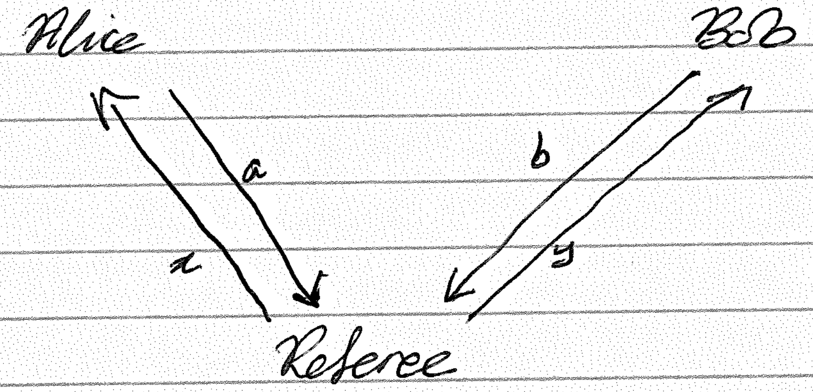
Nonlocal Games

Sources:
quant-ph/0404076 Cleve, Hoyer, Toner, Watrous

arXiv:1209.0448 Reichardt, Unger, Vazirani

arXiv:1207.0550 Ito, Vidick



$x \in X$, $y \in Y$
$a \in A$, $b \in B$

Referee sends questions (x,y) w. prob. $\pi(x,y)$.
Alice and Bob cannot communicate.
Respond with answers (a,b).

Win if $V(ab|xy)=1$, $V: X \times Y \times A \times B \to \{0,1\}$

Game determined by (π, V).

Classical Strategy: $p(ab|xy) = \sum_s \lambda_s a_s(x) b_s(y)$

λ_s = Shared Randomness / Hidden Variable

Classical value

$$\omega_c(G) = \max_{a,b} \sum_{x,y} \pi(x,y)\, a(x)\, b(y)\, V(a(x), b(y)|xy)$$

$a: X \to A$, $b: Y \to B$

Need only consider deterministic strategies by convexity.

Quantum strategies:

Alice and Bob could share an entangled state $|\Psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ with no a priori bound on dimension n.

$$p(ab|xy) = \langle \Psi | P_x^a \otimes Q_y^b | \Psi \rangle$$

where $\{P_x^a\}_a$, $\{Q_y^b\}_b$ are POVM's (different ones for different x, y).

Quantum / Entangled value

$$\omega^*(G) = \max_{|\Psi\rangle, \{P_x^a\}, \{Q_y^b\}} \sum_{x,y} \pi(x,y) \langle \Psi | P_x^a \otimes Q_y^b | \Psi \rangle V(ab|xy)$$

Bound on amount of entanglement needed:

Example: CHSH Game

Bell Inequalities $\longleftrightarrow$ Nonlocal Games

CHSH Inequality $\longleftrightarrow$ $\pi(x,y)$, $V(ab|xy)$

Choice of Experimental setup $\longleftrightarrow$ Choice of quantum strategy

Local Hidden Variable $\longleftrightarrow$ Convex Combination of Classical Strategies

$a,b,x,y \in \{0,1\}$, $\qquad \pi(x,y) = \frac{1}{4}$, $\forall x,y \in \{0,1\}$.

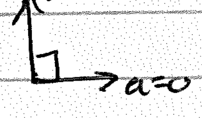
$$V(a,b|x,y) = \begin{cases} 1 & \text{if } a \oplus b = x \wedge y \\ 0 & \text{else} \end{cases}$$

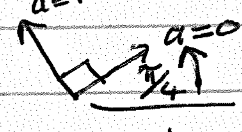
$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$$

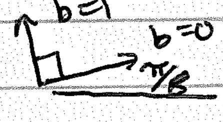
$\omega_c(G) = 3/4$. Always answer 0.

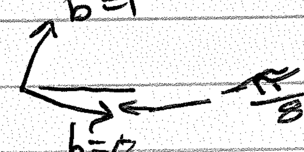
$\omega^*(G) = \cos^2 \pi/8 \approx 0.85$

$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$X_0 =$ 

$X_1 =$ 

$Y_0 =$ 

$Y_1 =$ 

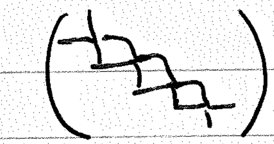
Rigidity of the CHSH Game [RUV]

Play N sequential CHSH games. If Alice and Bob win a sufficiently large fraction of these games, they must have been using (nearly) the optimal strategy in ~~all~~ these games.

Theorem: $N = \text{poly}(n)$ games.
If $\Pr[\text{win} \geq (85\% - \varepsilon) \text{ of games}] \geq 1 - \varepsilon$
Then with high probability for a random subset of n games,
Provers' actual Strategy $\approx$ Ideal Strategy.
for those n games

Theorem: 1-Game
If $\Pr[\text{win} \geq 85\% - \varepsilon]$
$\Rightarrow$ State and Measurements
are $\sqrt{\varepsilon}$-close to optimal strategy
(up to local isometries)
$\mathcal{H}_A \hookrightarrow \mathbb{C}^2 \otimes \mathcal{H}_{A'}$, $\mathcal{H}_B \hookrightarrow \mathbb{C}^2 \otimes \mathcal{H}_{B'}$
$|\psi_{AB}\rangle \longmapsto (\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) \otimes |\psi'\rangle_{A'B'}$.

Jordan's Lemma
Any 2-projections can be simultaneously block-diagonalized with blocks of dimension at most 2.

$P =$
Q

"$\rightsquigarrow$" 2-dimensional case

Tensor Product structure for Repeated CHSH-Games.

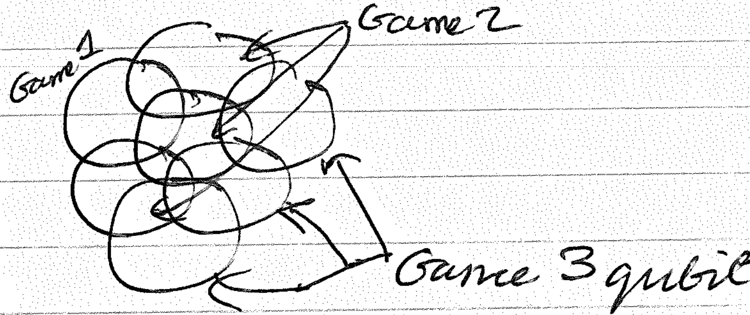
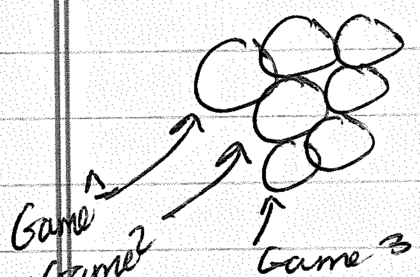


Figure 4 in
1209.0448

Single qubit result
$\rightarrow$ Nearby "multi-qubit ideal strategy"



In $\otimes$ but depend on previous
Games

Well-approx.^{d} by 

Application:

Delegated Quantum Computation with untrusted resources/quantum provers.

Computation by Teleportation

H, $G = \pi/4$ rotation about y-axis of Bloch sphere, CNOT.

Referee asks Bob to prepare many copies of resource state

$$|0\rangle \otimes (I \otimes H)|\psi\rangle \otimes (I \otimes G)|\psi\rangle \otimes CNOT_{2,4}(|\psi\rangle \otimes |\psi\rangle),$$

Bob applies measurements to his halves of shared EPR pairs and sends results to referee. Referee directs Alice to make a series of Bell measurements connecting output of 1 operation to input of another.

With certain Probabilities ~~1/4~~, ~~apply~~ apply following protocols:
2) & 3) INCLUDE SOME PLAYING OF CHSH GAMES

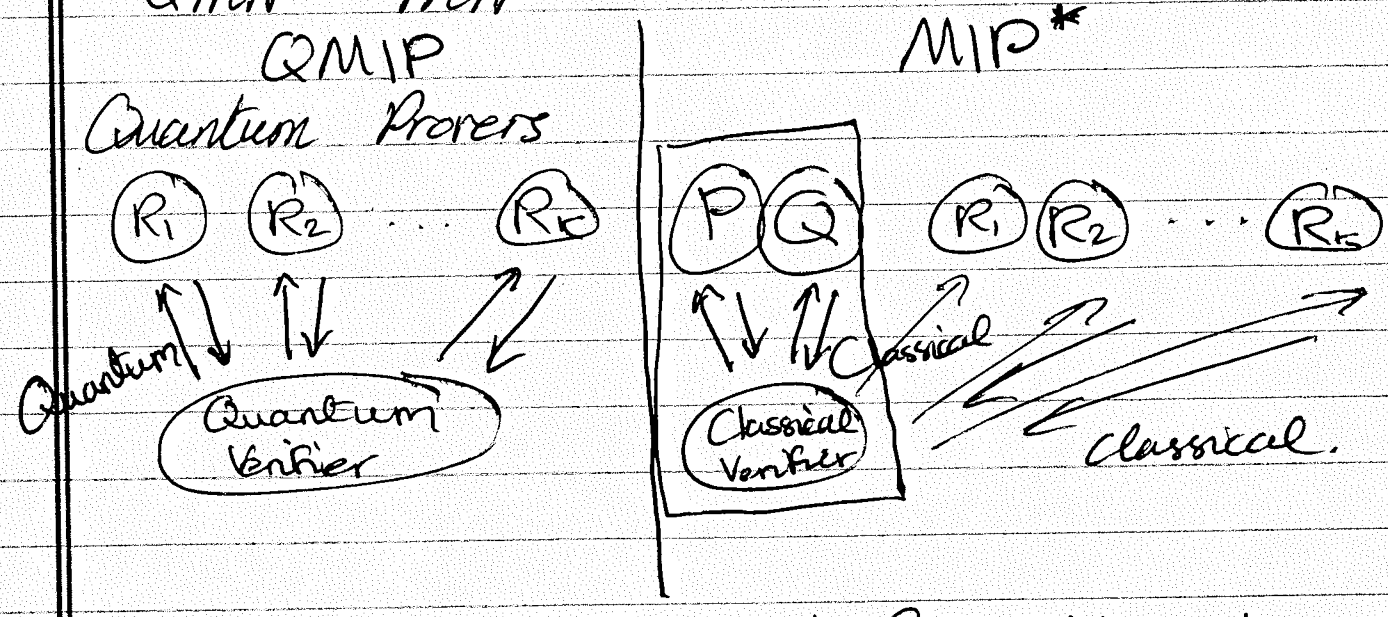
1) Play CHSH game w. Alice & Bob
2) Ask Bob to prepare resource state. Verify by pretending to play CHSH w. Alice
3) Ask Alice to apply Bell measurements. Verify by pretending to play CHSH w. Bob.
4) Computation by Teleportation.

Multi-Prover Interactive Proof*

MIP*: Class of decision problems for which a "YES" answer can be verified by an interactive proof. Probabilistic poly-time verifier ~~sends~~ exchanges messages (in poly # of rounds) with multiple provers. These provers are of unbounded computational power who are entangled but who cannot communicate with each other. poly. # of provers.
All messages are classical.

QMIP: Quantum messages. Quantum Verifier.

QMIP = MIP*



Add 2 new verifiers and force them to play the role of the quantum verifier from the QMIP-protocol.

[IV]

$$NEXP \subseteq MIP^*(\underset{\text{provers}}{3}, \underset{\text{rounds}}{\text{poly}}, \underset{\text{completeness}}{1}, \underset{\text{Soundness}}{2^{-q}})$$

poly

$MIP = NEXP$, so $MIP \subseteq MIP^*$

Relies on Multilinearity Test

Game w. Verifier and 3 players, finite field $\mathbb{F}$, and integer n.

Prob $\frac{1}{2}$:

- Consistency: ~~$x \mapsto A, B, C$~~
  x unif. at random from $\mathbb{F}^n$, $x \mapsto A, B, C$
  Answers from $\mathbb{F}$ should all be the same.
- Linearity: Chooses $x \in \mathbb{F}^n$, $i \in \{1, \ldots, n\}$, alters i^{th} position of x randomly to get y, z.
  $x \mapsto A$, $y \mapsto B$, $z \mapsto C$.
  Answers $a, b, c \in \mathbb{F}$.
  Accepts if $\dfrac{b-a}{y_i - x_i} = \dfrac{c-b}{z_i - y_i} = \dfrac{c-a}{z_i - x_i}$.

Classically: To win w. prob $> 1-\varepsilon$, players must use same multilinear function $g: \mathbb{F}^n \to \mathbb{F}$ (on $1 - O(n^2\varepsilon)$ of questions).

Quantum: ~~[illegible]~~

3 players share perm^n-inv. $|\psi\rangle$, win w. prob $> 1-\varepsilon$.

$\exists$ single measurement $\{V^g\}$, outcomes in multilinear $g: \mathbb{F}^n \to \mathbb{F}$, s.t. actions indistinguishable to player who

1. measures $|\psi\rangle$ w. $\{V^g\}$ obtaining g.
2. Answers $g(x)$.

With high prob., multilinear functions used by 3 players are identical.

Success in multilinearity game forces player to make only trivial use of their entanglement. $\{V_g\}$ independent of questions asked.

NEXP-complete problem of succinct-3-colorability.
Given $f: (\mathbb{F}^n)^2 \times (\mathbb{F})^2 \to \mathbb{F}$, low-degree poly.
Verify $\exists$ multilinear function $g: \mathbb{F}^n \to \mathbb{F}$ s.t.
$$F(x, y, g(x), g(y)) = 0.$$

Low-Degree Sum-check Test.