Parallel Repetition of Nonlocal Quantum Strategies

Richard Cleve
Cheriton School of Computer Science, U of Waterloo
& Perimeter Institute for Theoretical Physics

This is joint work with

William Slofstra
U of Waterloo

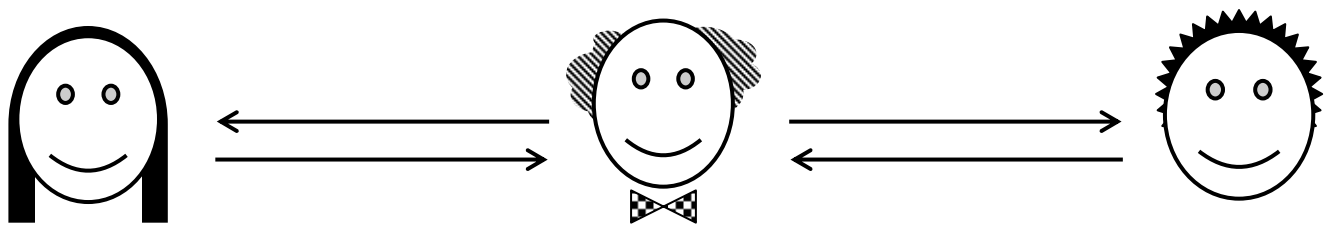
Falk Unger
CWI, Amsterdam

Sarvagya Upadhyay
U of Waterloo

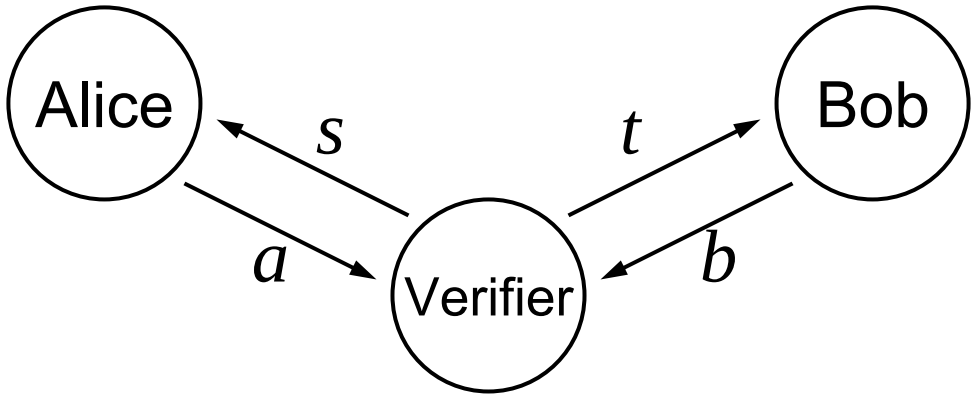
Question: what happens if multiple nonlocality tests (say, of Bell inequalities) are performed in parallel?

Can we just analyze them separately?

Such questions have connections with so-called ***multiprover interactive proof systems***, where the "provers" interact with a "verifier" to convince him of the truth of a mathematical statement



Bell nonlocality à la CHSH



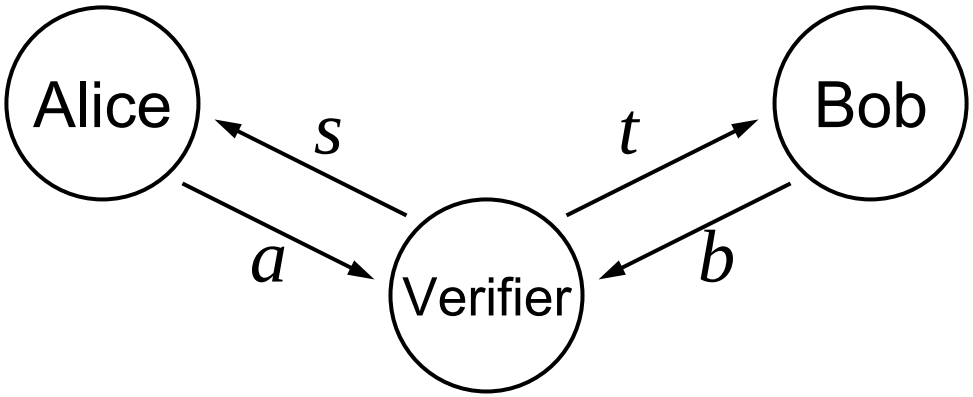
No communication between Alice and Bob during the game

- The Verifier chooses two random bits, s and t, and sends them to Alice and Bob, respectively
- Alice and Bob return bits a and b, resp.
- The Verifier ***accepts*** iff $a \oplus b = s \wedge t$ (Alice and Bob ***win*** iff Verifier accepts)

st	$a \oplus b$
00	0
01	0
10	0
11	1

[Bell '64; Clauser, Horne, Shimony, Holt '69]

CHSH game



For any ***classical*** strategy, Alice and Bob's success probability is at most ¾

Winning conditions: $a_s \oplus b_t = s \wedge t$

$$\begin{cases} a_0 \oplus b_0 = 0 \\ a_0 \oplus b_1 = 0 \\ a_1 \oplus b_0 = 0 \\ a_1 \oplus b_1 = 1 \end{cases}$$

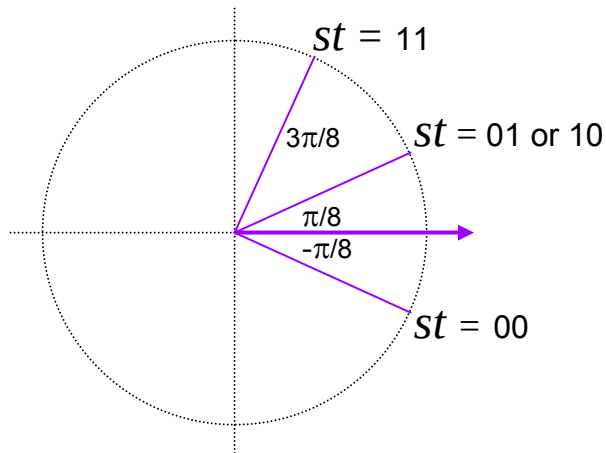
Equivalent to fact that ± 1 values must satisfy:

$$\frac{A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1}{4} \leq \frac{1}{2}$$

CHSH game

There is a ***quantum*** strategy that succeeds with probability $\frac{1}{2} + \frac{1}{4}\sqrt{2} = \cos^2(\pi/8) \approx 0.853$

- Alice and Bob start with entanglement $|\phi\rangle = |00\rangle - |11\rangle$
- If Alice applies rotation θ_A and Bob applies rotation θ_B: $\cos(\theta_A - \theta_B)\,(|00\rangle - |11\rangle) + \sin(\theta_A - \theta_B)\,(|01\rangle + |10\rangle)$
- Alice and Bob can organize their rotations so that $\theta_A - \theta_B$ takes on the following values for input st :



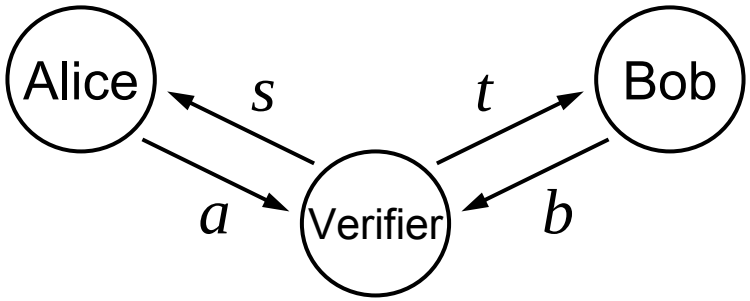
CHSH game

Can the success probability be improved?

No!

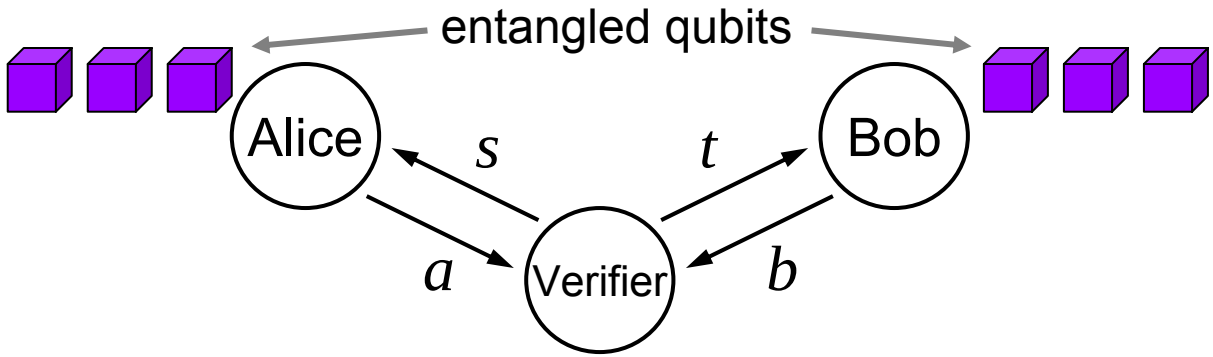
Theorem [Tsirelson ’80]**:** For ***any*** quantum strategy, the success probability is ***at most*** $\frac{1}{2} + \frac{1}{4}\sqrt{2}$

Nonlocality game framework



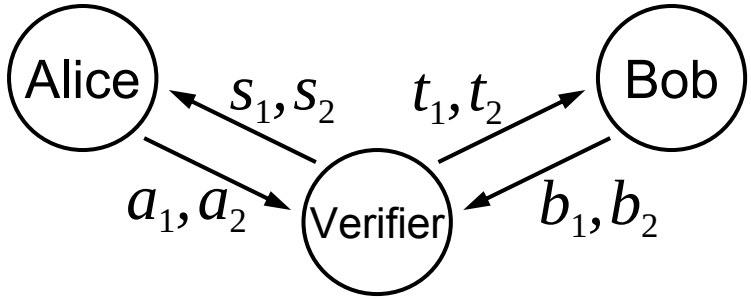
- A ***nonlocality game*** G consists of four sets A, B, S, T, a probability distribution π on $S \times T$, and a predicate $V : A \times B \times S \times T \to \{0,1\}$
- Verifier chooses $(s,t) \in S \times T$ according to π and, after receiving (a,b), ***accepts*** iff $V(a,b,s,t) = 1$
- The ***classical value*** of G, denoted as $\omega_c(G)$, is the maximum acceptance probability, over all classical strategies of Alice and Bob

Quantum strategies



- The ***quantum value*** of G, denoted as $\omega_q(G)$, is the maximum acceptance probability of quantum strategies
- An upper bound on $\omega_c(G)$ is a ***Bell inequality***
- A quantum strategy with success probability greater than $\omega_c(G)$ is a ***Bell inequality violation***
- An upper bound on $\omega_q(G)$ is a ***Tsirelson inequality***

Parallel repetition



- Two (or more) nonlocality games, G_1 and G_2, run in parallel
- Verifier chooses $(s_1, t_1) \in S_1 \times T_1$ & $(s_2, t_2) \in S_2 \times T_2$ independently
- Verifier accepts iff $V_1(a_1, b_1, s_1, t_1) = 1$ ***and*** $V_2(a_2, b_2, s_2, t_2) = 1$

One strategy: Alice and Bob play the two games separately

Question: is Alice and Bob's ***optimal*** strategy of this form?

If so, the value of this combined game is just $\omega(G_1)\,\omega(G_2)$

Answer is no for classical strategies!

For $G_1 = G_2$ = CHSH, we have $\omega_c(G_1) = \omega_c(G_2) = 3/4$

Playing G_1 and G_2 ***separately*** yields success probability $9/16$

But here's a strategy that succeeds with probability $10/16$

Alice:

$s_1 s_2$	$a_1 a_2$
00	00
01	00
10	00
11	01

Bob:

$t_1 t_2$	$b_1 b_2$
00	00
01	00
10	00
11	10

Intuition: Alice and Bob produce contextual outcomes so as to increase the overlap of the errors (erring on both games is no worse than erring on just one)

[Barrett, Collins, Hardy, Kent, Popescu '02] [Aaronson '06]

Same issue arose in the context of multiprover interactive proofs ...

Erroneous assumption [1988] that $\omega_c(G \text{ and } G) = \omega_c(G)\,\omega_c(G)$

The error was discovered [1990] with an example of a nonlocal game G such that $\omega_c(G) = 2/3 = \omega_c(G \text{ and } G)$

But a weaker qualitative multiplicative bound ***does*** hold ...

Theorem [Raz '95]: if $\omega_c(G) = \alpha < 1$ then there exists $\beta < 1$ such that $\omega_c(\underbrace{G \text{ and } G \text{ and } \ldots \text{ and } G}_{n \text{ times}}) \leq O(\beta^n)$

Open question: does a similar bound hold for $\omega_q(G)$?

⊕-games

- An ⊕***-game*** is a nonlocality game where:
  - Alice and Bob's messages, a and b, are single bits
  - The Verifier's decision is a function of s, t, $a \oplus b$ only (in other words, success iff $a \oplus b = f(s, t)$ for some f)
- **Examples:** CHSH, chained Bell inequalities, odd cycle game
- Classically, MIPs that are ⊕-games have exactly the same expressive power as those that are arbitrary games (NEXP)
- **Theorem** [C, Høyer, Toner, Watrous '04] [Wehner '05]**:** quantum MIPs that are ⊕-games have (apparently weaker) expressive power (EXP)

Answer is yes for quantum ⊕-games

What was the question?

Question: is the best strategy to play each game separately?

Main Theorem: for any ⊕-games G_1, G_2, ..., G_n,

$\omega_q(G_1 \text{ and } G_2 \text{ and } \ldots \text{ and } G_n) = \omega_q(G_1)\,\omega_q(G_2)\,\ldots\,\omega_q(G_n)$

Structure of the proof:

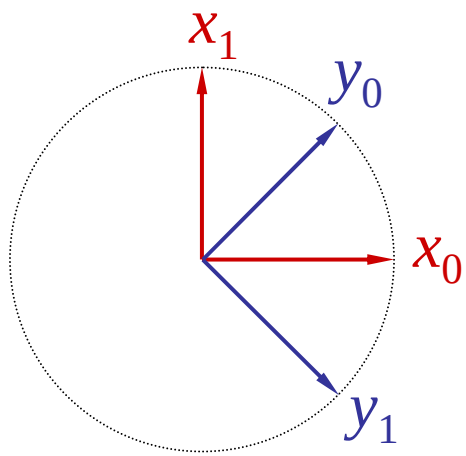
1. Use the known vector system characterization of ⊕-games, leading to semidefinite programs for their quantum values
2. Prove an additivity property for sums of ⊕-games to nicely express $\omega_q(G_1 \oplus \ldots \oplus G_n)$ in terms of $\omega_q(G_1), \ldots, \omega_q(G_n)$
3. Bound $\omega_q(G_1 \text{ and } \ldots \text{ and } G_n)$ in terms of expressions like $\omega_q(G_1 \oplus \ldots \oplus G_n)$

1. ⊕-games and vector systems

Quantum strategies for ⊕-games correspond to sets of unit vectors $\{x_s : s \in S\}$ and $\{y_t : t \in T\}$ in $\mathbb{R}^n$ such that, on input $(s,t) \in S \times T$,

$$\Pr[a \oplus b = 0] = (1 + x_s \cdot y_t)/2$$

E.g., vectors in $\mathbb{R}^2$ for the CHSH game:



[Tsirelson, ’87]

2. Are ⊕-games *additive*?

For ⊕-games G_1 and G_2, ***define*** the ⊕-game called $G_1 \oplus G_2$ to have success condition $a \oplus b = f_1(s_1, t_1) \oplus f_2(s_2, t_2)$

$a_1 \oplus b_1$ $a_2 \oplus b_2$

Obvious strategy: play each game separately, yielding a_1, b_1 and a_2, b_2 and then output $a = a_1 \oplus a_2$ and $b = b_1 \oplus b_2$

If $\omega(G_1) = \frac{1+\varepsilon_1}{2}$ and $\omega(G_2) = \frac{1+\varepsilon_2}{2}$ then success prob. is $\frac{1+\varepsilon_1\varepsilon_2}{2}$

Question: is this strategy optimal?

Classically, **no**: for CHSH⊕CHSH, this yields success prob. 5/8, whereas $\omega_c(\text{CHSH} \oplus \text{CHSH}) = 3/4 = \omega_c(\text{CHSH})$

2. Are ⊕-games *additive*?

For quantum strategies, **yes**:

if $\omega_q(G_1) = \frac{1+\varepsilon_1}{2}$ and $\omega_q(G_2) = \frac{1+\varepsilon_2}{2}$ then $\omega_q(G_1 \oplus G_2) = \frac{1+\varepsilon_1\varepsilon_2}{2}$

Why?

From their vector systems, $\omega_q(G_1), \omega_q(G_2)$ and $\omega_q(G_1 \oplus G_2)$ are all expressible as semidefinite programs (SDPs)

By various properties of the SDPs, it can be shown that the optimal vector system for $G_1 \oplus G_2$ is essentially the tensor product of the optimal vector systems for G_1 and G_2

3. Bounding $\omega_q(G_1$ and ... and $G_n)$

Let G_1, G_1, ..., G_n be $\oplus$-games with $\omega_q(G_k) = \frac{1+\varepsilon_k}{2}$

For any $M \in \{1,2,...,n\}$, we consider the $\oplus$-game $G_M = \bigoplus_{k \in M} G_k$

Additivity implies $\omega_q(G_M) = \frac{1+\varepsilon_M}{2}$ where $\varepsilon_M = \prod_{k \in [M]} \varepsilon_k$

$\omega_q(G_1$ and ... and $G_n)$ and the $\omega_q(G_M)$ are related by:

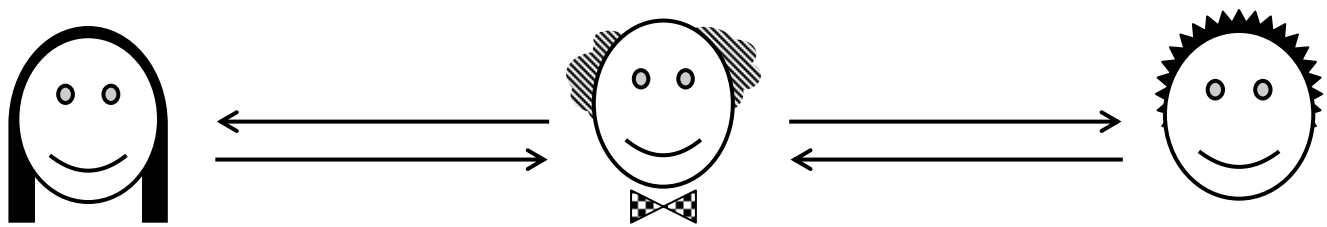
$$\omega_q(G_1 \text{ and } \ldots \text{ and } G_n) \leq \frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_M = \prod_{k=1}^{n} \left(\frac{1+\varepsilon_k}{2} \right) = \prod_{k=1}^{n} \omega_q(G_k)$$

Thus $\omega_q(G_1$ and ... and $G_n) \leq \prod_{k=1}^{n} \omega_q(G_k)$

Conclusions and open questions

Parallel repetition of Tsirelson-type bounds for $\oplus$-games are strongly multiplicative (unlike Bell-type bounds)

- For nonlocality games that are not $\oplus$-games is there a quantum analog of Raz's parallel repetition theorem? For example, does $\omega_q(G \text{ and } \ldots \text{ and } G)$ approach 0?
- What is the expressive power of multiprover interactive proof systems when the provers have shared entanglement?




THE END