$ with outcome a is given by

$$p(a) = \langle\psi|P_a|\psi\rangle.$$

Quantum Strategies for Iso(X, Y)

In the graph isomorphism game Iso(X, Y), Alice and Bob can devise a quantum strategy as follows.

- Before each round, prepare a joint quantum system $H = H_A \otimes H_B$ in state $|\psi\rangle \in H_A \otimes H_B$. ‘
- Since Alice and Bob are spatially separated and cannot communicate, Alice's equipment can only perform local measurements on her half of the system H_A. Similarly Bob's measurements act on H_B.
- A quantum strategy for Iso(X, Y) is given by $(H_A \otimes H_B, \psi)$ and a choice of local measurement systems

  $$(P_{xa})_{a \in V(Y)} \subset B(H_A), \quad (Q_{yb})_{b \in V(Y)} \subset B(H_B) \quad \forall x, y \in V(X),$$

  with joint measurement outcomes given by

  $$p(a, b|x, y) = \langle\psi|P_{xa} \otimes Q_{yb}|\psi\rangle.$$

Quantum Strategies for Iso(X, Y)

- Physical experiments (aka "Bell tests") tell us that it is possible for Alice and Bob to better correlate their outputs if they perform measurements on a shared entangled quantum state $|\psi\rangle \in H_A \otimes H_B$.
- $|\psi\rangle \in H_A \otimes H_B$ is entangled if it cannot be written as a product vector $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$.

  Example: Bell state/EPR pair: $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle\big)$.

Theorem (Atserias et al '16)

There exist pairs of non-isomorphic graphs X, Y for which there exists a winning quantum strategy $(H, |\psi\rangle, (P_{xa}), (Q_{yb}))$ for Iso(X, Y).

- The pair of graphs X, Y above are called quantum isomorphic, and we write $X \cong_q Y$.

Quantum Pseudo-Telepathy

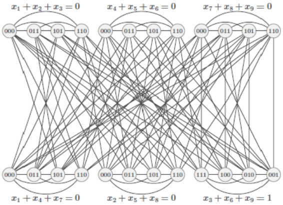
- In the above scenario, Alice and Bob (without communicating with each other!) can use quantum mechanics to trick you into believing that a pair of graphs is isomorphic when it is not.
- This is an instance of a "pseudo-telepathy" game: A nonlocal game with a winning quantum strategy, but no winning classical strategy.
- The fact that Alice and Bob can fool us is actually good news! In quantum computation pseudo-telepathy games provide physical models in which can experimentally verify the advantages of certain quantum algorithms over classical ones.
- These games are also useful for certifying entanglement (self-testing quantum states).

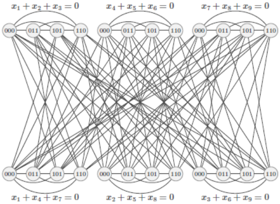
An Example: The Magic Square Graphs

- Consider the Mermin-Perez Magic Square:

x_1	x_2	x_3	0
x_4	x_5	x_6	0
x_7	x_8	x_9	0
0	0	1	

- It's impossible to globally fill this table with $x_i \in \{0, 1\}$ so that row sums and column sums are as shown. But this linear binary constraint system has "matrix solutions".
- Can build a pair of graphs X, Y from this data satisfying $X \cong_q Y$ but $X \ncong Y$:





Quantum Isomorphisms and Representation Theory

- Currently, the above construction using linear binary constraint systems is the only effective way to find pseudo-telepathic pairs of graphs X, Y.
- **Important Problem**: How to find more examples?
- One approach is to try and relate quantum isomorphisms $X \cong_q Y$ to the underlying **algebraic quantum symmetries** of the graphs X and Y. I.e., the quantum groups $G^+(X)$ and $G^+(Y)$ introduced earlier.
- In fact, there turns out to be a deep connection between the existence of quantum isomorphisms $X \cong_q Y$ and the (finite dimensional unitary) representation theory of the quantum groups $G^+(X)$ and $G^+(Y)$.

The tensor category of unitary representations of $G^+(X)$

Just as in the case for classical groups (e.g., $G(X)$), we can study the tensor category of finite-dimensional unitary representations of the quantum group $G^+(X)$, denoted by $\mathrm{Rep}(G^+(X))$.

Quantum Isomorphisms and Representation Theory

Let X, Y be graphs with adjacency matrices A_X, A_Y.

Theorem (B.,Chirvastu,Eifler,Harris,Paulsen,Su,Wasilewski)

The following conditions are equivalent.

1. $X \cong_q Y$
2. *The representation categories Rep$(G^+(X))$ and Rep$(G^+(Y))$ are "the same".*

More precisely, in (2) we mean that there is a **unitary monoidal equivalence** of tensor categories $F : \mathrm{Rep}(G^+(X)) \to \mathrm{Rep}(G^+(Y))$ such that

$$F(\mathbb{C}^{|V(X)|}) = \mathbb{C}^{|V(Y)|},\ F(m_X) = m_Y, F(u_X) = u_Y,\ \&\ F(A_X) = A_Y.$$

Is this categorical characterization of $X \cong_q Y$ useful? Yes!!!

Some Applications

- This shows that understanding quantum isomorphisms $X \cong_q Y$ amounts to understanding the structure of $G^+(X)$.
- The above theorem + some deep work of Slofstra work on linear BCS games $\implies$ our generic group algebra embeddings

$$\mathbb{C}\Gamma \hookrightarrow \mathcal{C}(G^+(X)).$$

- The representation categories $\mathrm{Rep}(G^+(X))$ admit a nice diagrammatic description via **simple planar graphs**. This can be exploited to planar analogue of Lovász' criterion for graph isomorphism.

A Really Beautiful Combinatorial Application

Theorem (Mančinska-Roberson '19)

Given two graphs X, Y, TFAE:

1. $X \cong_q Y$
2. *For every planar graph K,*

$$|\mathit{Hom}(K, X)| = |\mathit{Hom}(K, Y)|$$

where $\mathit{Hom}(K, Z)$ is the set of graph homomorphisms $K \to Z$.

THANKS!