Quantum entanglement, Tsirelson's problem, and group theory

William Slofstra

University of Waterloo

April 4th, 2018

Finite-dimensional models... of groups

$G = \langle x_1, \ldots, x_n : r_1, \ldots, r_m \rangle$, a finitely presented group

Finite-dimensional model of G:

complex matrices $X_1, \ldots, X_n$ such that

$r_i(X_1, \ldots, X_n) = 1$ for $1 \leq i \leq m$

a.k.a.

a finite-dimensional representation $G \to \mathrm{GL}(\mathbb{C}^d)$

Question: when can we recover G from its finite-dimensional models?

Question: when can we recover G from its finite-dimensional models?

- G is *linear*: a subgroup of $\mathrm{GL}(\mathbb{C}^d)$ for some d
- G is *residually finite-dimensional (RFD)*: for every $w \in G \setminus \{e\}$, there is a finite-dimensional representation ϕ with $\phi(w) \neq 1$.

Question: when can we recover G from its finite-dimensional models?

- G is *linear*: a subgroup of $\mathrm{GL}(\mathbb{C}^d)$ for some d

> G is *residually finite-dimensional (RFD)*: for every $w \in G \setminus \{e\}$, there is a finite-dimensional representation ϕ with $\phi(w) \neq 1$.

Residually finite-dimensional groups

> G is *residually finite-dimensional (RFD)*: for every $w \in G \setminus \{e\}$, there is a finite-dimensional representation ϕ with $\phi(w) \neq 1$.

Are there non-RFD groups?

Residually finite-dimensional groups

> G is *residually finite-dimensional (RFD)*: for every $w \in G \setminus \{e\}$, there is a finite-dimensional representation ϕ with $\phi(w) \neq 1$.

Are there non-RFD groups? Yes, lots...

- Baumslag-Solitar group: $BS(2,3) = \langle x, y : xy^2x^{-1} = y^3 \rangle$
- Higman's group:
  $\langle a, b, c, d : aba^{-1} = b^2, bcb^{-1} = c^2, cdc^{-1} = d^2, dad^{-1} = a^2 \rangle$
  (Higman's group has no non-trivial finite-dimensional reps)

Quantum mechanics (quantum probability)

... is a framework for working with physical systems

Axioms of quantum mechanics

- Physical systems = Hilbert space H
- State of system = unit vector $v \in H$
- Measurement:

  projections $\{P_a\}_{a \in O}$ on H with $\sum_a P_a = 1$.

  O = set of measurement outcomes

  Probability of measuring a is $v^* P_a v$
- ...

Surprising features of quantum mechanics

Uncertainty principle

Might not be able to measure two properties simultaneously

Can measure $\{M_a\}$ and $\{N_b\}$ simultaneously only if

$$M_a N_b = N_b M_a \text{ for all } a, b$$

Surprising features: contextuality

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

Problem:

assign ± 1 to $x_1, \ldots, x_9$ so that

1. product across rows is 1
2. product across columns is -1

(this is a linear system over $\mathbb{Z}_2$ with 9 variables, 6 equations)

Not possible by parity argument

Mermin-Peres magic square

Surprising features: contextuality

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

Imagine a physical system, where state of system is set, and then we measure either a row or a column

If magic square conditions are satisfied, then x_i seems to depend on whether it is measured as part of a row or column

Mermin-Peres magic square

Surprising features: contextuality

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

Quantum solution: there are unitaries $X_1, \ldots, X_9$ such that

0. $X_i^2 = 1$ for $i = 1, \ldots, 9$
1. product across rows is 1
2. product across columns is -1
3. if X_i, X_j belong to the same row or column, then $X_i X_j = X_j X_i$

Interpretation: quantum mechanics is contextual!

Mermin-Peres magic square

Quantum solutions of linear systems

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

Quantum solution:

Collection of unitaries $X_1, \ldots, X_n \in \mathcal{U}(\mathcal{H})$ such that

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

Quantum solutions of linear systems

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

Solution group of $Ax = b$

$$\Gamma(A,b) = \langle\, x_1, \ldots, x_n, J \;:\; x_j^2 = 1 = [x_j, J] = J^2 \text{ for all } j$$
$$\prod_j x_j^{A_{ij}} = J^{b_i}, i = 1, \ldots, m$$
$$[x_j, x_k] = 1 \text{ if } A_{ij}, A_{ik} \neq 0, \text{ some } i \,\rangle$$

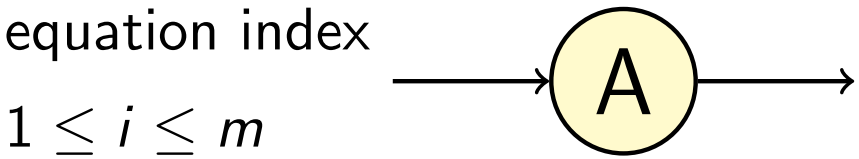
Group commutator: $[a,b] = aba^{-1}b^{-1}$

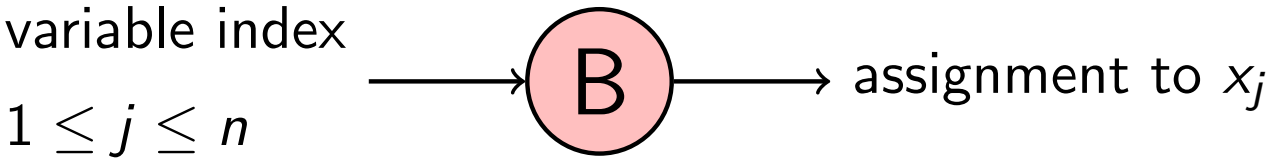
Linear system non-local games

Mermin-Peres contextuality is hard to observe in an experiment

$m \times n$ linear system $Ax = b$

$\Longrightarrow$ game with two separated players (Aravind, Cleve-Mittal)



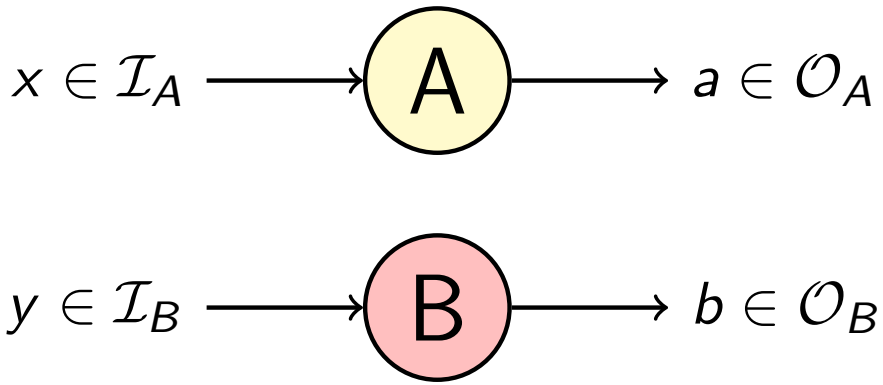


Inputs chosen at random

Players win if Alice's output is consistent with Bob's output

Non-local game

Linear system games are examples of non-local games:



Win if

$V(a, b|x, y) = 1$

Inputs chosen from $\mathcal{I}_A \times \mathcal{I}_B$ according to some distribution

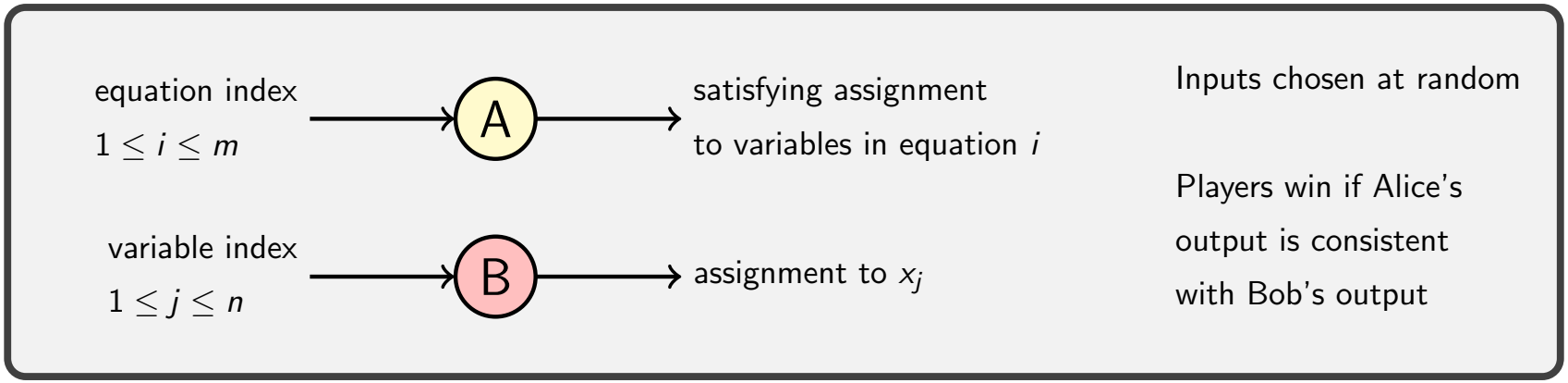
Winning condition: function $V : \mathcal{O}_A \times \mathcal{O}_B \times \mathcal{I}_A \times \mathcal{I}_B \to \{0, 1\}$

Players know rules of game, want to cooperate to win

Cannot communicate once game starts...

may not be able to play perfectly

Linear system non-local games: classical strategies



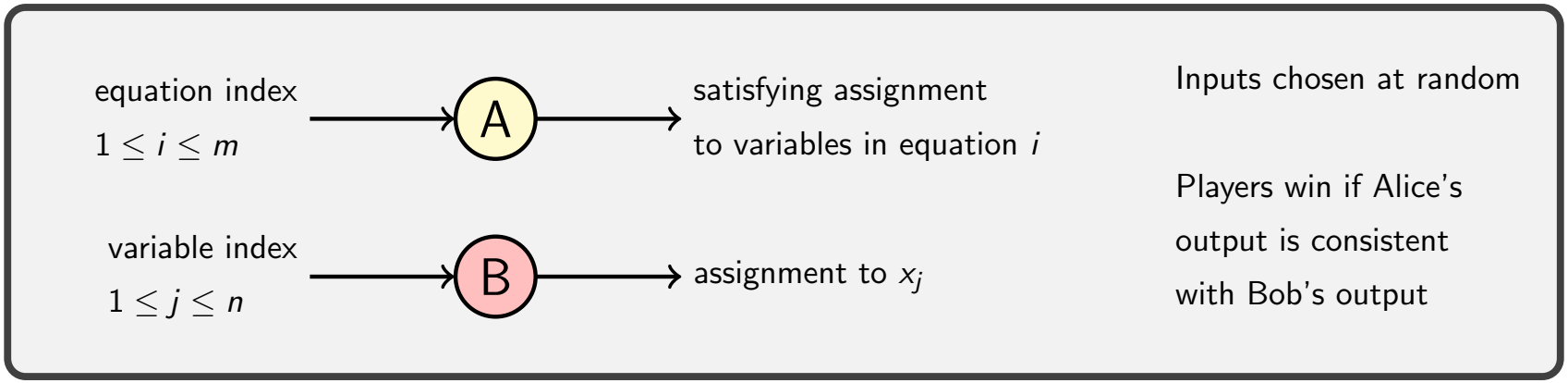
Classical strategies (deterministic or shared randomness):

Optimal strategy achieved by a deterministic strategy

Players can play perfectly if and only if $Ax = b$ has a solution

(Otherwise optimal strategy has success probability $p < 1$)

Linear system non-local games: quantum strategies



Theorem (Cleve-Mittal)

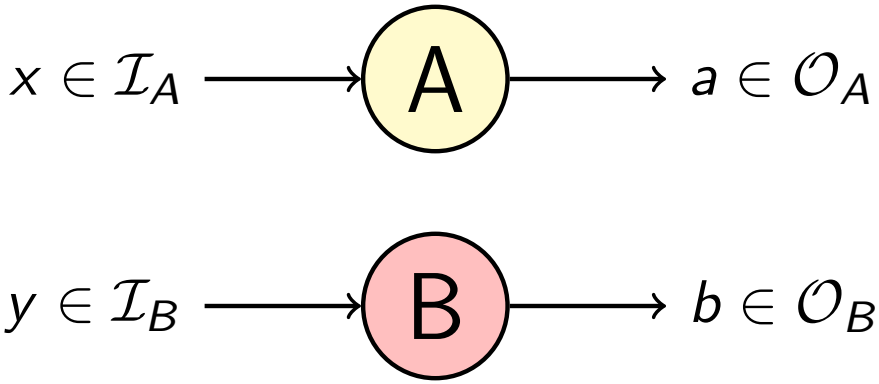
The game associated to $Ax = b$ has a perfect quantum strategy if and only if $Ax = b$ has a finite-dimensional quantum solution.

Mermin-Peres square: perfect quantum strategy

Best classical strategy succeeds with probability 35/36

Bell test: success probability $> 35/36 \implies$ non-classicality

Quantum strategies and quantum correlations



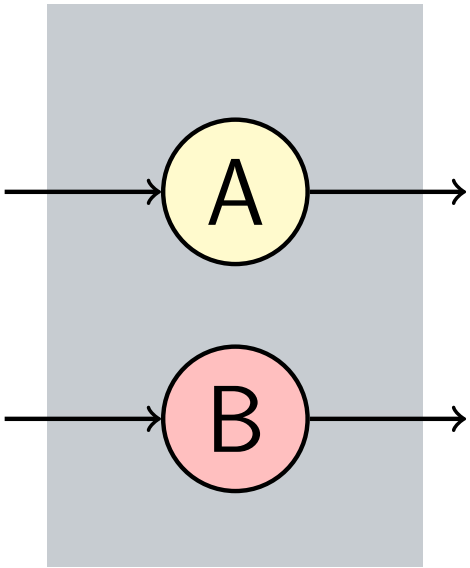
Alice and Bob's behaviour in a non-local game is described by a family of probability distributions

$$\{p(a,b|x,y)\} \subset \mathbb{R}^{\mathcal{O}_A \times \mathcal{O}_B \times \mathcal{I}_A \times \mathcal{I}_B}$$

where $p(a,b|x,y) =$ probability of output (a,b) on input (x,y)

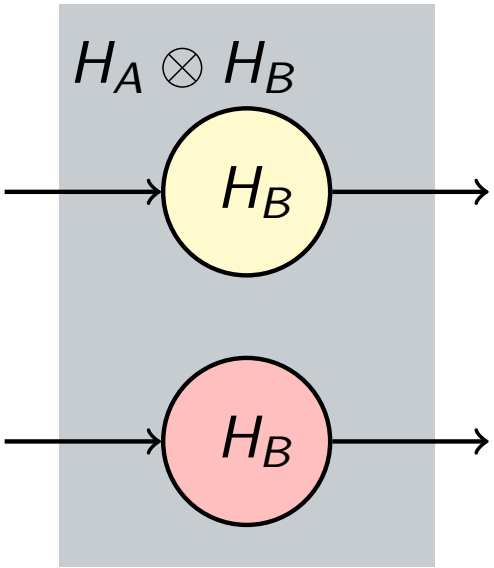
$\{p(a,b|x,y)\}$ is called a correlation matrix

Quantum strategies and quantum correlations



Which correlations can arise in quantum mechanics?

Quantum strategies and quantum correlations



Which correlations can arise in quantum mechanics?

> Axiom for separated subsystems
>
> If H_A and H_B are Hilbert spaces of two separated systems, then joint system has Hilbert space $H_A \otimes H_B$

Important note:

State of joint system does not have to be a product $v \otimes w$

We can have entangled states like $e_1 \otimes e_1 + e_2 \otimes e_2$

Quantum correlations: formal definition

Quantum correlations: Alice and Bob generate output by measuring a shared quantum state

Definition

A correlation $\{p(a,b|x,y)\} \in \mathbb{R}^{\mathcal{O}_A \times \mathcal{O}_B \times \mathcal{I}_A \times \mathcal{I}_B}$ is quantum if there are:

- Hilbert spaces H_A, H_B,
- a state $v \in H_A \otimes H_B$,
- measurements $\{M_a^x\}_{a \in \mathcal{O}_A}$ on H_A for every $x \in \mathcal{I}_A$, and
- measurements $\{N_b^y\}_{b \in \mathcal{O}_B}$ on H_B for every $y \in \mathcal{I}_B$,

such that $p(a,b|x,y) = v^* M_a^x \otimes N_b^y v$ for all a, b, x, y.

Sets of correlations

- $C_c = C_c(\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B) :=$ classical correlations
- $C_q :=$ quantum correlations with finite-dimensional Hilbert spaces
- $C_{qs} :=$ Quantum correlations with any Hilbert spaces

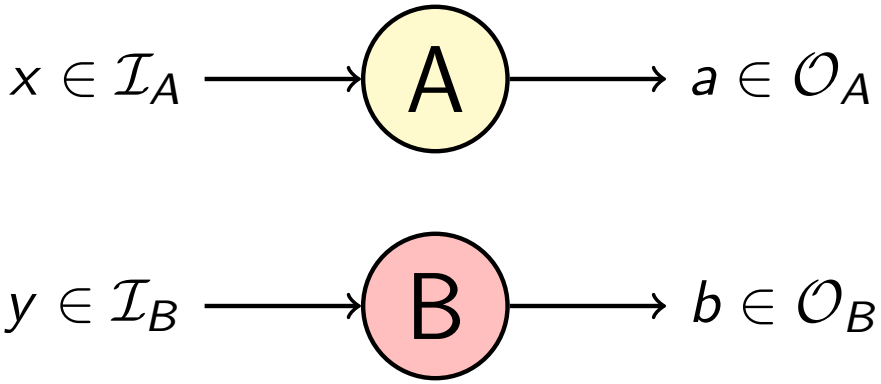
All three sets are convex, C_c is closed

C_q and C_{qs} capture behaviour of entangled states

What correlation set matches reality?

(what correlations can we generate in nature?)

Bell tests rule out classical correlations



Win if

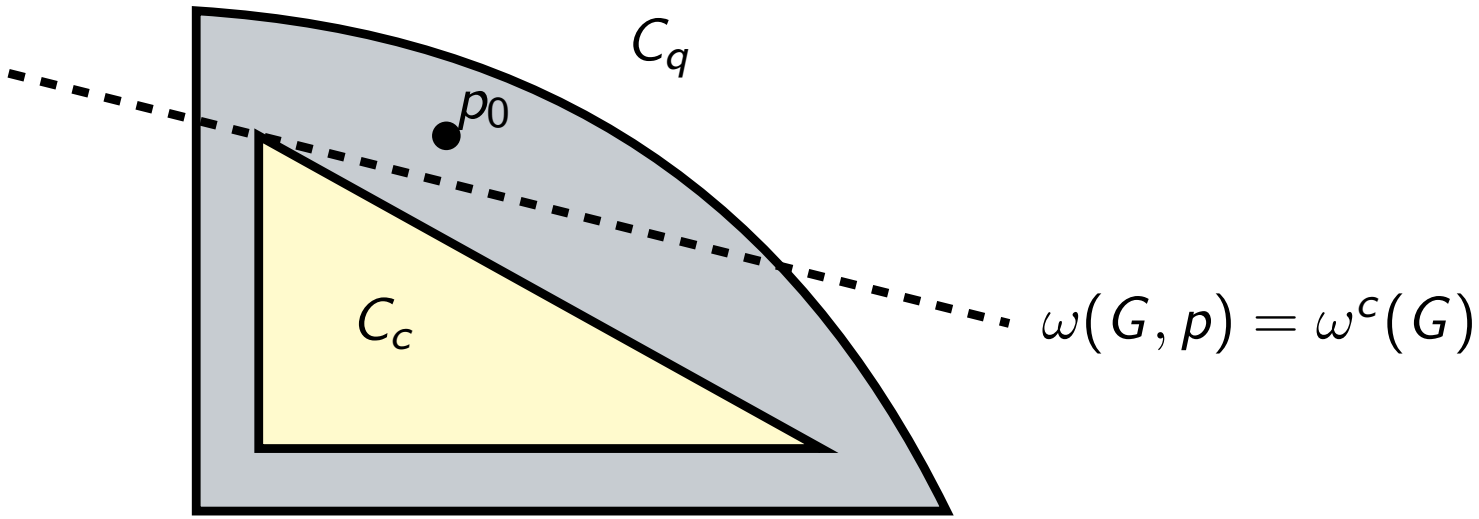
$$V(a, b|x, y) = 1$$

If Alice and Bob play game G using correlation $p = \{p(a, b|x, y)\}$, then success probability is

$$\omega(G; p) := \sum_{a,b,x,y} \pi(x, y) V(a, b|x, y) p(a, b|x, y).$$

Classical success probability of game G is $\omega^c(G) := \max_{p \in C_c} \omega(p)$ (maximum of linear functional over closed convex set)

Bell tests rule out classical correlations II



If $\omega(G; p_0) > \omega^c(G)$, then p_0 can't be classical

Non-classical correlations have been generated in experiments:

Freedman and Clauser, 1972

Hensen et. al., TU Deflt, loop-hole free Bell tests, 2015

Sets of correlations ct'd

- $C_c = C_c(\mathcal{O}_A, \mathcal{O}_B, \mathcal{I}_A, \mathcal{I}_B) :=$ classical correlations
- $C_q :=$ quantum correlations with finite-dimensional Hilbert spaces
- $C_{qs} :=$ Quantum correlations with any Hilbert spaces

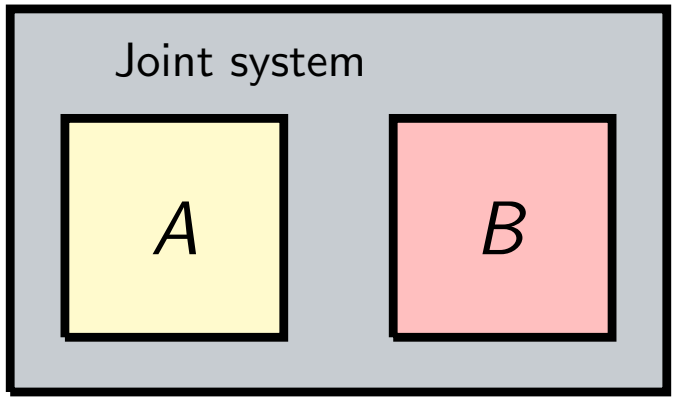
All three sets are convex, C_c is closed

C_q and C_{qs} capture behaviour of entangled states

Which correlation set matches reality, and are there any other options?

Yes... $C_{qa} := \overline{C_q} = \overline{C_{qs}}$

Commuting operator correlations



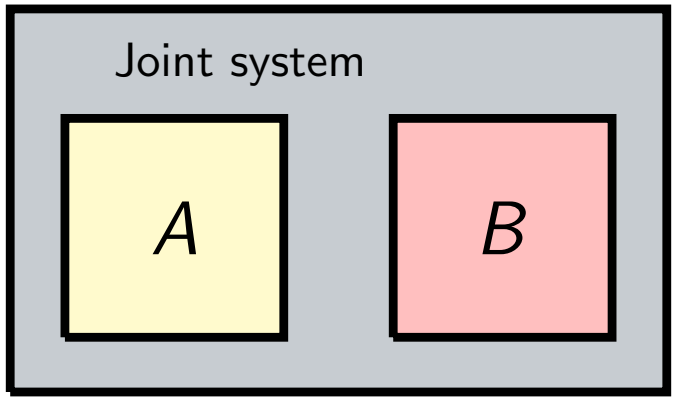
Recall:

Tensor product approach to separated subsystems:

Physical system = Hilbert space

If H_A and H_B are Hilbert spaces of two separated systems, then joint system has Hilbert space $H_A \otimes H_B$

Commuting operator correlations



Different approach (used for instance in Haag-Kastler axioms):

Commuting operator appraoch:

Physical system $=$ C^*-algebra $\mathcal{A}$, subsystem $=$ subalgebra $\mathcal{S}$

Two subalgebras $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathcal{A}$ are separated if $[\mathcal{S}_1, \mathcal{S}_2] = 0$.

(We can assume $\mathcal{A} = \mathcal{B}(H)$, and states are still unit vectors in H)

Commuting-operator correlations: formal definition

Definition

A correlation $\{p(a,b|x,y)\}$ is commuting-operator if there is:

- a Hilbert space H and a state $v \in H$,
- measurements $\{M_a^x\}_{a \in \mathcal{O}_A}$ on H for every $x \in \mathcal{I}_A$, and
- measurements $\{N_b^y\}_{b \in \mathcal{O}_B}$ on H for every $y \in \mathcal{I}_B$,

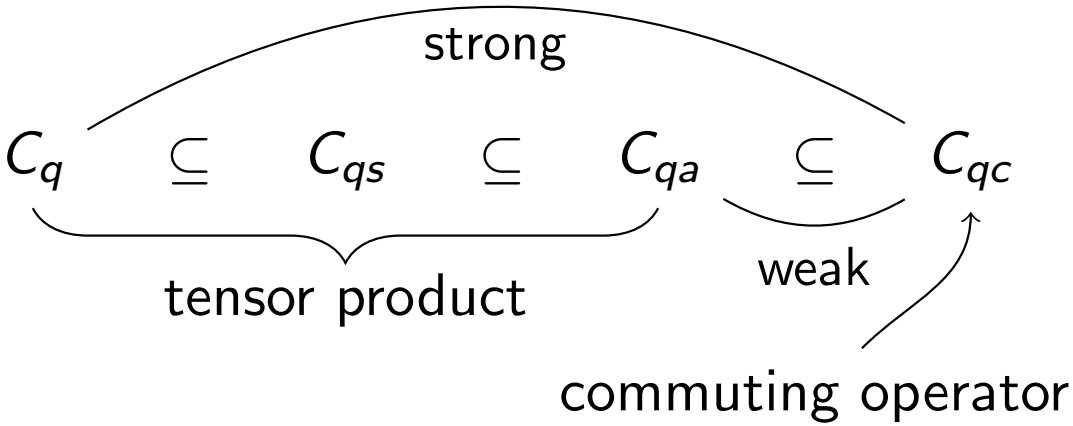
such that

- $M_a^x N_b^y = N_b^y M_a^x$ for every a, b, x, y, and
- $p(a,b|x,y) = v^* M_a^x N_b^y v$ for all a, b, x, y.

(if H is finite-dimensional, then $p \in C_q$)

Tsirelson's problems

C_{qc} := commuting-operator correlations



All sets are convex... C_{qc} and C_{qa} are closed

Which set describes reality? Are these sets even different?

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

Strongest version is $C_q \stackrel{?}{=} C_{qc}$: do ∞-dim'l commuting-operator correlations have finite-dimensional models?

Recall: quantum solutions of linear systems

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

Quantum solution:

Collection of unitaries $X_1, \ldots, X_n \in \mathcal{U}(\mathcal{H})$ such that

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

Recall: quantum solutions of linear systems

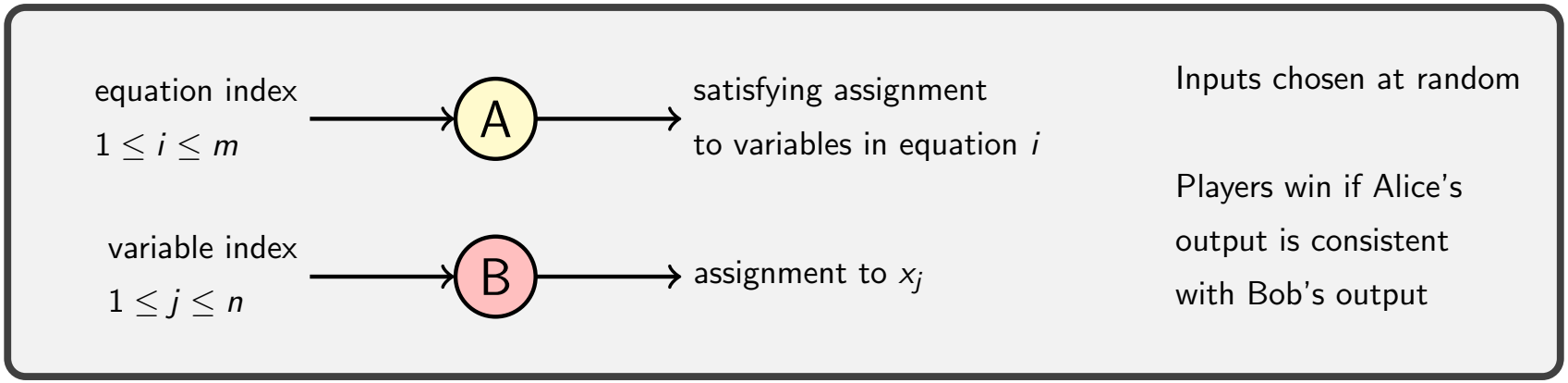
$Ax = b$: $m \times n$ linear system over $\mathbb{Z}_2$

Solution group of $Ax = b$

$$\Gamma(A,b) = \langle\, x_1, \ldots, x_n, J \;:\; x_j^2 = 1 = [x_j, J] = J^2 \text{ for all } j$$
$$\prod_j x_j^{A_{ij}} = J^{b_i}, i = 1, \ldots, m$$
$$[x_j, x_k] = 1 \text{ if } A_{ij}, A_{ik} \neq 0, \text{ some } i \,\rangle$$

Group commutator: $[a,b] = aba^{-1}b^{-1}$

Recall: Linear system non-local games



Theorem (Cleve-Mittal)

G = game associated to $Ax = b$. The following are equivalent:

- *there is $p \in C_q$ with $\omega(G; p) = 1$,*
- *$Ax = b$ has a finite-dimensional quantum solution, and*
- *J is non-trivial in a finite-dim'l representation of $\Gamma(A, b)$*

Theorem (Cleve-Mittal)

G = game associated to $Ax = b$. The following are equivalent:

- *there is $p \in C_q$ with $\omega(G; p) = 1$,*
- *$Ax = b$ has a finite-dimensional quantum solution, and*
- *J is non-trivial in a finite-dim'l representation of $\Gamma(A, b)$.*

Theorem (Cleve-Liu-S.)

G = game associated to $Ax = b$. The following are equivalent:

- *there is $p \in C_{qc}$ with $\omega(G; p) = 1$,*
- *$Ax = b$ has a quantum solution, and*
- *J is non-trivial in a representation of $\Gamma(A, b)$.*

Theorem (Cleve-Mittal)

G = game associated to $Ax = b$. The following are equivalent:

- *there is $p \in C_q$ with $\omega(G; p) = 1$,*
- *$Ax = b$ has a finite-dimensional quantum solution, and*
- *J is non-trivial in a finite-dim'l representation of $\Gamma(A, b)$.*

Theorem (Cleve-Liu-S.)

G = game associated to $Ax = b$. The following are equivalent:

- *there is $p \in C_{qc}$ with $\omega(G; p) = 1$,*
- *$Ax = b$ has a quantum solution, and*
- *J is non-trivial in a representation of $\Gamma(A, b)$.*

Theorem (Cleve-Mittal)

G = game associated to $Ax = b$. The following are equivalent:

- *there is $p \in C_q$ with $\omega(G; p) = 1$,*
- *$Ax = b$ has a finite-dimensional quantum solution, and*
- *J is non-trivial in a finite-dim'l representation of $\Gamma(A, b)$.*

Theorem (Cleve-Liu-S.)

G = game associated to $Ax = b$. The following are equivalent:

- *there is $p \in C_{qc}$ with $\omega(G; p) = 1$,*
- *$Ax = b$ has a quantum solution, and*
- *J is non-trivial in $\Gamma(A, b)$.*

Focus on the group theory

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

G = game associated to $Ax = b$. Then:

- *there is $p \in C_q$ with $\omega(G; p) = 1$ if and only if J is non-trivial in a finite-dim'l representation of $\Gamma(A, b)$.*
- *there is $p \in C_{qc}$ with $\omega(G; p) = 1$ if and only if J is non-trivial in $\Gamma(A, b)$.*

Question: is there a group $\Gamma(A, b)$ where J is non-trivial, but trivial in finite-dimensional representations?

(In other words, can we find a non-residually-finite solution group?)

What groups are solution groups?

$$\Gamma(A,b) = \langle\, x_1, \ldots, x_n, J \;:\; x_j^2 = 1 = [x_j, J] = J^2 \text{ for all } j$$
$$\prod_j x_j^{A_{ij}} = J^{b_i}, i = 1, \ldots, m$$
$$[x_j, x_k] = 1 \text{ if } A_{ij}, A_{ik} \neq 0, \text{ some } i \,\rangle$$

Imagine we can write down any group presentation we want, but generators in the relation will be forced to commute

Example ($S_3 = \langle a, b : a^2 = b^2 = 1, (ab)^3 = 1\rangle$)

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

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

Group embedding theorem

Despite this seemingly strong restriction on our relations, solution groups are as complicated as general groups!

Theorem (S)

Any finitely-presented group G can be embedded in a solution group $\Gamma(A, b)$. Given a central involution J_0 of G, the embedding can be constructed to send J_0 to $J \in \Gamma(A, b)$.

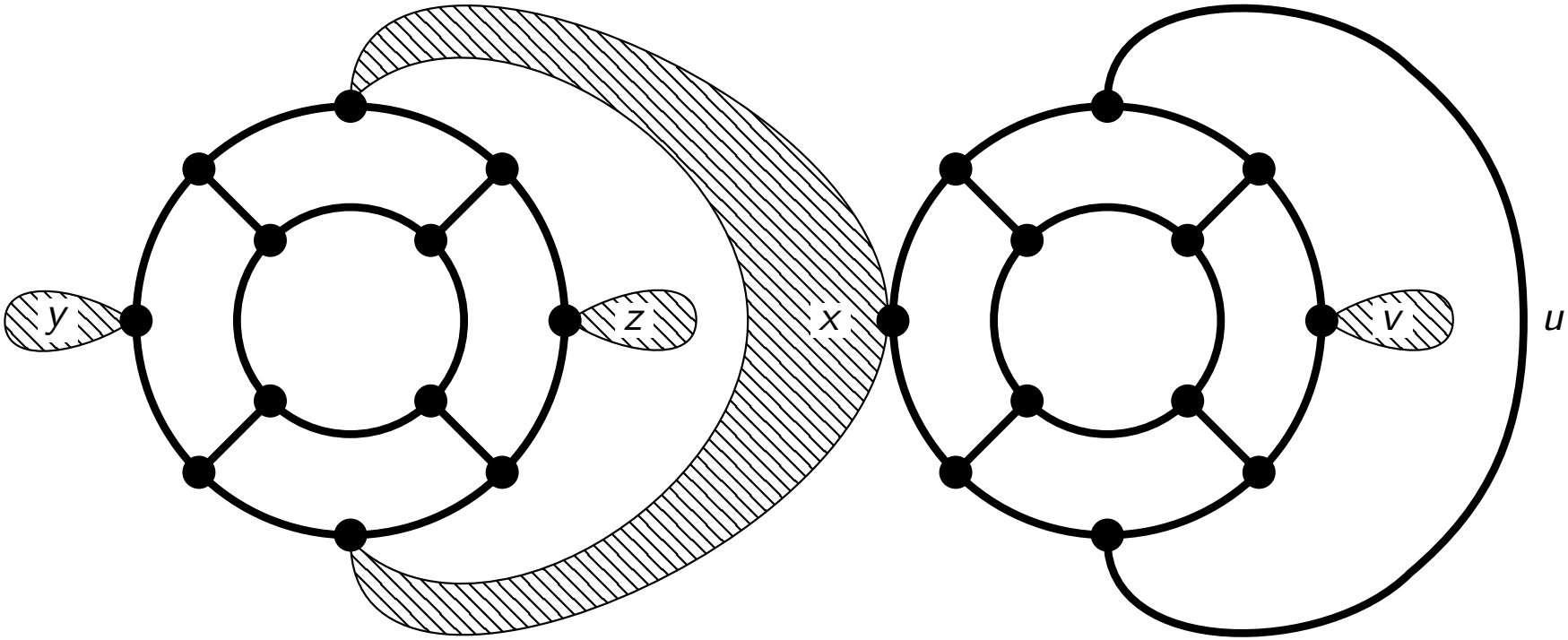
Gives us a way to translate group theory into non-local games

Corollary

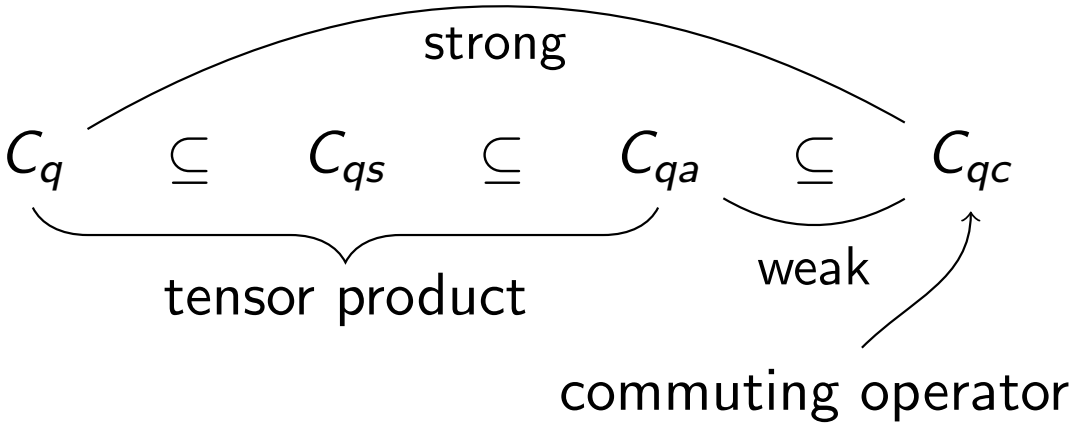
There is a solution group $\Gamma(A, b)$ where $J \neq 1$ but J is trivial in all finite-dim'l reps. As a result, $C_q \neq C_{qc}$.

How do we prove the embedding theorem

Can represent linear systems $Ax = b$ / $\mathbb{Z}_2$ by hypergraphs



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



- Refinement of this approach: $C_{qa} \neq C_{qs}$, i.e. C_q and C_{qs} are not closed
- Size of parameters: $|\mathcal{O}_A| = 8$, $|\mathcal{O}_B| = 2$, but $|\mathcal{I}_A|, |\mathcal{I}_B| \sim 200$.
- Dykema-Paulsen-Prakash: possible to get $C_{qa} \neq C_{qs}$ with $|\mathcal{I}_A| = |\mathcal{I}_B| = 5$, $|\mathcal{O}_A| = |\mathcal{O}_B| = 2$.
- Can we further reduce the number of inputs?

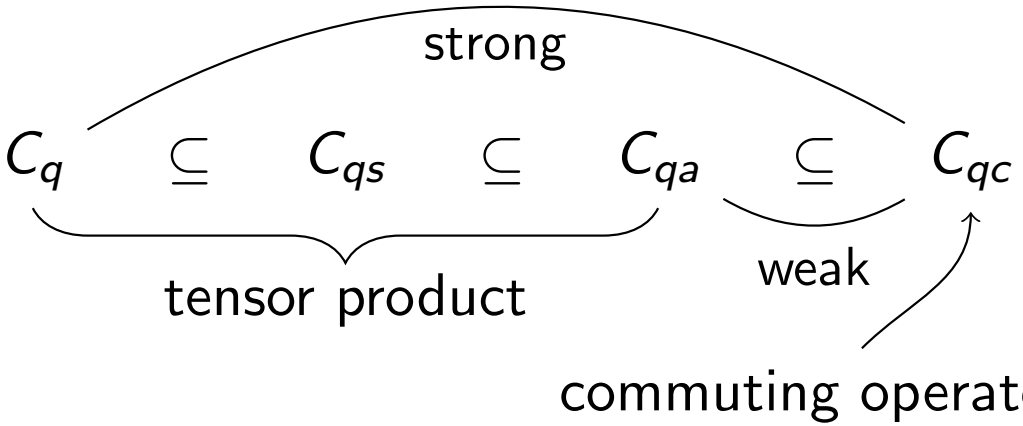
What else can we do with embedding theorem

Theorem (S)

Any finitely-presented group G can be embedded in a solution group $\Gamma(A, b)$. Given a central involution J_0 of G, the embedding can be constructed to send J_0 to $J \in \Gamma(A, b)$.

Word problem for groups is undecidable, so:

- Undecidable to determine whether there is $p \in C_t$ with $\omega(G, p) = 1$ for any $t \in \{q, qs, qa, qc\}$.
- T. Fritz: quantum logic is undecidable



Final question: what about the weak Tsirelson problem?

This is equivalent to asking whether we can separate C_{qc} from C_t, $t \in \{q, qs, qa\}$ with a Bell inequality

Theorem (Fritz, JNPPSW, Ozawa)

The weak Tsirelson problem is equivalent to the Connes embedding problem.