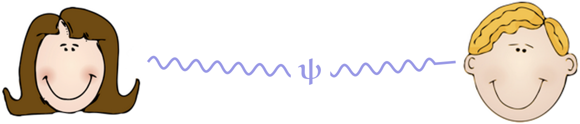
Quantum groups and nonlocal games

Laura Mančinska
QMATH, University of Copenhagen



Plan for today

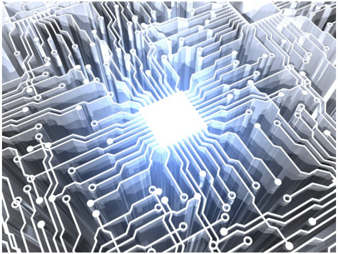
1. Motivation: quantum computing
   - What is quantum computing all about?
   - Entanglement and nonlocal games
2. Graph isomorphism games

Take-away: quantum groups arise in quantum computing via nonlocal games.

Quantum computing and information

Goal: Exploit quantum mechanical effects to process information.

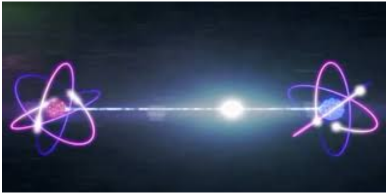
- better security guarantees
- faster algorithms
- higher communication rates, etc.



Early examples

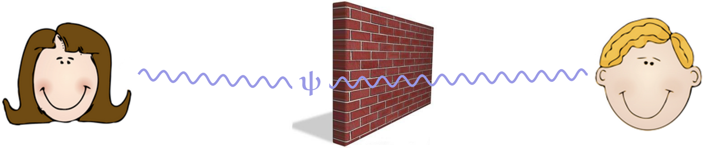
- Unconditionally secure communication channel (Bennett-Brassard'84, Ekert'91)
- Polynomial-time integer factorization (Shor'94)

What is quantum entanglement?



- Property of composite systems.
- Effects experienced by one of the parts affect the state of the other.

- Can be leveraged by **distant agents** to **correlate** their behaviors beyond classical limits.



Quantum entanglement leads to

- **improvement for communication**
  - replacing quantum communication with classical (teleportation)[1]
  - doubling the classical capacity of quantum channels[2]
  - increasing zero-error capacity of classical channels[3]
- **secure protocols** which can be run **on untrusted devices**[4]
  - private randomness generation[5]
  - certification of quantum devices[6]
- **insights to black hole dynamics**[7]

---

[1] Bennett, Brassard, Crépeau et al. *Phys. Rev. Lett.* **70**(13), 1993.
[2] Bennett, Wiesner, Phys. Rev. Lett. **69**, 1992.
[3] Leung, Mančinska, Matthews, Ozols, Roy, *Comm. Math. Phys.* **311**(1), 2012.
[4] Mayers, Yao, *FOCS'98*, 503–509.
[5] Pironio, Acín, Massar et al. *Nature* **464**(7291), 2010.
[6] Magniez, Mayers, Mosca, Ollivier, *ICALP'06*, 72–83.
[7] Hayden, Preskill, *J. High Energ. Phys.*, 2007(09):120, 2007.

Entanglement allows us to outperform classical technologies

. . . **BUT**

- entanglement-enabled strategies are often hard to understand
- we are yet to uncover the full range of advantages that entanglement can bring.

Therefore, we need to

1. develop general methods for analyzing entanglement
2. identify novel operational applications of entanglement

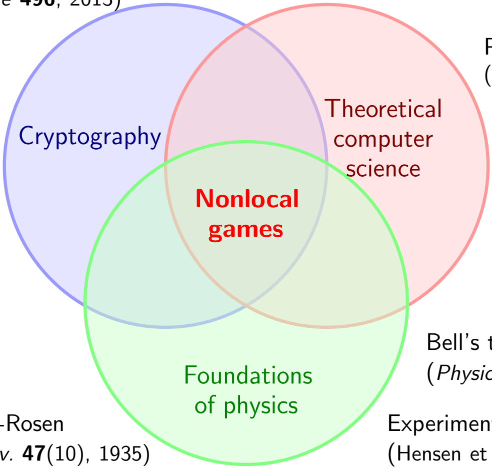
We need a versatile abstract model!

Nonlocal games are central to various fields

Protocols for untrusted devices
(Pironio et al. *Nature* **464**(7291), 2010;
Vazirani et al. *Nature* **496**, 2013)

One-round two-prover interactive
proof systems (Ben-Or et al., *STOC'88*)

PCP theorem
(Arora et al.
J. ACM **45**(3), 1998)

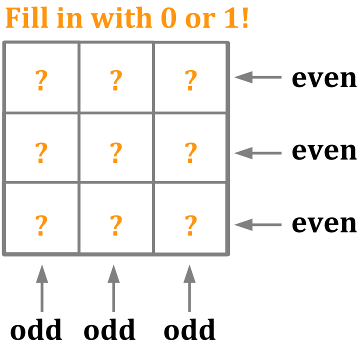


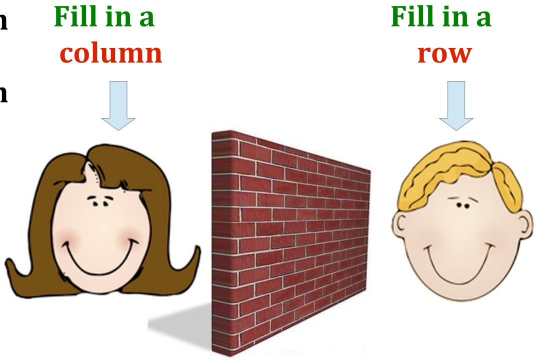
Bell's theorem
(*Physics* **1**(3), 1964)

Einstein-Podolsky-Rosen
paradox (*Phys. Rev.* **47**(10), 1935)

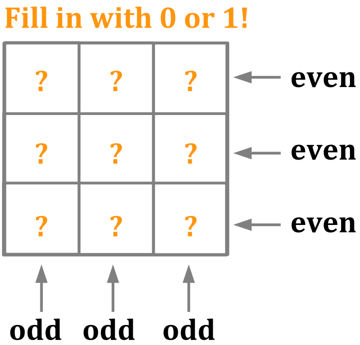
Experimental demonstration
(Hensen et al. *Nature* **526**, 2015)

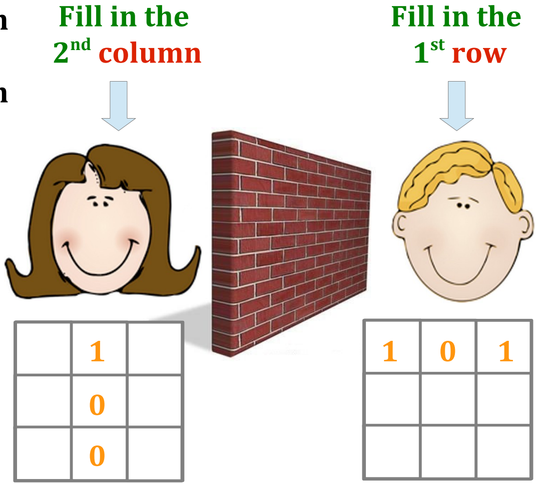
Magic square game





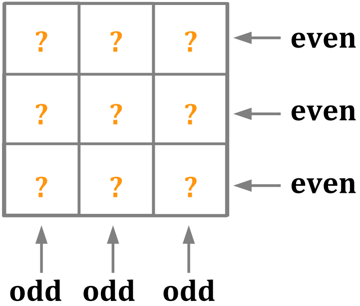
Magic square game

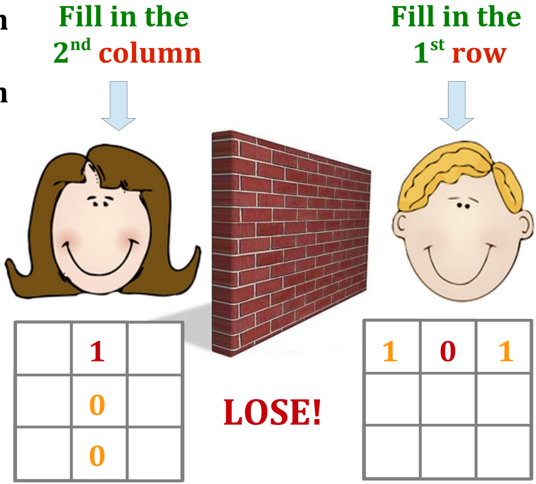




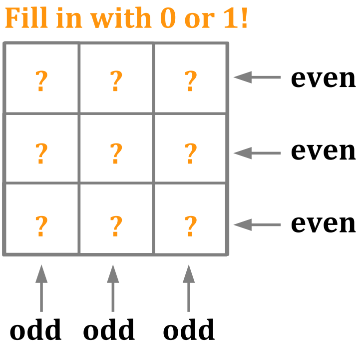
Magic square game

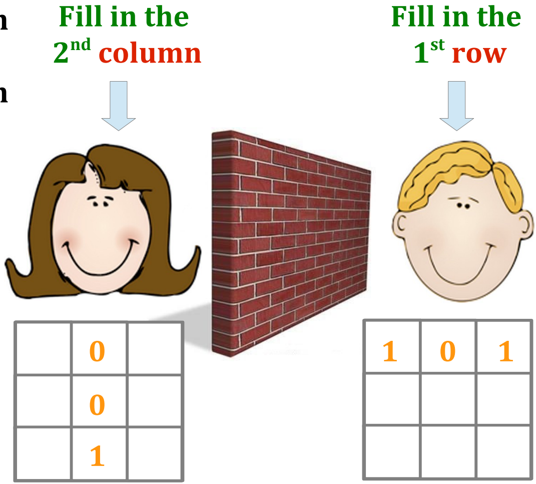
Fill in with 0 or 1!



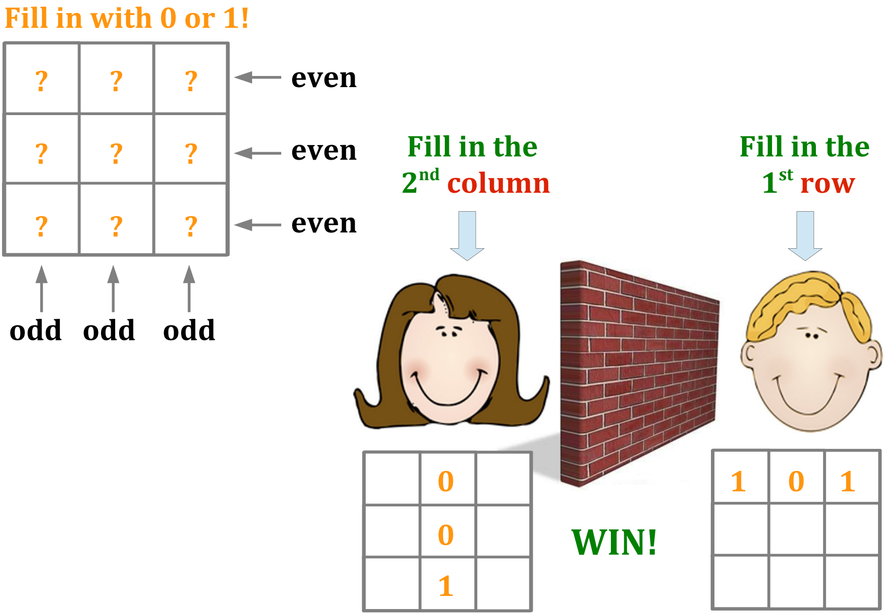


Magic square game



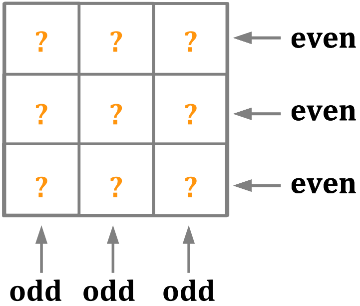


Magic square game



Magic square game

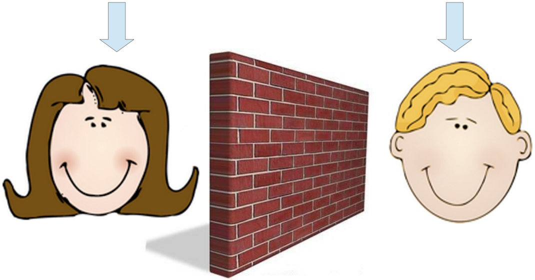
Fill in with 0 or 1!



Strategy = filling of the 3x3 grid

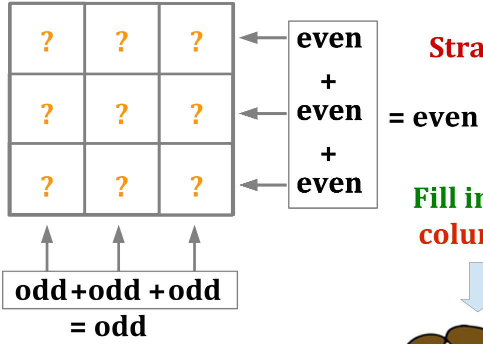
Fill in a column

Fill in a a row

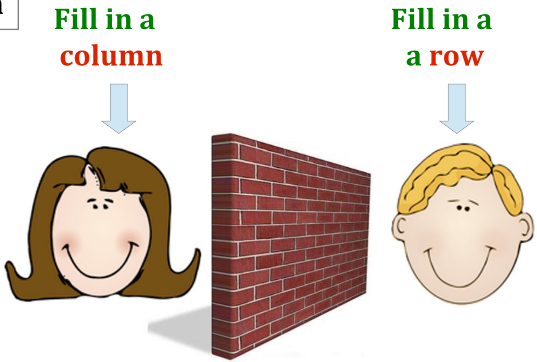


Magic square game

Fill in with 0 or 1!



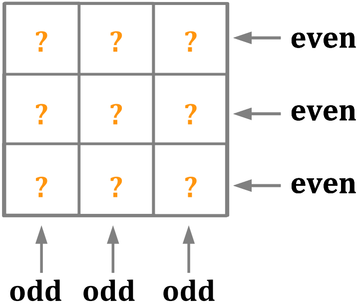
Strategy = filling of the 3x3 grid

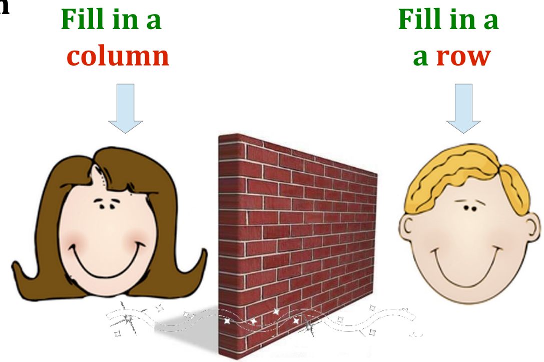


IMPOSSIBLE!

Magic square game

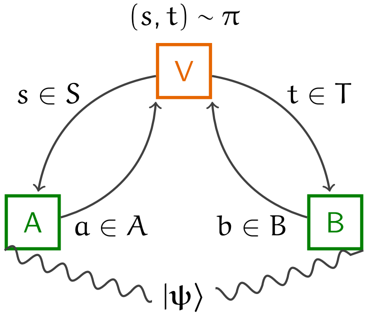
Fill in with 0 or 1!





POSSIBLE with quantum entanglement + measurements

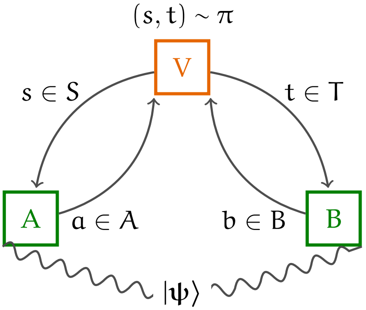
What is a nonlocal game?



lose **win**

- **verification function V** : $(a, b|s, t) \mapsto \{0, 1\}$
- **Players want to** maximize their chances of winning
  - Highest classical success probability: $\omega(\mathbf{G})$
  - Highest entangled success probability: $\omega^*(\mathbf{G})$

Nonlocal games reveal if entanglement can be useful



Operational/cryptographic task $\iff$ **Nonlocal game**

Can entanglement be helpful?
How helpful?

Is $\omega^* > \omega$?
How large is $\omega^* - \omega$?

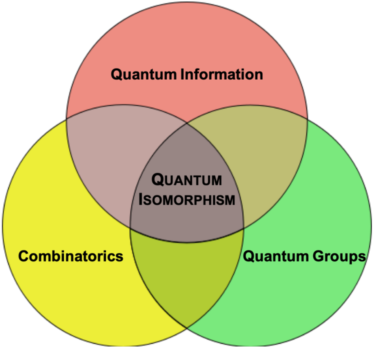
Complication: ω^* cannot be computed[1] or even approximated[2]!
How so? A: Need to optimize over states of arbitrarily high dimension.

[1] Slofstra, *Forum of Mathematics, Pi*, **vol. 7**, 2019.
[2] **MIP*=RE**. Ji, Natarjan, Vidick, Wright, Yuen. arXiv:2001.04383

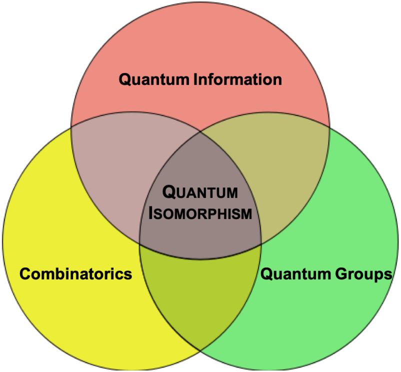
Summary so far

- **Nonlocal games** provide a general framework for studying entanglement
- **Problem:** Entanglement-assisted strategies for arbitrary nonlocal games are **hard to analyze**

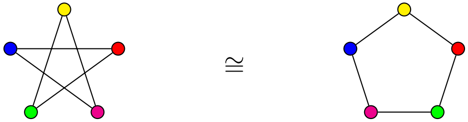
Line of attack: Focus on a **well-behaved** class of games



Quantum Isomorphisms



Graph isomorphism



A map $f : V(G) \to V(H)$ is an **isomorphism** from G to H if

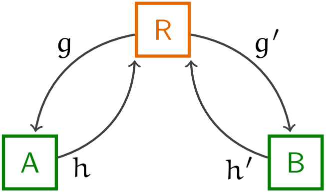
- f is a bijection and
- $g \sim g'$ if and only if $f(g) \sim f(g')$.

If such a map exists, we say that G and H are **isomorphic** and write $G \cong H$.

Matrix formulation: $PA_GP^\dagger = A_H$ for some **permutation** matrix P

(G, H)-Isomorphism Game

Intuition: Alice and Bob want to convince a referee that $G \cong H$.



- To win players must reply h, h' such that $\text{rel}(h, h') = \text{rel}(g, g')$
- No communication during game

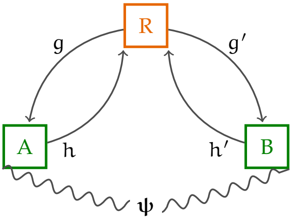
Fact. $G \cong H \Leftrightarrow$ **Classical** players can win the game with certainty

Def. (Quantum isomorphism)
We say that $G \cong_{qc} H$ if **quantum**[1] players can win the game with certainty.

[1] We work in the **commuting rather than the tensor-product model.**

Quantum commuting strategies

$G \cong_{qc} H :=$ **Quantum** players can win the (G, H)-isomorphism game

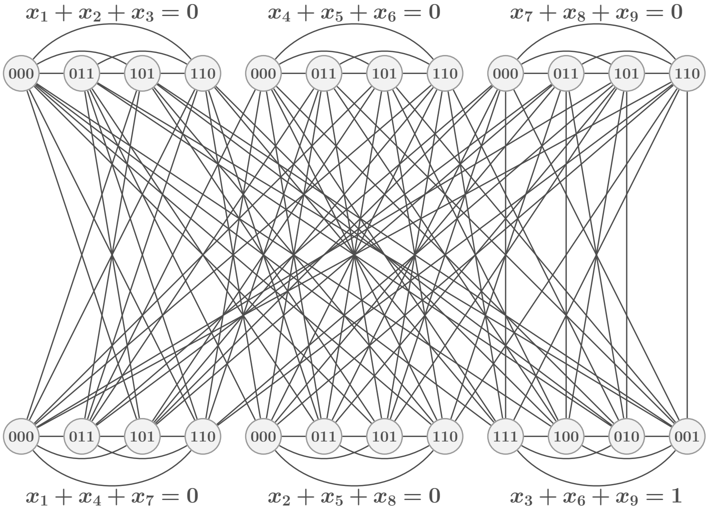


- Alice and Bob share a quantum state ψ
  ψ is a unit vector in a Hilbert space $\mathcal{H}$
- Upon receiving g, Alice performs a local measurement $\mathcal{E}_g$ to get $h \in V(H)$
  $\mathcal{E}_g = \{E_{gh} \in \mathcal{B}(\mathcal{H}) : h \in V(H)\}$ where
  $$E_{gh} \succeq 0, \quad \sum_h E_{gh} = I.$$
- Bob measures with $\mathcal{F}_{g'}$
- E_{gh} and $F_{g'h'}$ commute

The probability that players respond with h, h' on questions g, g' is

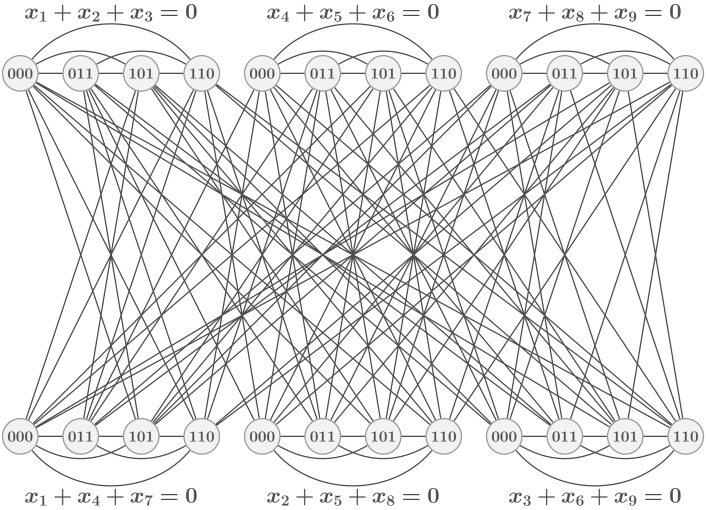
$$p(h, h'|g, g') = \langle \psi, \left(E_{gh} F_{g'h'}\right) \psi \rangle$$

Example: $G \not\cong H$ but $G \cong_{qc} H$



Construction based on reduction from linear system games.

Example: $G \not\cong H$ but $G \cong_{qc} H$



Construction based on reduction from linear system games.

Undecidability

Cor. Given two graphs G and H it is undecidable to test whether they are quantum isomorphic.

Quantum isomorphism and quantum groups
(1st characterization of $\cong_{qc}$)

Def. A matrix $\mathcal{P} = (p_{ij})$ whose entries are elements of a C^*-algebra is a **quantum permutation matrix** (QPM), if

- p_{ij} is a projection, i.e., $p_{ij}^2 = p_{ij} = p_{ij}^*$ for all i, j
- $\sum_k p_{ik} = \mathbf{1} = \sum_\ell p_{\ell j}$ for all i, j

Remark. A QPM with entries from $\mathbb{C}$ is a permutation matrix.

Thm. (Lupini, M., Roberson)

$$G \cong_{qc} H \quad \Leftrightarrow \quad \mathcal{P} A_G \mathcal{P}^\dagger = A_H \text{ for some } \textbf{quantum permutation matrix } \mathcal{P}$$

Quantum automorphism group, $\mathrm{Qut}(X)$, of a graph

Def. (Banica 2005)
$C(\mathrm{Qut}(X))$ is the universal C^*-algebra generated by elements p_{ij}, $i, j \in V(X)$, satisfying the following:

1. $\mathcal{P} = (p_{ij})$ is a quantum permutation matrix.
2. $A_X \mathcal{P} = \mathcal{P} A_X$.

The **quantum automorphism group,** $\mathrm{Qut}(X)$**, of a graph** X **is given by** $C(\mathrm{Qut}(X))$ together with the comultiplication map

$$\Delta(p_{ij}) = \sum_k p_{ik} \otimes p_{kj}$$

The matrix $\mathcal{P}$ is called the **fundamental representation** of $\mathrm{Qut}(X)$.

Orbits of $\mathrm{Qut}(X)$
(2^{nd} characterization of $\cong_{qc}$)

$\mathcal{P} = (p_{ij})$ - fundamental representation of $\mathrm{Qut}(X)$.

Def. Vertices $i, j \in V(X)$ are in the same **orbit** of $\mathrm{Qut}(X)$ if $p_{ij} \neq 0$.

Lemma. The above is an equivalence relation.

Thm. Let G and H be connected graphs.

$G \cong_{qc} H \quad \Leftrightarrow \quad$ There exist $g \in V(G)$, $h \in V(H)$ in the same orbit of $\mathrm{Qut}(G \cup H)$.

Quantum isomorphism and homomorphism counting
(3rd characterization of $\cong_{qc}$)

Thm. (M., Roberson)

$G \cong_{qc} H \quad \Leftrightarrow \quad$ graphs G and H have the same number of homomorphisms from all planar graphs.

Main component of our proof: Provide a *combinatorial description* of the **intertwiners** of $\mathrm{Qut}(G)$.

An (ℓ, k)-intertwiner T of $\mathrm{Qut}(G)$ is a $V(G)^\ell \times V(G)^k$ $\mathbb{C}$-valued matrix s.t.

$$\mathcal{P}^{\otimes \ell} T = T \mathcal{P}^{\otimes k}$$

Chassaniol 2019: Intertwiners of $\mathrm{Qut}(G) = \langle U, M, A_G \rangle_{\circ, \otimes, *, \text{lin}}$

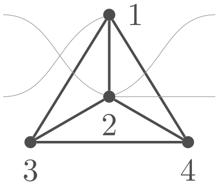
$$U = \sum_{i \in V(G)} e_i, \quad M(e_i \otimes e_j) = \delta_{ij} e_i \ \forall i, j \in V(G).$$

Bi-labeled graphs

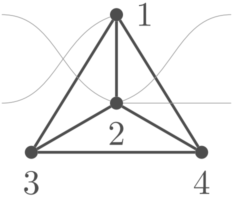
Def. (Lovász, Large Networks and Graph Limits)
An (ℓ, k)-**bi-labeled graph** is a triple $\vec{F} = (F, \vec{a}, \vec{b})$ where

- F is a graph
- $\vec{a} = (a_1, \ldots, a_\ell)$ and $\vec{b} = (b_1, \ldots, b_k)$ are tuples of vertices of F.

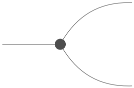
Example. $\vec{F} = \big(K_4, (2,1), (2,2)\big)$



How to draw bi-labeled graphs



$\vec{\mathsf{F}} = \big(\mathsf{K}_4, (2,1), (2,2)\big)$



$\vec{U} = \big(K_1, (1), \varnothing\big)$ $\quad \vec{M} = \big(K_1, (1), (1,1)\big)$ $\quad \vec{A} = \big(K_2, (1), (2)\big)$

Homomorphism matrices

Let G be a graph and $\vec{F} = (F, (a), (b))$ an $(1,1)$-bi-labeled graph.

Def. (G-homomorphism matrix of $\vec{F}$)
For $u, v \in V(G)$, the uv-entry of the **homomorphism matrix** $T^{\vec{F}}$ is

$$\left|\{\text{homs } \varphi : F \to G \mid \varphi(a) = u,\ \varphi(b) = v\}\right|.$$

Example. $\vec{A} = (K_2, (1), (2))$ 

$$\left(T^{\vec{A}}\right)_{u,v} = \begin{cases} 1 & \text{if } u \sim v \\ 0 & \text{otherwise} \end{cases}$$

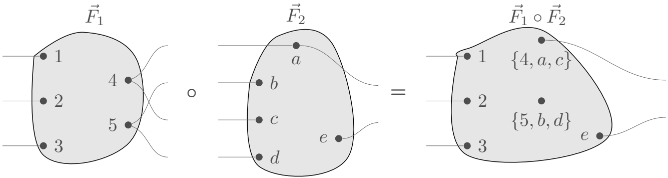
So $T^{\vec{A}} = A_G$. Similarly, $T^{\vec{U}} = U$, $\quad T^{\vec{M}} = M$.

Operations on bi-labeled graphs: Products

Thm. For a graph G and bi-labeled graphs $\vec{F}_1, \vec{F}_2$,

$$T^{\vec{F}_1} T^{\vec{F}_2} = T^{\vec{F}_1 \circ \vec{F}_2},$$

where $\vec{F}_1 \circ \vec{F}_2$ is defined as

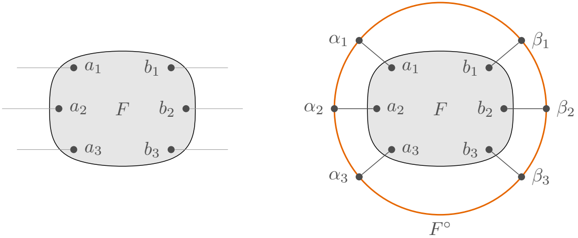


Planar bi-labeled graphs

Recall: Intertwiners of $\mathrm{Qut}(G) = \langle \mathcal{U}, \mathcal{M}, \mathcal{A}_G \rangle_{\circ,\otimes,*,\text{lin}}$

So we want to know what bi-labeled graphs are in $\langle \vec{\mathcal{U}}, \vec{\mathcal{M}}, \vec{\mathcal{A}} \rangle_{\circ,\otimes,*}$.

Def.

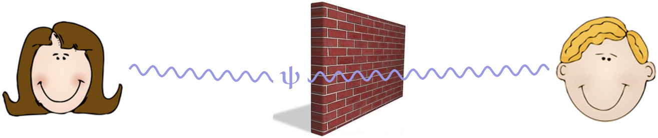


$\mathcal{P} = \{\vec{F} : F^\circ$ has planar embedding w/ **enveloping cycle** bounding outer face$\}$

Thm. (informal) Intertwiners of $\mathrm{Qut}(G)$ are given by the span of homomorphism matrices of planar bi-labeled graphs.

Summary

- Entanglement can be harnessed for operational and cryptographic tasks.
- Nonlocal games provide a mathematical framework for studying entanglement



- $G \cong_{qc} H :=$ **Quantum** players can win the isomorphism game

Quantum isomorphisms and quantum groups:

- **Thm.** $G \cong_{qc} H \quad \Leftrightarrow \quad \mathcal{P} A_G \mathcal{P}^\dagger = A_H$ for some **quantum permutation matrix** $\mathcal{P}$
- **Thm.** $G \cong_{qc} H \quad \Leftrightarrow \quad$ There exist $g \in V(G)$, $h \in V(H)$ in the same orbit of $\mathrm{Qut}(G \cup H)$
- **Thm.** $G \cong_{qc} H \quad \Leftrightarrow \quad \hom(F, G) = \hom(F, H)$ for all **planar** F

Thank you!