# Tsirelson's problem and linear system games

William Slofstra

IQC, University of Waterloo

January 20th, 2017

includes joint work with Richard Cleve and Li Liu

# A speculative question

Conventional wisdom: Finite time / volume / energy / etc. $\Longrightarrow$ can always describe nature by finite-dimensional Hilbert spaces

## A speculative question

Conventional wisdom: Finite time / volume / energy / etc. $\implies$ can always describe nature by finite-dimensional Hilbert spaces

But... many models in quantum mechanics and quantum field theory require infinite-dimensional Hilbert spaces (e.g. CCR)

Could nature be "intrinsically" infinite-dimensional?

## A speculative question

Conventional wisdom: Finite time / volume / energy / etc. $\Longrightarrow$ can always describe nature by finite-dimensional Hilbert spaces

But... many models in quantum mechanics and quantum field theory require infinite-dimensional Hilbert spaces (e.g. CCR)

Could nature be "intrinsically" infinite-dimensional?

Answer: Probably not

## A speculative question

Conventional wisdom: Finite time / volume / energy / etc. $\implies$ can always describe nature by finite-dimensional Hilbert spaces

But... many models in quantum mechanics and quantum field theory require infinite-dimensional Hilbert spaces (e.g. CCR)

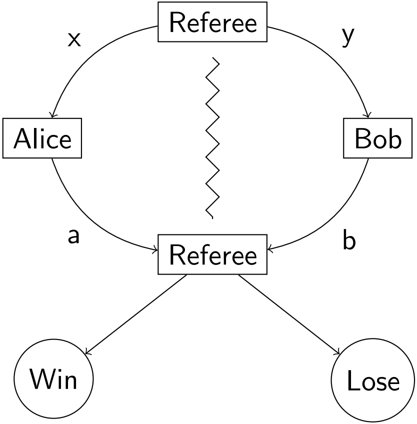
Could nature be "intrinsically" infinite-dimensional?

Answer: Probably not

But if it was... could we recognize that fact in an experiment?

(For instance, in a Bell-type experiment?)

# Non-local games (aka Bell-type experiments)



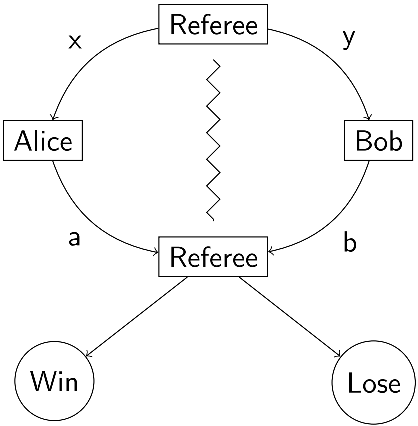

Win/lose based on outputs $a, b$ and inputs $x, y$

Alice and Bob must cooperate to win

Winning conditions known in advance

Complication: players cannot communicate while the game is in progress

# Non-local games ct'd



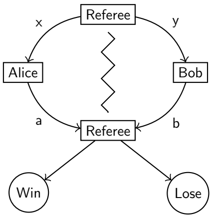

Suppose game is played many times, with inputs drawn from some public distribution $\pi$

To outside observer, Alice and Bob's strategy is described by:

$P(a, b|x, y) =$ the probability of output $(a, b)$ on input $(x, y)$

*Correlation matrix:* collection of numbers $\{P(a, b|x, y)\}$

# What can $P(a, b|x, y)$ be?




$P(a, b|x, y) =$ the probability of output $(a, b)$ on input $(x, y)$

$n$ questions, $m$ answers: $\{P(a, b|x, y)\} \subset \mathbb{R}^{m^2 n^2}$

---

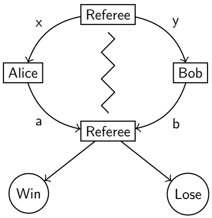
Classically

$$P(a, b|x, y) = p_a^x \cdot q_b^y$$

Probability that Alice outputs $a$ on input $x$

Same for Bob

# What can $P(a, b|x, y)$ be?




$P(a, b|x, y) =$ the probability of output $(a, b)$ on input $(x, y)$

$n$ questions, $m$ answers: $\{P(a, b|x, y)\} \subset \mathbb{R}^{m^2 n^2}$

---

<u>Classically</u>

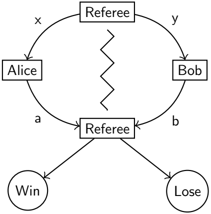
$$P(a, b|x, y) = \sum_i \lambda_i \cdot p_a^{xi} \cdot q_b^{yi}$$

Shared randomness

Probability that Alice outputs $a$ on input $x$

Same for Bob

# What can $P(a,b|x,y)$ be?




$P(a,b|x,y)$ = the probability of output $(a,b)$ on input $(x,y)$

$n$ questions, $m$ answers: $\{P(a,b|x,y)\} \subset \mathbb{R}^{m^2 n^2}$

---

Quantum

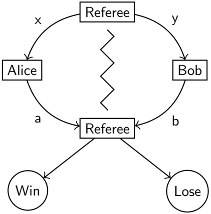
$$P(a,b|x,y) = \langle\psi| \; M_a^x \otimes N_b^y \; |\psi\rangle$$

Alice's measurement on input $x$

Bob's measurement on input $y$

shared state on $H_1 \otimes H_2$

# What can $P(a, b|x, y)$ be?




$P(a, b|x, y) =$ the probability of output $(a, b)$ on input $(x, y)$

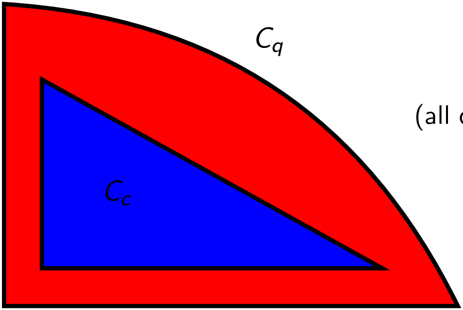
$n$ questions, $m$ answers: $\{P(a, b|x, y)\} \subset \mathbb{R}^{m^2 n^2}$

Quantum

$$P(a, b|x, y) = \langle\psi| \; M_a^x \underset{\substack{\uparrow \\ \text{tensor product}}}{\otimes} N_b^y \; |\psi\rangle$$

Why? axiom of quantum mechanics for composite systems

# Bell inequalities



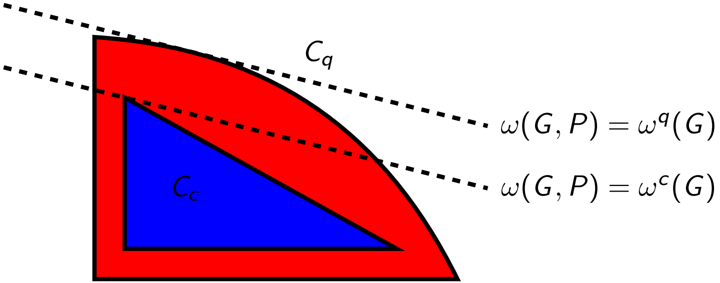

(all diagrams are schematic)

$C_c(m, n) =$ set of classical correlation matrices

$C_q(m, n) =$ set of quantum correlation matrices

Both are convex subsets of $\mathbb{R}^{m^2 n^2}$.

# Bell inequalities ct'd

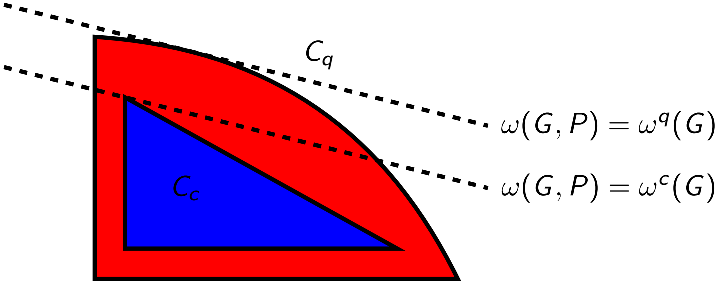



$\omega(G,P) =$ probability of winning game $G$ with correlation $P$

$\omega^c(G) =$ maximum winning probability for $P \in C_c(m,n)$

$\omega^q(G) =$ same thing but with $C_q(m,n)$

# Bell inequalities ct'd

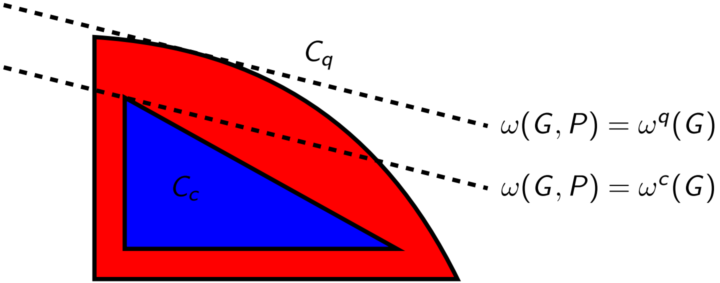



If $\omega^c(G) < \omega^q(G)$, then

(1) $C_c \subsetneq C_q$, and

(2) we can (theoretically) show this in an experiment

# Bell inequalities ct'd




If $\omega^c(G) < \omega^q(G)$, then

(1) $C_c \subsetneq C_q$, and

(2) we can (theoretically) show this in an experiment

Bell's theorem + many experiments: this happens!

# Finite versus infinite-dimensional

Quantum correlations:

$$P(a, b|x, y) = \langle\psi| M_a^x \otimes N_b^y |\psi\rangle$$

where $|\psi\rangle \in H_1 \otimes H_2$

---

# Finite versus infinite-dimensional

Quantum correlations:

$$P(a, b|x, y) = \langle\psi| M_a^x \otimes N_b^y |\psi\rangle$$

where $|\psi\rangle \in H_1 \otimes H_2$

---

Correlation set $C_q$:

$H_1$, $H_2$ must be finite-dimensional

(but, no bound on dimension)

## Finite versus infinite-dimensional

Quantum correlations:

$$P(a,b|x,y) = \langle\psi| M_a^x \otimes N_b^y |\psi\rangle$$

where $|\psi\rangle \in H_1 \otimes H_2$

---

Correlation set $C_q$:

$H_1$, $H_2$ must be finite-dimensional

(but, no bound on dimension)

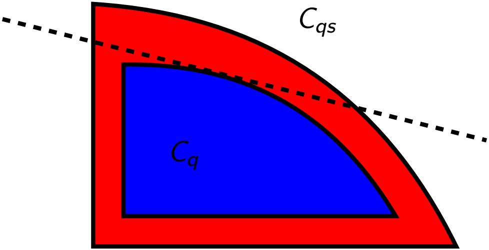
Correlation set $C_{qs}$ :

$H_1$, $H_2$ allowed to be infinite-dimensional

(the 's' stands for 'spatial tensor product')

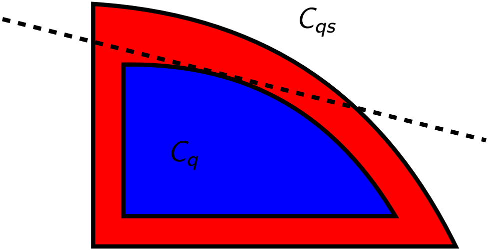
# Finite versus infinite-dimensional ct'd

Can we separate $C_q$ from $C_{qs}$ with a Bell inequality?



# Finite versus infinite-dimensional ct'd

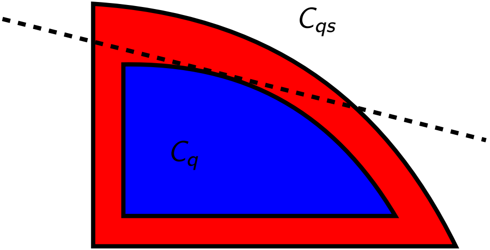
Can we separate $C_q$ from $C_{qs}$ with a Bell inequality?




NO!

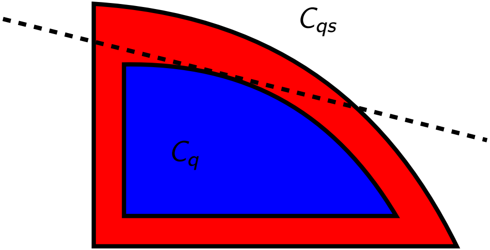
This is the wrong picture

# How is this picture wrong?




$C_q$ and $C_{qs}$ are not known to be closed.

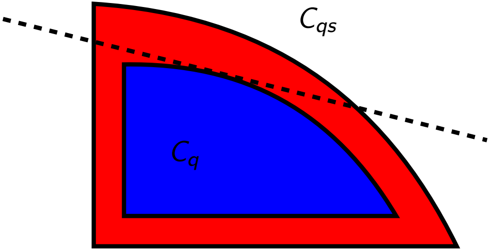
# How is this picture wrong?




$C_q$ and $C_{qs}$ are not known to be closed.

Even worse: $\overline{C_{qs}} = \overline{C_q}$

## How is this picture wrong?




$C_q$ and $C_{qs}$ are not known to be closed.

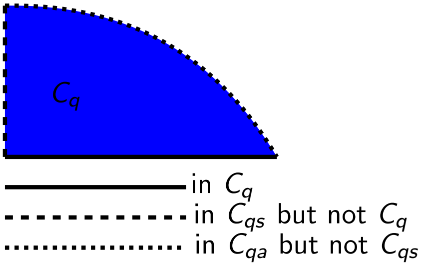
Even worse: $\overline{C_{qs}} = \overline{C_q}$

New correlation set $C_{qa} := \overline{C_q}$

contains limits of finite-dimensional correlations
indistinguishable from $C_q$ and $C_{qs}$ in experiment

# The real picture

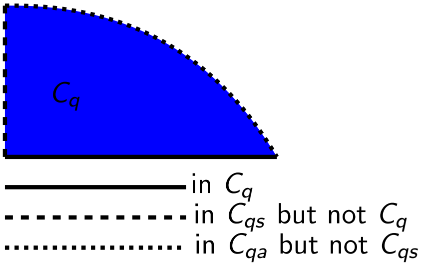
Could look like:




We know $C_q \subseteq C_{qs} \subseteq C_{qa}$ ... but nothing else!

## The real picture

Could look like:




We know $C_q \subseteq C_{qs} \subseteq C_{qa}$ ... but nothing else!

Fortunately, this is not the end of the story

We've assumed that $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$... maybe this is too restrictive

# Commuting-operator model

Another model of composite systems

Correlation set $C_{qc}$:

$$P(a, b|x, y) = \langle\psi| M_a^x \cdot N_b^y |\psi\rangle$$

where

(1) $|\psi\rangle$ belongs to a joint Hilbert space $H$ (possibly infinite-dimensional)

(2) Measurements commute: $M_a^x N_b^y = N_b^y M_a^x$ for all $x, y, a, b$

'qc' stands for 'quantum-commuting'

# What do we know about $C_{qc}$

Correlation set $C_{qc}$: $P(a,b|x,y) = \langle\psi| M_a^x \cdot N_b^y |\psi\rangle$

$C_{qc}$ is closed!

Get a hierarchy $C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{qc}$ of convex sets

## What do we know about $C_{qc}$

Correlation set $C_{qc}$: $P(a,b|x,y) = \langle\psi| M_a^x \cdot N_b^y |\psi\rangle$

$C_{qc}$ is closed!

Get a hierarchy $C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{qc}$ of convex sets

If $H$ is finite-dimensional, then $\{P(a,b|x,y)\} \in C_q$

$$\text{Can find } H_1,\ H_2 \text{ such that } H = H_1 \otimes H_2,$$

$$M_a^x \cong \widetilde{M}_a^x \otimes I \text{ and } N_b^y \cong I \otimes \widetilde{N}_b^y \text{ for all } x, y, a, b$$

This argument doesn't work if $H$ is infinite-dimensional

# Tsirelson's problem(s)

strong

$$\underbrace{C_q \subseteq C_{qs} \subseteq C_{qa}}_{\text{tensor product}} \subseteq C_{qc}$$

weak

commuting operator

Tsirelson problems: is $C_t$, $t \in \{q, qs, qa\}$ equal to $C_{qc}$

# Tsirelson's problem(s)

$$\overbrace{\underbrace{C_q \subseteq C_{qs} \subseteq C_{qa}}_{\text{tensor product}} \subseteq C_{qc}}^{\text{strong}}$$

weak

commuting operator

Tsirelson problems: is $C_t$, $t \in \{q, qs, qa\}$ equal to $C_{qc}$

These are fundamental questions

1. Comparing two axiom systems:

   Strong Tsirelson: is $C_q = C_{qc}$?

# Tsirelson's problem(s)

$$\overbrace{\underbrace{C_q \subseteq C_{qs} \subseteq C_{qa}}_{\text{tensor product}} \subseteq C_{qc}}^{\text{strong}}$$

weak

commuting operator

Tsirelson problems: is $C_t$, $t \in \{q, qs, qa\}$ equal to $C_{qc}$

These are fundamental questions

1. Comparing two axiom systems:

   Strong Tsirelson: is $C_q = C_{qc}$?

2. Is $\omega^q(G) < \omega^{qc}(G)$ for any game?

   Equivalent to weak Tsirelson: is $C_{qa} = C_{qc}$?

# What do we know?

strong

$$C_q \quad \subseteq \quad C_{qs} \quad \subseteq \quad C_{qa} \quad \subseteq \quad C_{qc}$$

weak

**Theorem (Ozawa, JNPPSW, Fr)**

$C_{qa} = C_{qc}$ *if and only if Connes' embedding problem is true*

# What do we know?

strong

$$C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{qc}$$

weak

**Theorem (Ozawa, JNPPSW, Fr)**

*$C_{qa} = C_{qc}$ if and only if Connes' embedding problem is true*

**Theorem (S)**

$C_{qs} \neq C_{qc}$

# Other fundamental questions

1. Resource question:

   A non-local game $G$ is a computational task

   Bell's theorem: can do better with entanglement

   Can $G$ be played optimally with finite Hilbert space dimension?

   Yes $\iff$ $C_q = C_{qa}$ (in other words, is $C_q$ closed?)

   Variants of games: finite dimensions do not suffice [LTW13],[MV14],[RV15]

# Other fundamental questions

1. Resource question:

   A non-local game $G$ is a computational task

   Bell's theorem: can do better with entanglement

   Can $G$ be played optimally with finite Hilbert space dimension?

   Yes $\iff$ $C_q = C_{qa}$ (in other words, is $C_q$ closed?)

   Variants of games: finite dimensions do not suffice [LTW13],[MV14],[RV15]

2. Can we compute $\omega^q(G)$ or $\omega^{qc}(G)$?

   (what is the power of $MIP^*$?)

# What do we know?

Question: can we compute $\omega^q(G)$ or $\omega^{qc}(G)$?

# What do we know?

Question: can we compute $\omega^q(G)$ or $\omega^{qc}(G)$?

Brute force search through strategies on $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^n$, converges to $\omega^q$ (from below)

Navascués, Pironio, Acín: Given a non-local game, there is a hierarchy of SDPs which converge in value to $\omega^{qc}$ (from above)

# What do we know?

Question: can we compute $\omega^{q}(G)$ or $\omega^{qc}(G)$?

Brute force search through strategies on $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^n$, converges to $\omega^q$ (from below)

Navascués, Pironio, Acín: Given a non-local game, there is a hierarchy of SDPs which converge in value to $\omega^{qc}$ (from above)

In both cases, no way to tell how close we are to the correct answer

# What do we know?

Question: can we compute $\omega^q(G)$ or $\omega^{qc}(G)$?

Brute force search through strategies on $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^n$, converges to $\omega^q$ (from below)

Navascués, Pironio, Acín: Given a non-local game, there is a hierarchy of SDPs which converge in value to $\omega^{qc}$ (from above)

In both cases, no way to tell how close we are to the correct answer

**Theorem (S)**

*It is undecidable to tell if* $\omega^{qc} < 1$

# What do we know?

Question: can we compute $\omega^q(G)$ or $\omega^{qc}(G)$?

Brute force search through strategies on $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^n$, converges to $\omega^q$ (from below)

Navascués, Pironio, Acín: Given a non-local game, there is a hierarchy of SDPs which converge in value to $\omega^{qc}$ (from above)

In both cases, no way to tell how close we are to the correct answer

**Theorem (S)**

*It is undecidable to tell if* $\omega^{qc} < 1$

General cases of other questions completely open!

# Undecidability

**Theorem (S)**

*It is undecidable to tell if* $\omega^{qc} < 1$

# Undecidability

**Theorem (S)**

*It is undecidable to tell if* $\omega^{qc} < 1$

NPA hierarchy: there is no computable function

$$L : \text{ Games } \to \mathbb{N}$$

such that $\omega^{qc}(G) = L(G)$th level of NPA hierarchy

## Undecidability

**Theorem (S)**

*It is undecidable to tell if $\omega^{qc} < 1$*

NPA hierarchy: there is no computable function

$$L : \text{ Games } \rightarrow \mathbb{N}$$

such that $\omega^{qc}(G) = L(G)$th level of NPA hierarchy

We still don't know: can we compute $\omega^{qc}(G)$ to within some given error?

(Ji '16: this problem is $MIP^*$-complete)

If weak Tsirelson is true, then $\omega^{qc}$ *is* computable in this stronger sense

# Undecidability comes from exact error?

Comparison point: Can decide if optimal value of finite SDP is $< 1$ (very inefficient algorithm)

# Undecidability comes from exact error?

Comparison point: Can decide if optimal value of finite SDP is $< 1$ (very inefficient algorithm)

More generally: first-order logic for field of real numbers is decidable

Contrast: first-order logic for integers and rationals is undecidable

# Undecidability comes from exact error?

Comparison point: Can decide if optimal value of finite SDP is $< 1$ (very inefficient algorithm)

More generally: first-order logic for field of real numbers is decidable

Contrast: first-order logic for integers and rationals is undecidable

Consequence of undecidability of $\omega^{qc} < 1$ due to Tobias Fritz:

> quantum logic (first order theory for projections on Hilbert spaces) is undecidable

# Quantum logic is undecidable

## Theorem (Tobias Fritz)

*The following problem is undecidable:*
*Given* $n \geq 1$ *and a collection of subsets* $\mathcal{C}$ *of* $\{1, \ldots, n\}$, *determine if there are self-adjoint projections* $P_1, \ldots, P_n$ *such that*

$$\sum_{i \in S} P_i = I, \quad P_i P_j = P_j P_i = 0 \text{ if } i \neq j \in S$$

*for all* $S \in \mathcal{C}$.

Proof: follows from undecidability of $\omega^{qc} < 1$

Builds on Acín-Fritz-Leverrier-Sainz '15.

# Two theorems

**Theorem (S)**

$C_{qs} \neq C_{qc}$

**Theorem (S)**

*It is undecidable to tell if* $\omega_{qc} < 1$

Theorems look very different...

# Two theorems

**Theorem (S)**

$C_{qs} \neq C_{qc}$

**Theorem (S)**

*It is undecidable to tell if* $\omega_{qc} < 1$

Theorems look very different...

But: proof follows from a single theorem in group theory

Connection with group theory comes from linear system games

# Linear system games

Start with $m \times n$ linear system $Ax = b$ over $\mathbb{Z}_2$

# Linear system games

Start with $m \times n$ linear system $Ax = b$ over $\mathbb{Z}_2$

Inputs:

- Alice receives $1 \leq i \leq m$ (an equation)
- Bob receives $1 \leq j \leq n$ (a variable)

# Linear system games

Start with $m \times n$ linear system $Ax = b$ over $\mathbb{Z}_2$

Inputs:

- Alice receives $1 \leq i \leq m$ (an equation)
- Bob receives $1 \leq j \leq n$ (a variable)

Outputs:

- Alice outputs an assignment $a_k$ for all variables $x_k$ with $A_{ik} \neq 0$
- Bob outputs an assignment $b_j$ for $x_j$

## Linear system games

Start with $m \times n$ linear system $Ax = b$ over $\mathbb{Z}_2$

Inputs:

- Alice receives $1 \leq i \leq m$ (an equation)
- Bob receives $1 \leq j \leq n$ (a variable)

Outputs:

- Alice outputs an assignment $a_k$ for all variables $x_k$ with $A_{ik} \neq 0$
- Bob outputs an assignment $b_j$ for $x_j$

They win if:

- $A_{ij} = 0$ (assignment irrelevant) or
- $A_{ij} \neq 0$ and $a_j = b_j$ (assignment consistent)

## Linear system games

Start with $m \times n$ linear system $Ax = b$ over $\mathbb{Z}_2$

Inputs:

- Alice receives $1 \leq i \leq m$ (an equation)
- Bob receives $1 \leq j \leq n$ (a variable)

Outputs:

- Alice outputs an assignment $a_k$ for all variables $x_k$ with $A_{ik} \neq 0$
- Bob outputs an assignment $b_j$ for $x_j$

They win if:

- $A_{ij} = 0$ (assignment irrelevant) or
- $A_{ij} \neq 0$ and $a_j = b_j$ (assignment consistent)

Such games go back to Mermin-Peres magic square, more recently studied by Cleve-Mittal, Ji, Arkhipov

# Quantum solutions of $Ax = b$

Observables $X_j$ such that

1. $X_j^2 = I$ for all $j$
2. $\prod_{j=1}^{n} X_j^{A_{ij}} = (-I)^{b_i}$ for all $i$
3. If $A_{ij}, A_{ik} \neq 0$, then $X_j X_k = X_k X_j$

(We've written linear equations multiplicatively)

# Quantum solutions of $Ax = b$

Observables $X_j$ such that

1. $X_j^2 = I$ for all $j$
2. $\prod_{j=1}^{n} X_j^{A_{ij}} = (-I)^{b_i}$ for all $i$
3. If $A_{ij}, A_{ik} \neq 0$, then $X_j X_k = X_k X_j$

(We've written linear equations multiplicatively)

**Theorem (Cleve-Mittal,Cleve-Liu-S)**

*Let $G$ be the game for linear system $Ax = b$. Then:*

- *$G$ has a perfect strategy in $C_{qs}$ if and only if $Ax = b$ has a finite-dimensional quantum solution*
- *$G$ has a perfect strategy in $C_{qc}$ if and only if $Ax = b$ has a quantum solution*

## Group theory ct'd

The *solution group* $\Gamma$ of $Ax = b$ is the group generated by $X_1, \ldots, X_n, J$ such that

1. $X_j^2 = [X_j, J] = J^2 = e$ for all $j$
2. $\prod_{j=1}^{n} X_j^{A_{ij}} = J^{b_i}$ for all $i$
3. If $A_{ij}, A_{ik} \neq 0$, then $[X_j, X_k] = e$

where $[a, b] = aba^{-1}b^{-1}$, $e =$ group identity

**Theorem (Cleve-Mittal,Cleve-Liu-S)**

*Let $G$ be the game for linear system $Ax = b$. Then:*

- *$G$ has a perfect strategy in $C_{qs}$ if and only if $\Gamma$ has a finite-dimensional representation with $J \neq I$*
- *$G$ has a perfect strategy in $C_{qc}$ if and only if $J \neq e$ in $\Gamma$*

# Groups and local compatibility

Suppose we can write down any group relations we want...

But: generators in the relation will be forced to commute!

# Groups and local compatibility

Suppose we can write down any group relations we want...

But: generators in the relation will be forced to commute!

Call this condition *local compatibility*

Local compatibility is (a priori) a very strong constraint

# Groups and local compatibility

Suppose we can write down any group relations we want...

But: generators in the relation will be forced to commute!

Call this condition *local compatibility*

Local compatibility is (a priori) a very strong constraint

For instance, $S_3$ is generated by $a, b$ subject to the relations

$$a^2 = b^2 = e, (ab)^3 = e$$

If $ab = ba$, then $(ab)^3 = a^3 b^3 = ab$

So relations imply $a = b$, and $S_3$ becomes $\mathbb{Z}_2$

## Group embedding theorem

Solution groups satisfy local compatibility

Nonetheless:

Solution groups are as complicated as general groups

**Theorem (S)**

*Let $G$ be any finitely-presented group, and suppose we are given $J_0$ in the center of $G$ such that $J_0^2 = e$.*

*Then there is an injective homomorphism $\phi : G \hookrightarrow \Gamma$, where $\Gamma$ is the solution group of a linear system $Ax = b$, with $\phi(J_0) = J$.*

## How do we prove the embedding theorem?

Linear system $Ax = b$ over $\mathbb{Z}_2$ equivalent to labelled hypergraph:

Edges are variables

Vertices are equations

$v$ is adjacent to $e$ if and only if $A_{ve} \neq 0$

$v$ is labelled by $b_i \in \mathbb{Z}_2$

# How do we prove the embedding theorem?

Linear system $Ax = b$ over $\mathbb{Z}_2$ equivalent to labelled hypergraph:

Edges are variables

Vertices are equations

$v$ is adjacent to $e$ if and only if $A_{ve} \neq 0$

$v$ is labelled by $b_i \in \mathbb{Z}_2$

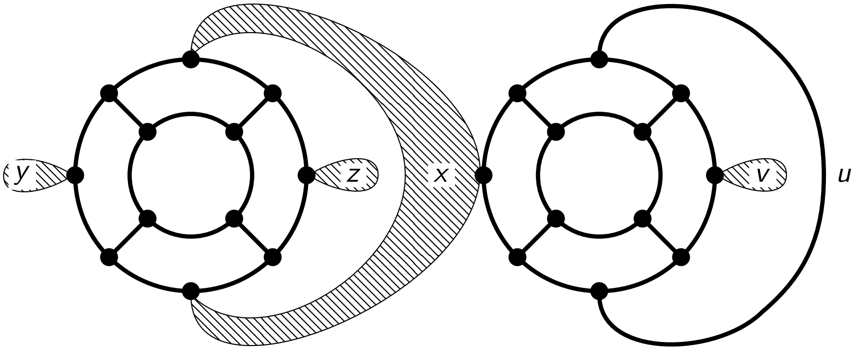
---

Given finitely-presented group $G$, we get $\Gamma$ from a linear system

But what linear system?

Can answer this pictorially by writing down a hypergraph?

# The hypergraph by example




$$\langle x, y, z, u, v : xyxz = xuvu = e = x^2 = y^2 = \cdots = v^2 \rangle$$

# Further directions

1. Further refinements to address $C_q$ vs $C_{qa}$
2. Is $\omega^q(G) < 1$ decidable?

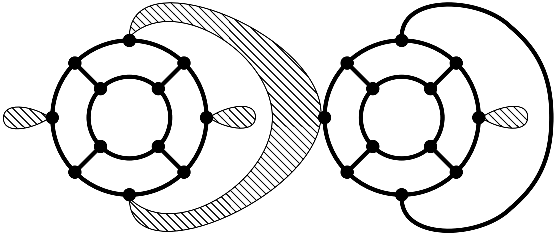
# Further directions

1. Further refinements to address $C_q$ vs $C_{qa}$
2. Is $\omega^q(G) < 1$ decidable?
3. Embedding theorem: for any f.p. group $G$, get a non-local game such that Alice and Bob are forced to use $G$ to play perfectly

   (Caveat: but might need to use infinite-dimensional commuting-operator strategy to achieve this)

   Applications to self-testing / device independent protocols?

# The end



$$\langle x, y, z, u, v : xyxz = xuvu = e = x^2 = y^2 = \cdots = v^2 \rangle$$

Thank-you!

# Extra slide: Higman's group

$$G = \langle a, b, c, d : aba^{-1} = b^2, bcb^{-1} = c^2, cdc^{-1} = d^2, dad^{-1} = a^2$$

Only finite-dimensional representation is the trivial representation

On the other hand, $a, b, c, d$ are all non-trivial in $G$