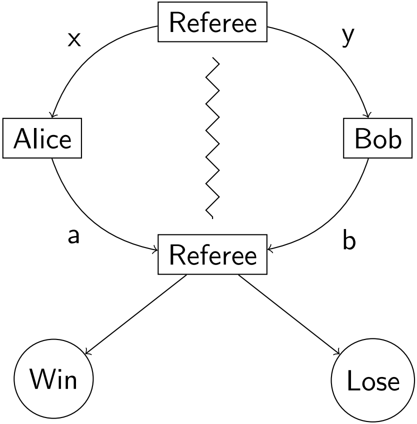
Entanglement requirements in non-local games

William Slofstra

IQC, University of Waterloo

August 31, 2017

Non-local games (aka Bell scenarios)



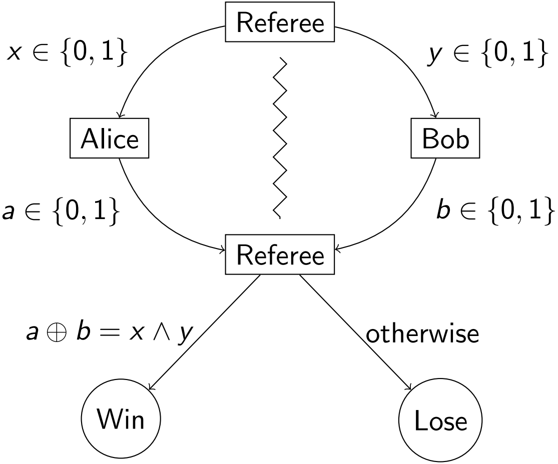
Win/lose based on outputs a, b and inputs x, y

Alice and Bob must cooperate to win

Winning conditions known in advance

Complication: players cannot communicate while the game is in progress

Example: the CHSH game



Compare with:

$$A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1$$

Non-local games more formally

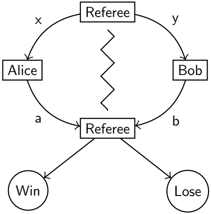
A non-local game consists of:

Finite input sets: $\mathcal{I}_X$, $\mathcal{I}_Y$

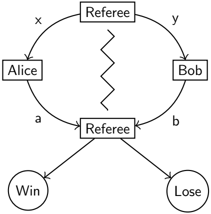
Finite output sets: $\mathcal{O}_X$, $\mathcal{O}_Y$

A prob. distribution π on $\mathcal{I}_X \times \mathcal{I}_Y$

A function $V : \mathcal{O}_X \times \mathcal{O}_Y \times \mathcal{I}_X \times \mathcal{I}_Y \to \{0, 1\}$



Non-local games more formally



A non-local game consists of:

Finite input sets: $\mathcal{I}_X$, $\mathcal{I}_Y$

Finite output sets: $\mathcal{O}_X$, $\mathcal{O}_Y$

A prob. distribution π on $\mathcal{I}_X \times \mathcal{I}_Y$

A function $V : \mathcal{O}_X \times \mathcal{O}_Y \times \mathcal{I}_X \times \mathcal{I}_Y \to \{0, 1\}$

Interpretation:

If Alice and Bob win on inputs (x, y) and outputs (a, b) then $V(a, b|x, y) = 1$.

Otherwise $V(a, b|x, y) = 0$.

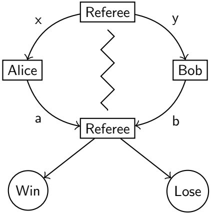
Strategies: what can Alice and Bob do?

Deterministic local strategies:

Choose a_x's and b_y's ahead of time

Alice outputs a_x on input x

Bob outputs b_y on input y



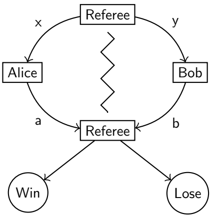
Strategies: what can Alice and Bob do?

Deterministic local strategies:

Choose a_x's and b_y's ahead of time

Alice outputs a_x on input x

Bob outputs b_y on input y



The winning probability for this strategy S is

$$\omega(S) = \sum_{x\mathcal{I}_A, y\in\mathcal{I}_B} \pi(x,y)V(a_x, b_y|x,y).$$

The *classical value* of the game G is

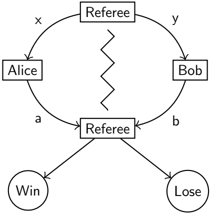
$$\omega^c(G) = \max\{\omega(S) : \text{ deterministic strategies } S\}.$$

What can the players do?

Quantum strategy:

Alice and Bob share quantum state $|\psi\rangle \in H_A \otimes H_B$

Choose outputs according to PVMs $\{P_a^x\}$, $\{Q_b^y\}$

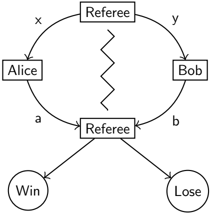


What can the players do?

Quantum strategy:

Alice and Bob share quantum state $|\psi\rangle \in H_A \otimes H_B$

Choose outputs according to PVMs $\{P_a^x\}$, $\{Q_b^y\}$



The winning probability for this strategy S is

$$\omega(S) = \sum_{x\mathcal{I}_A, y\in\mathcal{I}_B} \pi(x,y)V(a_x, b_y|x,y) \langle\psi| P_a^x \otimes Q_b^y |\psi\rangle .$$

The quantum value of the game G is

$$\omega^q(G) = \sup\{\omega(S) : \text{ quantum strategies } S\}.$$

Note: no bound on dim H_A, H_B assumed

Entanglement requirements

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

G is a distributed computational task with quantum advantage

Entanglement requirements

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

G is a distributed computational task with quantum advantage

We'd like a resource theory for non-local games

How much "entanglement" is required to achieve

$\omega^q(G)$? (the quantum value)

$\omega^q(G) - \epsilon$? (near the quantum value)

Entanglement requirements

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

G is a distributed computational task with quantum advantage

We'd like a resource theory for non-local games

How much "entanglement" is required to achieve

$\omega^q(G)$? (the quantum value)

$\omega^q(G) - \epsilon$? (near the quantum value)

Possible resources: local Hilbert space dimension, von Neumann entropy, "non-locality"

Why do we care about entanglement requirements?

- Test cases for power of entanglement
- Certify presence of entanglement
- Self-test quantum states:

  For some games G, achieving $\omega^q(G)$ or $\omega^q(G) - \epsilon$ can require states or strategies of a certain form.
- Device independent protocols in cryptography

Why do we care about entanglement requirements?

- Test cases for power of entanglement
- Certify presence of entanglement
- Self-test quantum states:

  For some games G, achieving $\omega^q(G)$ or $\omega^q(G) - \epsilon$ can require states or strategies of a certain form.
- Device independent protocols in cryptography

There are other important questions, like:

Can we compute value of $\omega^q(G)$?

(Note: $\omega^c(G)$ is relatively easy to compute)

What do we know about entanglement requirements?

Bounded entanglement is not enough: there are games with $O(n)$ questions requiring dimension $2^{\Omega(n)}$ to play optimally

What do we know about entanglement requirements?

Bounded entanglement is not enough: there are games with $O(n)$ questions requiring dimension $2^{\Omega(n)}$ to play optimally

Is a finite amount of entanglement required for every fixed G?

What do we know about entanglement requirements?

Bounded entanglement is not enough: there are games with $O(n)$ questions requiring dimension $2^{\Omega(n)}$ to play optimally

Is a finite amount of entanglement required for every fixed G?

Conjecture [PV10]: there is a game with three questions and two answers per player for which finite local dimensions are not enough

Finite dimensions are not sufficient for variants of non-local games: [LTW13], [MV13], [RV15]

What do we know about entanglement requirements?

Bounded entanglement is not enough: there are games with $O(n)$ questions requiring dimension $2^{\Omega(n)}$ to play optimally

Is a finite amount of entanglement required for every fixed G?

Conjecture [PV10]: there is a game with three questions and two answers per player for which finite local dimensions are not enough

Finite dimensions are not sufficient for variants of non-local games: [LTW13], [MV13], [RV15]

Theorem (S): there is a non-local game (with several hundred questions per player) for which finite local dimensions does not suffice to achieve $\omega^q(G)$

New tool: connection to group theory

Linear system game:

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

Inputs: Alice receives $1 \leq i \leq m$ (equation)
Bob receives $1 \leq j \leq n$ (variable)

Outputs: Alice: assignment to variables x_k with $A_{ik} \neq 0$
Bob: assignment to variable x_j

Win if Alice's assignment satisfies equation i, and
either $A_{ij} = 0$ or Alice's assignment agrees with Bob's

New tool: connection to group theory

Linear system game:

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

Inputs: Alice receives $1 \leq i \leq m$ (equation)
Bob receives $1 \leq j \leq n$ (variable)

Outputs: Alice: assignment to variables x_k with $A_{ik} \neq 0$
Bob: assignment to variable x_j

Win if Alice's assignment satisfies equation i, and
either $A_{ij} = 0$ or Alice's assignment agrees with Bob's

Classically: can play perfectly iff $Ax = b$ has a solution

(Play perfectly $=$ win with probability 1)

Quantum solutions of $Ax = b$

Theorem (Cleve-Mittal, Cleve-Liu-S): Can play linear system game perfectly with a quantum strategy iff:

there are 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 $Ax = b$

Theorem (Cleve-Mittal, Cleve-Liu-S): Can play linear system game perfectly with a quantum strategy iff:

there are 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)

If this happens, say that $Ax = b$ has a quantum solution

(Warning: there are some big footnotes here)

Connection with group theory

The *solution group* Γ 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)

Let G be the game for linear system $Ax = b$. Then G has a perfect (tensor-product) strategy if and only if J is non-trivial in some finite-dimensional representation of the solution group Γ.

What groups can be solution groups?

There are non-residually finite groups, i.e. groups with elements which are non-trivial but trivial in all finite-dimensional representations

Example (A non-residually finite group)

$K = \langle x, y, a, b : xyx^{-1} = y, yay^{-1} = b, yby^{-1} = a \rangle.$

ab^{-1} is trivial in finite-dimensional representations, but non-trivial in approximate representations

What groups can be solution groups?

There are non-residually finite groups, i.e. groups with elements which are non-trivial but trivial in all finite-dimensional representations

Example (A non-residually finite group)

$K = \langle x, y, a, b : xyx^{-1} = y, yay^{-1} = b, yby^{-1} = a \rangle$.

ab^{-1} is trivial in finite-dimensional representations, but non-trivial in approximate representations

Solution groups don't look very complicated, but:

Theorem (S)

Every finitely-presented group embeds in a solution group.

Other consequences of embedding theorem

- Undecidable to determine if $\omega^q(G) < 1$

Other consequences of embedding theorem

- Undecidable to determine if $\omega^q(G) < 1$
- Tobias Fritz: quantum logic is undecidable

Other consequences of embedding theorem

- Undecidable to determine if $\omega^q(G) < 1$
- Tobias Fritz: quantum logic is undecidable
- Tsirelson's problem: there are commuting-operator correlations which are not tensor-product correlations

Other consequences of embedding theorem

- Undecidable to determine if $\omega^q(G) < 1$
- Tobias Fritz: quantum logic is undecidable
- Tsirelson's problem: there are commuting-operator correlations which are not tensor-product correlations
- Big open question: Can we separate commuting-operator correlations from tensor-product correlations with a Bell inequality?

Other consequences of embedding theorem

- Undecidable to determine if $\omega^q(G) < 1$
- Tobias Fritz: quantum logic is undecidable
- Tsirelson's problem: there are commuting-operator correlations which are not tensor-product correlations
- Big open question: Can we separate commuting-operator correlations from tensor-product correlations with a Bell inequality?
- Self-testing: we can self-test any group
- In progress (with Li Liu): self-test any finite group robustly

Other consequences of embedding theorem

- Undecidable to determine if $\omega^q(G) < 1$
- Tobias Fritz: quantum logic is undecidable
- Tsirelson's problem: there are commuting-operator correlations which are not tensor-product correlations
- Big open question: Can we separate commuting-operator correlations from tensor-product correlations with a Bell inequality?
- Self-testing: we can self-test any group
- In progress (with Li Liu): self-test any finite group robustly

The end!