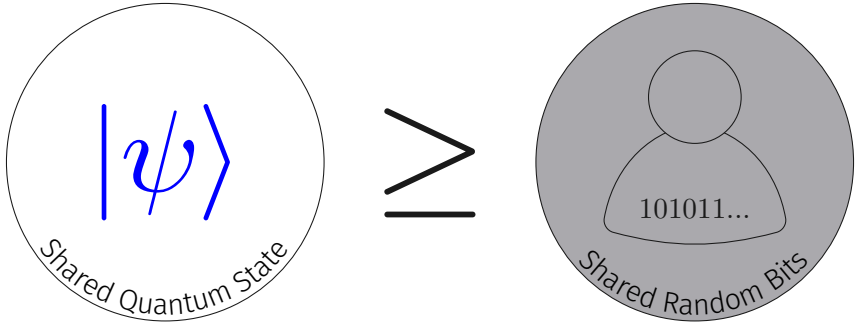
Tight Limits on Nonlocality from Nontrivial Communication Complexity

Noah Shutty, joint work with Mary Wootters and Patrick Hayden
Stanford University

Entanglement is strictly better than *shared random coins* for some tasks.



Such tasks include ***nonlocal games*** and ***distributed computation***.

CHSH[1]*, a Nonlocal Game:*

[1][CHSH69]

CHSH[1]*, a Nonlocal Game:*

Players Win if $xy = a + b \mod 2$

[1][CHSH69]

CHSH[1], *a Nonlocal Game:*

Players Win if $xy = a + b \mod 2$

[1][CHSH69]

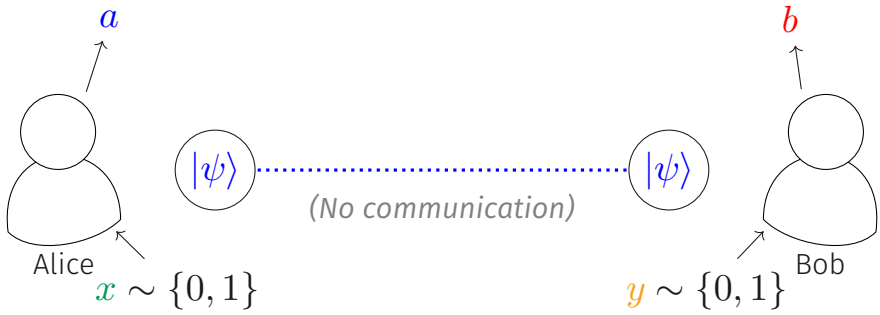
CHSH[1], *a Nonlocal Game:*

Players Win if $xy = a + b \mod 2$

Classical Players win 75% of games

[1][CHSH69]

CHSH[2], *a Nonlocal Game:*

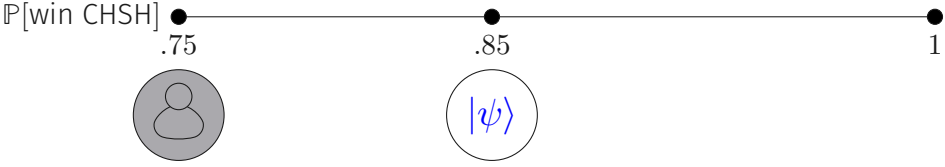


Players Win if $xy = a + b \mod 2$

Classical Players win 75% of games

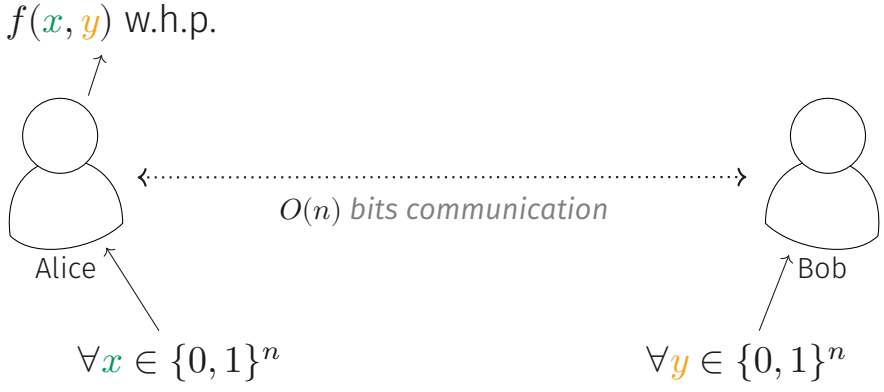
Entangled Players win $\approx$ 85.3% of games

[2][CHSH69]

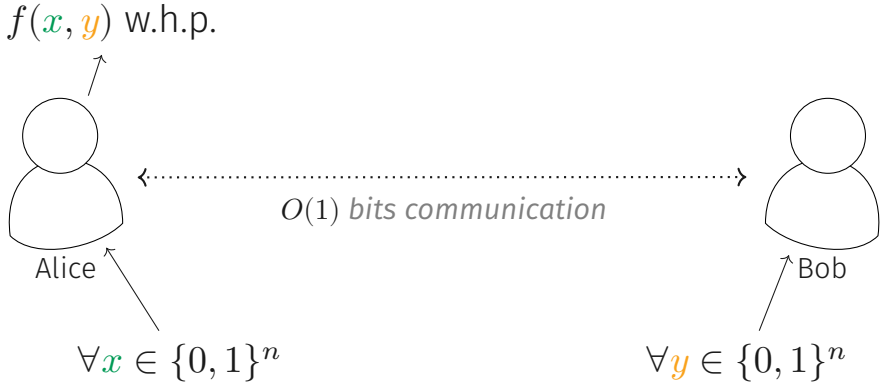

ℙ[win CHSH]
.75
.85
1
$|\psi\rangle$

Distributed Computation:

Distributed Computation:

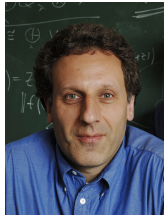


Trivial Communication Complexity:



What is the relationship between *nonlocal games* and *trivial communication complexity*?



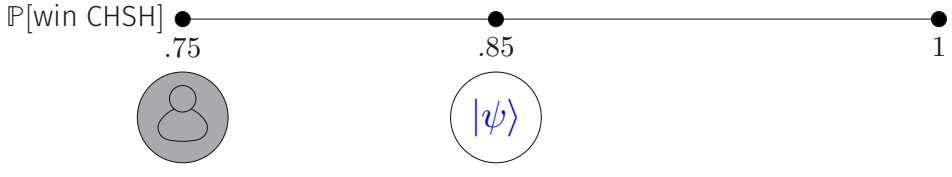



Brassard Buhrman Linden Méthot Tapp Unger

Theorem [BBL+06] (informal)

Communication complexity is trivial if two players win more than $\approx 90.8\%$ of CHSH games.

What is the relationship between *nonlocal games* and *trivial communication complexity*?

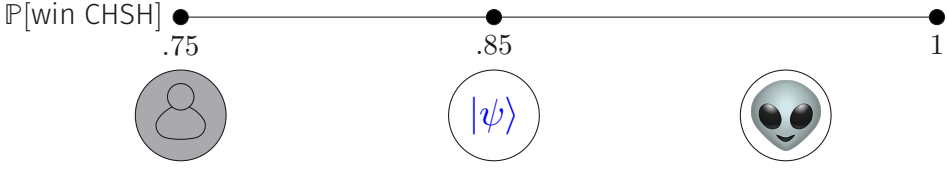


Theorem [Cleve], [van Dam], [Brassard, Buhrman, Linden, Méthot, Tapp, and Unger]

If it were possible to win CHSH with $\mathbb{P}[\text{win}] > .908$, communication complexity would become trivial.

$\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.908$

What is the relationship between *nonlocal games* and *trivial communication complexity*?

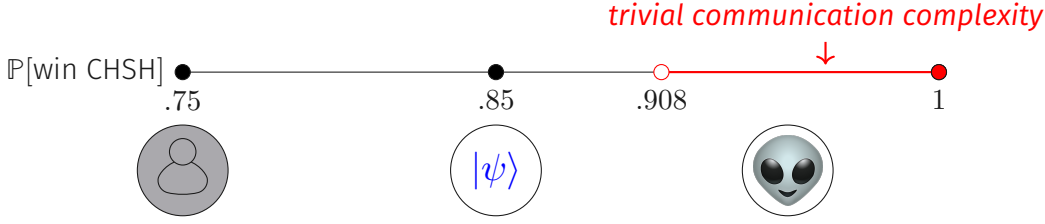


Theorem [Cleve], [van Dam], [Brassard, Buhrman, Linden, Méthot, Tapp, and Unger]

If it were possible to win CHSH with $\mathbb{P}[\text{win}] > .908$, communication complexity would become trivial.

$\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.908$

What is the relationship between *nonlocal games* and *trivial communication complexity*?



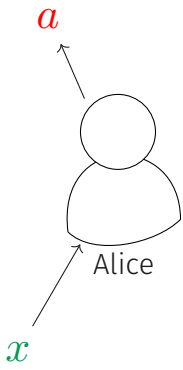
Theorem [Cleve], [van Dam], [Brassard, Buhrman, Linden, Méthot, Tapp, and Unger]

If it were possible to win CHSH with $\mathbb{P}[\text{win}] > .908$, communication complexity would become trivial.

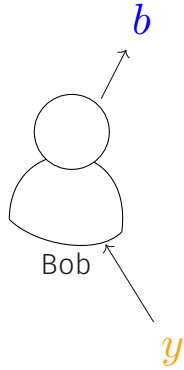
$\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.908$

Alice + Bob's strategy as a conditional probability distribution:

Alice + Bob's strategy as a conditional probability distribution:



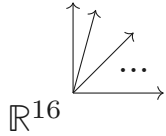
$$\mathbb{P}[a, b | x, y] \in \mathbb{R}^{16}$$



Alice + Bob's strategy as a conditional probability distribution:

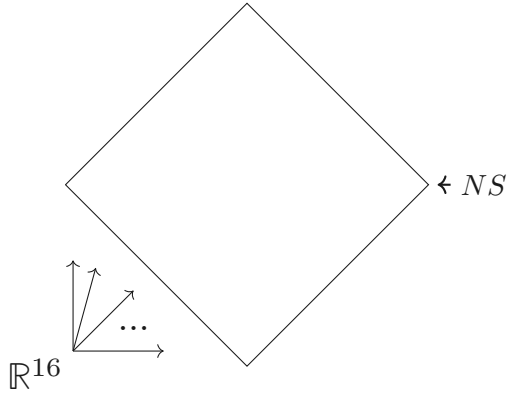
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^{16}$$

Alice + Bob's strategy as a conditional probability distribution:



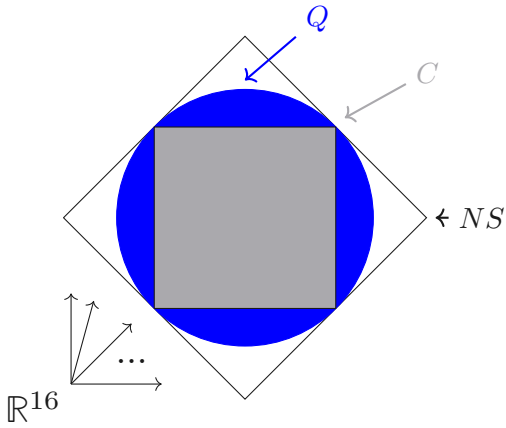
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^{16}$$

Alice + Bob's strategy as a conditional probability distribution:



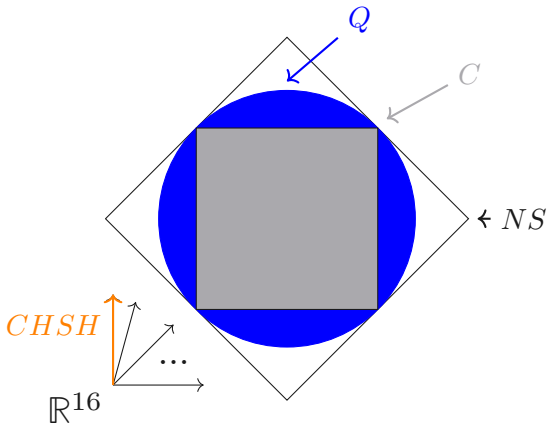
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^{16}$$

Alice + Bob's strategy as a conditional probability distribution:



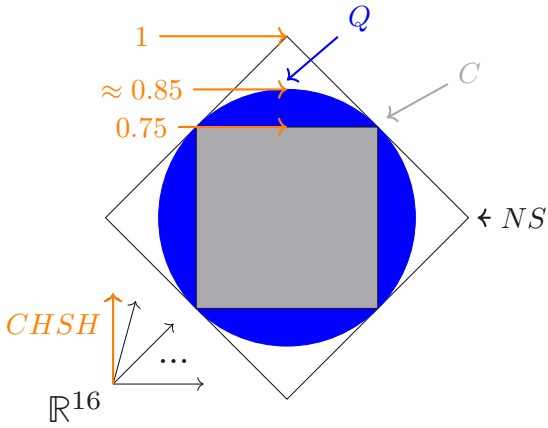
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^{16}$$

Alice + Bob's strategy as a conditional probability distribution:



$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^{16}$$

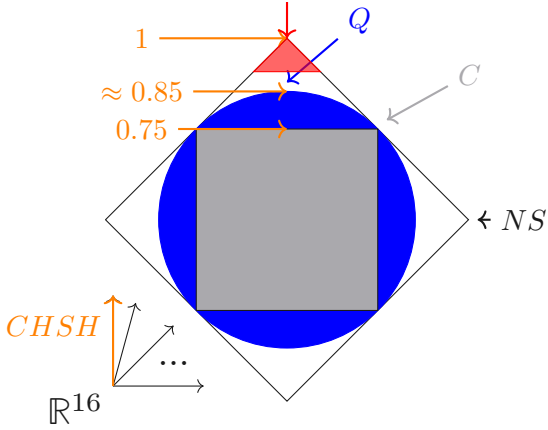
Alice + Bob's strategy as a conditional probability distribution:



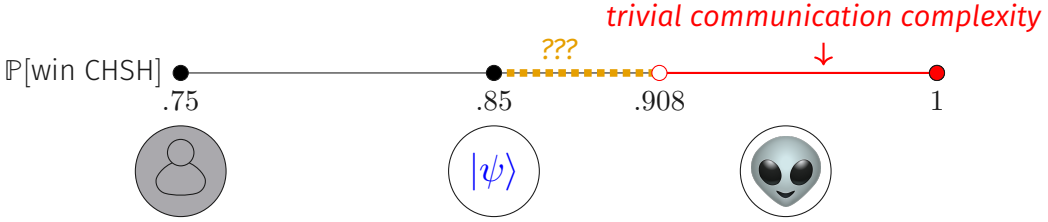
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^{16}$$

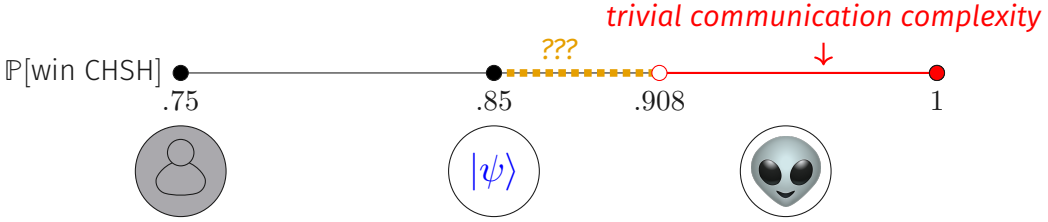
Alice + Bob's strategy as a conditional probability distribution:

trivial communication complexity [BBL+06, vD13, Cle]

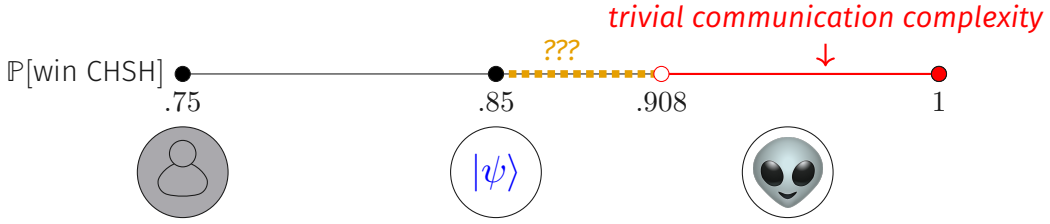


$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^{16}$$


trivial communication complexity
???
ℙ[win CHSH]
.75
.85
.908
1
$|\psi\rangle$



The [BBLMTU] proof used the fact that formulas of $\mathrm{AND}_\epsilon, \mathrm{XOR}_0$ gates for $\epsilon < 1/6$ support reliable computation.



The [BBLMTU] proof used the fact that formulas of $\mathrm{AND}_\epsilon, \mathrm{XOR}_0$ gates for $\epsilon < 1/6$ support reliable computation.

We give a tight upper bound that limits this approach:

Theorem 1

Reliable computation by formulas of ϵ-noisy AND gates and noise-free XOR gates is impossible for $\epsilon \geq 1/6$

Question

Is there a nonlocal game for which *any super-quantum success probability* causes communication complexity to become trivial?

Question

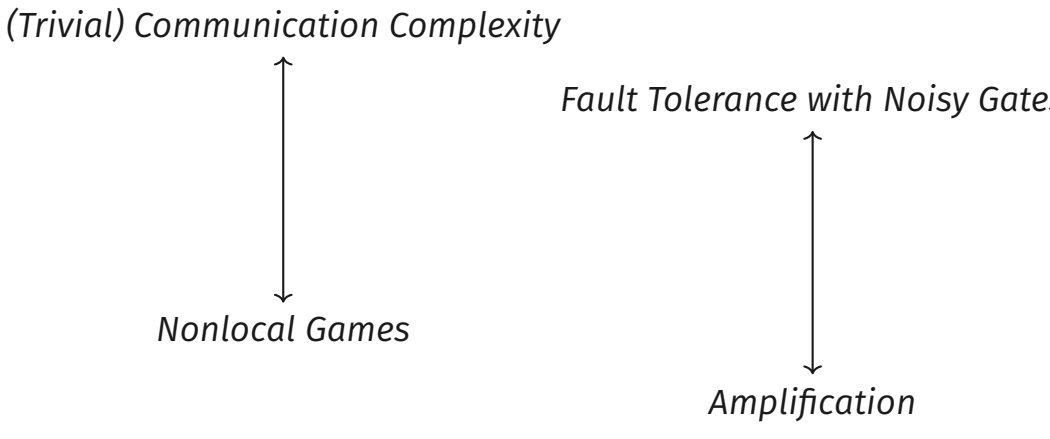
Is there a nonlocal game for which *any super-quantum success probability* causes communication complexity to become trivial?

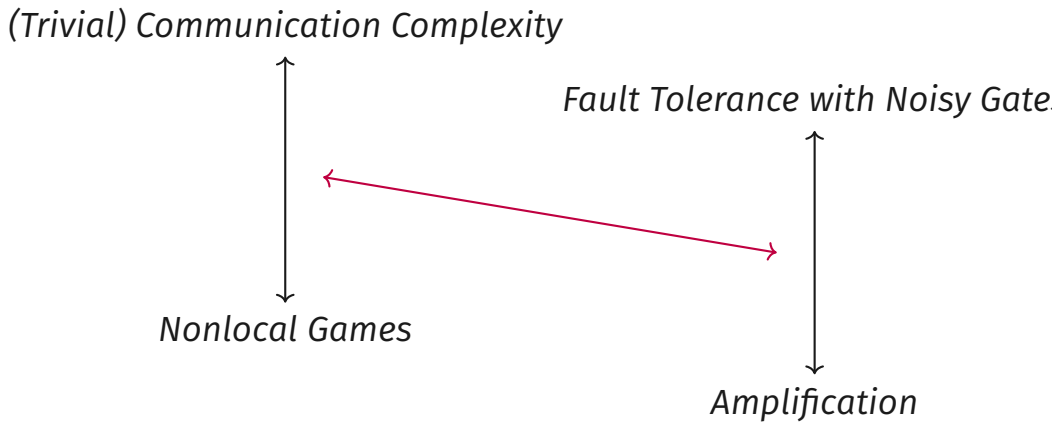
Theorem 3

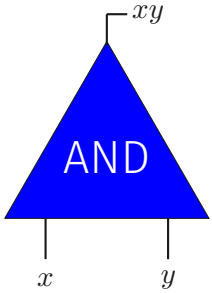
Yes.

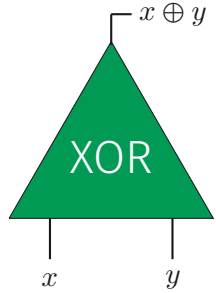
(Trivial) Communication Complexity

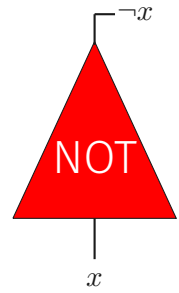
Nonlocal Games

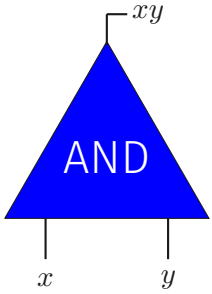

(Trivial) Communication Complexity
Nonlocal Games
Fault Tolerance with Noisy Gates
Amplification

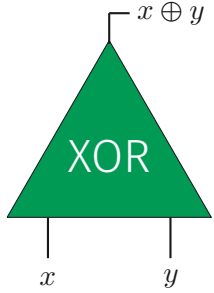

(Trivial) Communication Complexity
Fault Tolerance with Noisy Gates
Nonlocal Games
Amplification

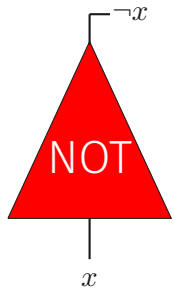

xy
AND
x
y


$x \oplus y$
XOR
x
y


$\neg x$
NOT
x

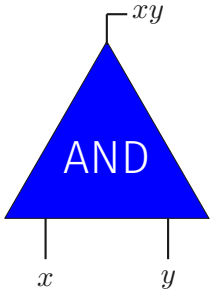


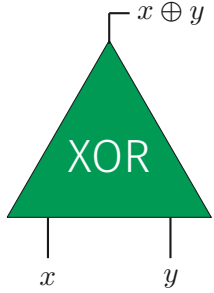


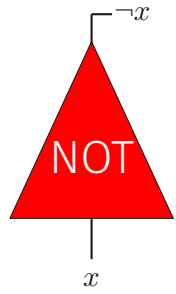


Question

Can you compute an arbitrary function using a formula of AND, XOR, and NOT gates?





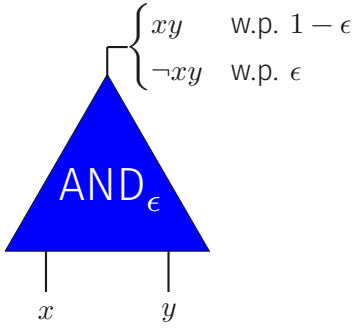


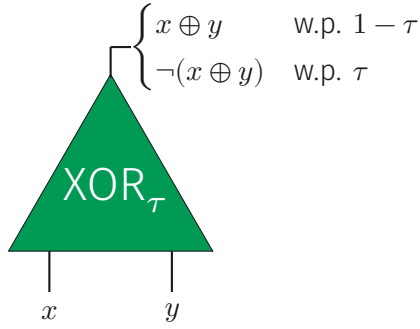
Question

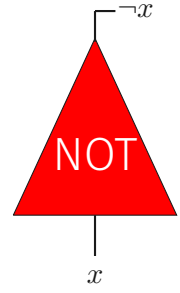
Can you compute an arbitrary function using a formula of AND, XOR, and NOT gates?

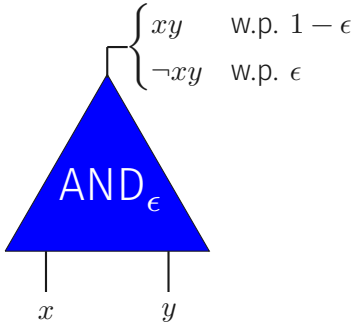
Answer

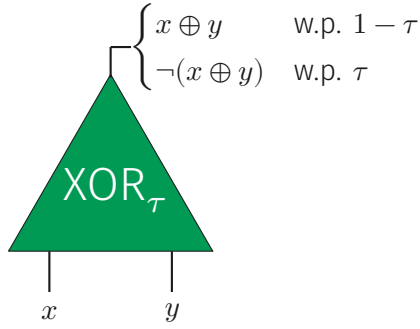
Yes! This set of gates is functionally universal.

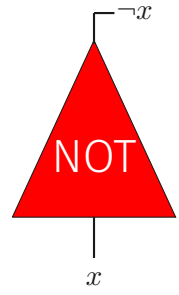

xy w.p. $1-\epsilon$
$\neg xy$ w.p. ϵ
AND$_\epsilon$
x
y


$x \oplus y$ w.p. $1-\tau$
$\neg(x \oplus y)$ w.p. τ
XOR$_\tau$
x
y


$\neg x$
NOT
x

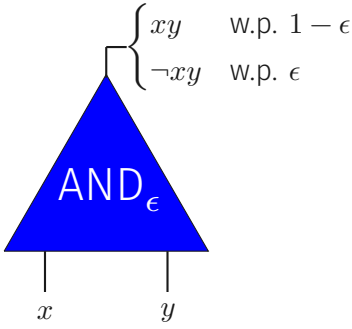


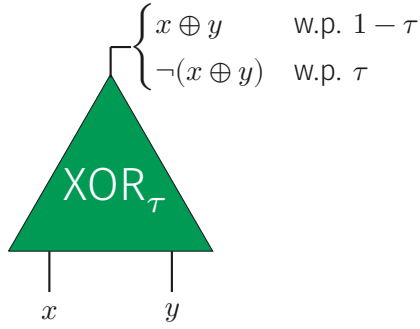


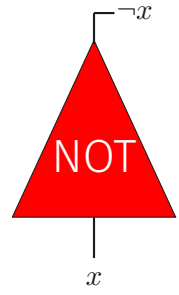


Question

Can you compute an arbitrary function with *bounded probability of error* using a formula of AND_ϵ, XOR_τ, and NOT gates?





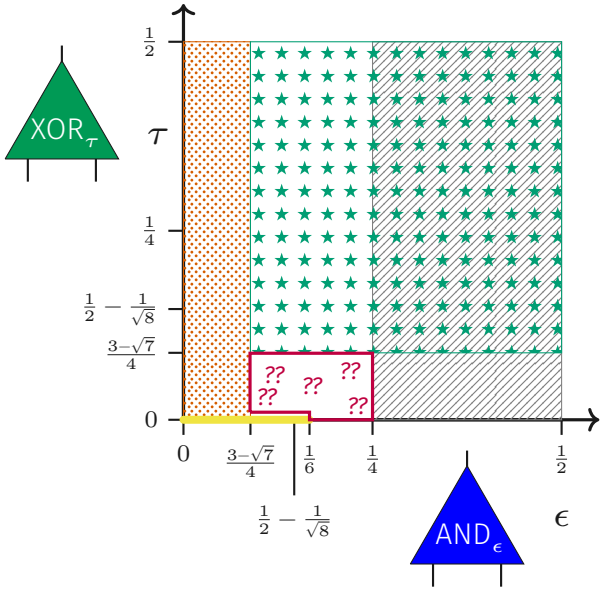


Question

Can you compute an arbitrary function with *bounded probability of error* using a formula of AND_ϵ, XOR_τ, and NOT gates?

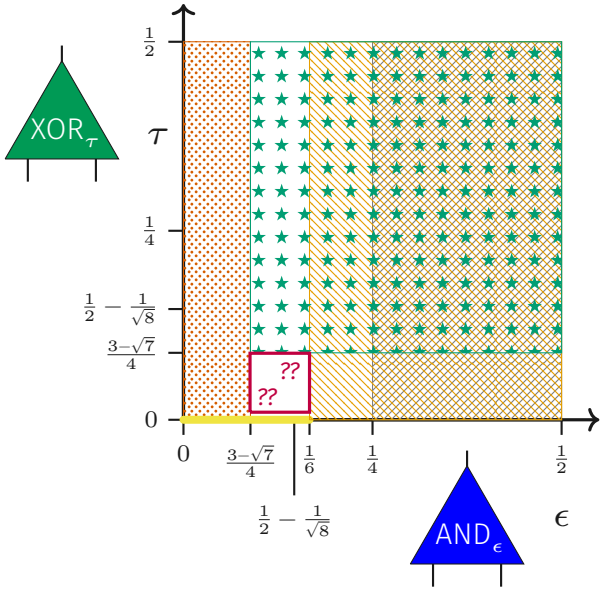
Answer

It depends on ϵ and τ!



Yes
- [EP98]
- [BBL$^+$06]

No
- folklore
- [ES99, EP98, Ung07]



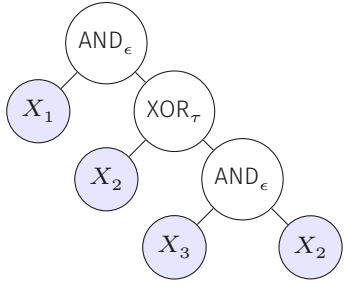
Yes
- [EP98]
- [BBL$^+$06]

No
- folklore
- [ES99, EP98, Ung07]
- our work

Noise Threshold Proof Ingredients:

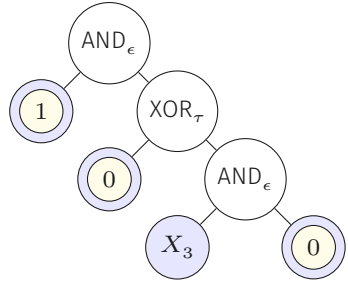
Noise Threshold Proof Ingredients:

- Probabilistic version of Pippenger's reduction [Pip88]
- Taming noise-free XOR gates



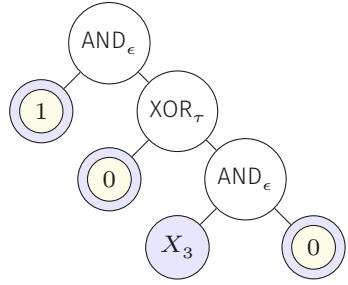
Noise Threshold Proof Ingredients:

- Probabilistic version of Pippenger's reduction [Pip88]
- Taming noise-free XOR gates



Noise Threshold Proof Ingredients:

- Probabilistic version of Pippenger's reduction [Pip88]
- Taming noise-free XOR gates



Question: Is there a ***simple characterization*** of which noisy gate sets allow for fault-tolerant classical computation?

Question: Is there a ***simple characterization*** of which noisy gate sets allow for fault-tolerant classical computation?

Simplifying Assumption: We are allowed to use convex combinations of circuits.

$\sum_i p_i C_i :=$ "with probability p_i, apply circuit C_i"

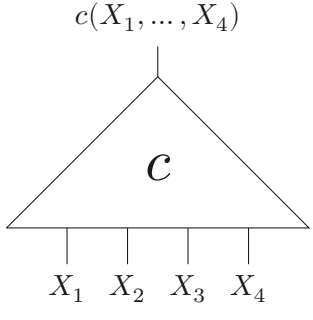
Question: Is there a ***simple characterization*** of which noisy gate sets allow for fault-tolerant classical computation?

Simplifying Assumption: We are allowed to use convex combinations of circuits.

$\sum_i p_i C_i :=$ "with probability p_i, apply circuit C_i"

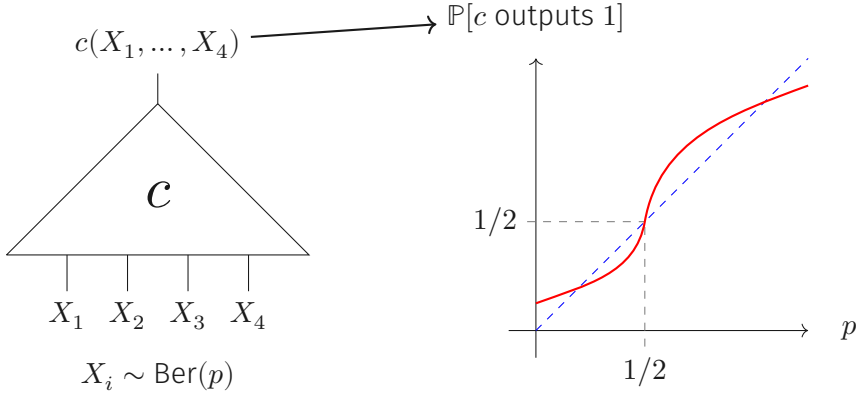
Answer: Yes, there is a simple characterization.

An ***amplifier*** is any circuit c, such that if we feed in i.i.d. bits $\sim$ Bernoulli(p), we get something like this:



Amplifier away from $1/2$

An ***amplifier*** is any circuit c, such that if we feed in i.i.d. bits $\sim$ Bernoulli(p), we get something like this:

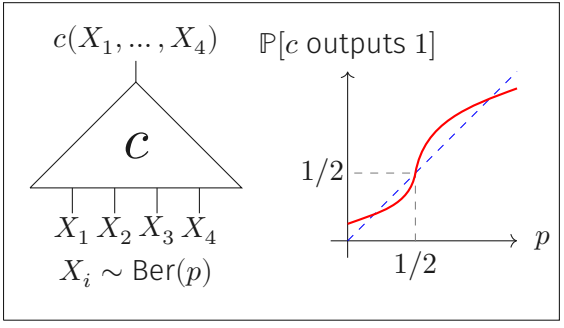


Amplifier away from $1/2$

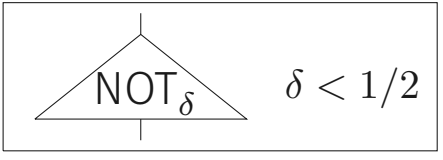
Theorem 2

A set of noisy circuits closed under convex combinations allows fault-tolerant computation if and only if it contains an amplifier away from $1/2$ and a (noisy) NOT gate.

$\Leftrightarrow$



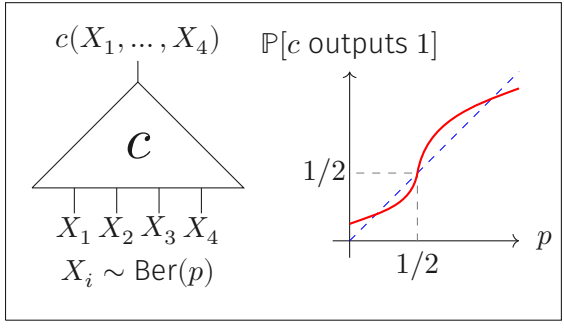
&



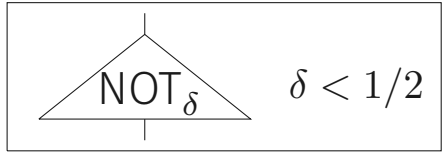
Theorem 2

A set of noisy circuits closed under convex combinations allows fault-tolerant computation if and only if it contains an amplifier away from $1/2$ and a (noisy) NOT gate.

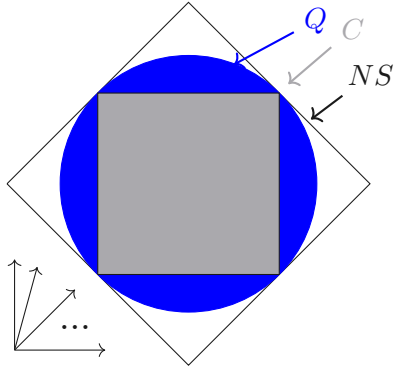
$\Leftrightarrow$



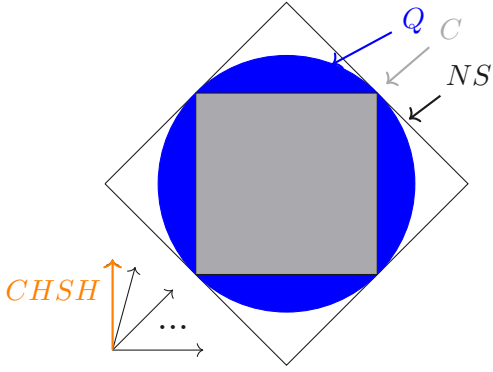
&



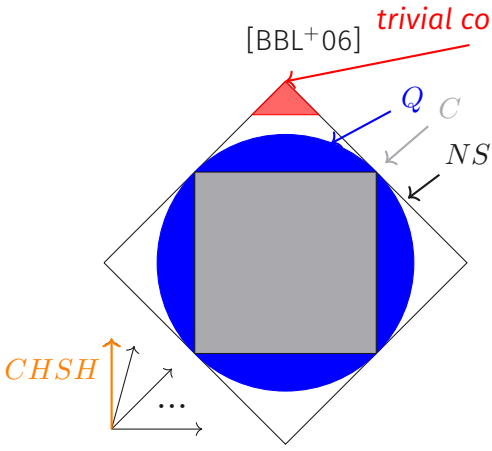
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^N$$



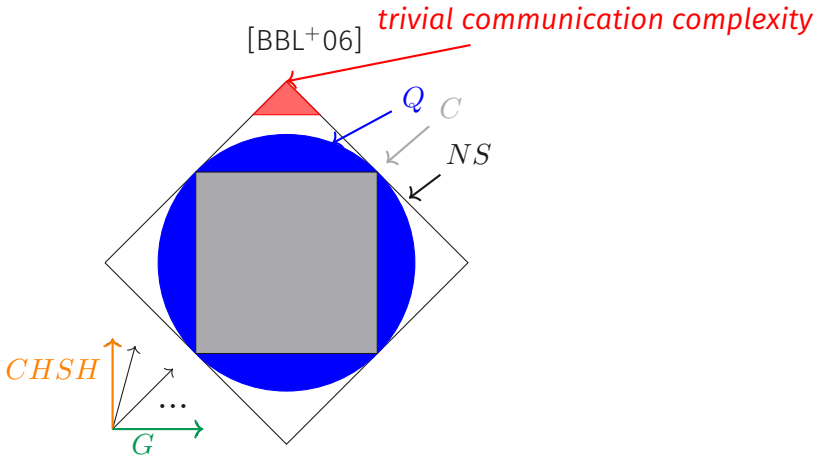
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^N$$



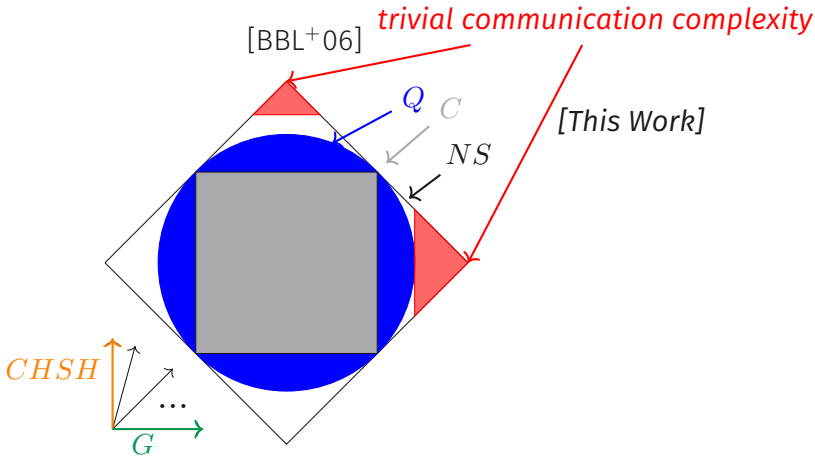
$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^N$$



$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^N$$



$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^N$$



$$\mathbb{P}[a, b|x, y] \in \mathbb{R}^N$$

Question

Is there a nonlocal game for which *any super-quantum success probability* causes communication complexity to become trivial?

Question

Is there a nonlocal game for which *any super-quantum success probability* causes communication complexity to become trivial?

Theorem 3

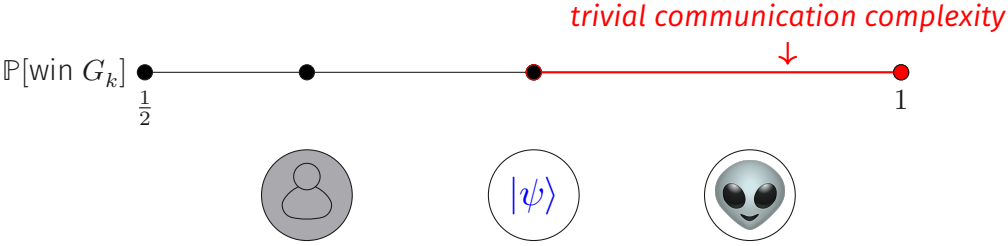
$\forall k \geq 1$, there is a nonlocal game G_k, such that a win probability above the quantum value causes communication complexity to become trivial.

Question

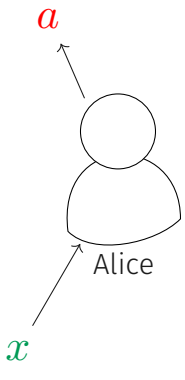
Is there a nonlocal game for which *any super-quantum success probability* causes communication complexity to become trivial?

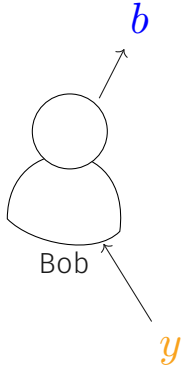
Theorem 3

$\forall k \geq 1$, there is a nonlocal game G_k, such that a win probability above the quantum value causes communication complexity to become trivial. Conversely, if communication complexity is trivial, then $\exists k$ such that the win probability for G_k is above the quantum value.

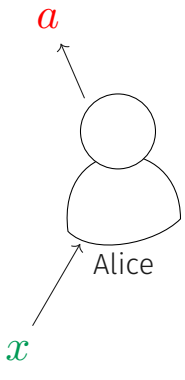

trivial communication complexity
$\mathbb{P}[\text{win } G_k]$
$\frac{1}{2}$
1
$|\psi\rangle$

Alice + Bob as a conditional probability distribution:

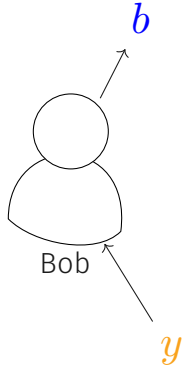




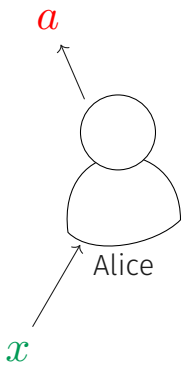
Alice + Bob as a conditional probability distribution:



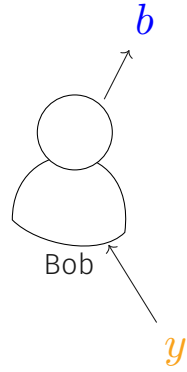
$$\mathbb{P}[a, b | x, y]$$



Alice + Bob as a conditional probability distribution:

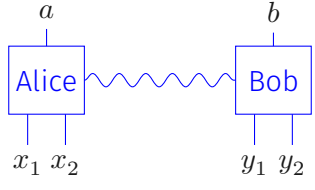


$$\mathbb{P}[a, b|x, y]$$

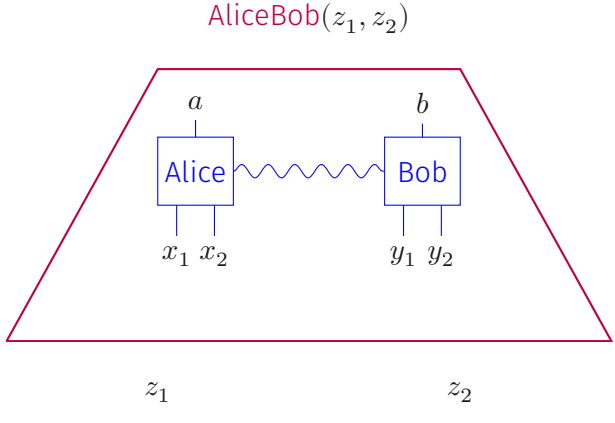


$$\mathbb{P}[\text{win game}] = \sum_{x,y,a,b} \mathbb{P}[a, b|x, y]\mathbb{P}[x, y]V(a, b; x, y)$$

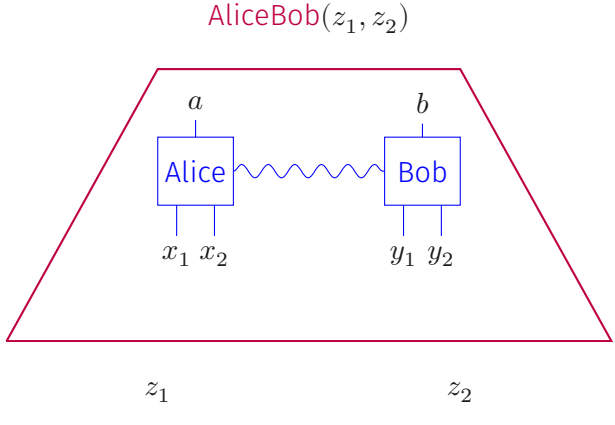
Turning Strategies (Conditional Probability Distributions) Into Gates:



Turning Strategies (Conditional Probability Distributions) Into Gates:

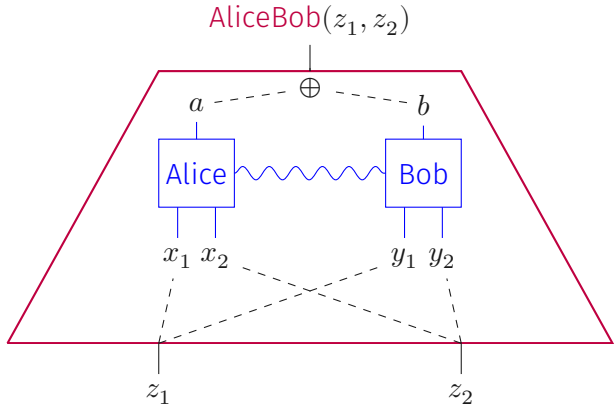


Turning Strategies (Conditional Probability Distributions) Into Gates:



pick $x_i \sim \{0,1\}$, $y_i = z_i + x_i \mod 2$

Turning Strategies (Conditional Probability Distributions) Into Gates:



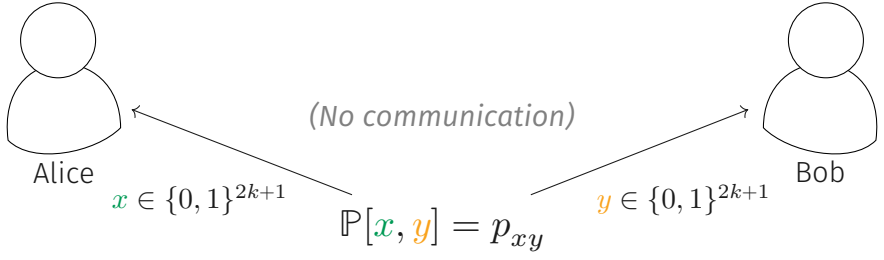
pick $x_i \sim \{0,1\}$, $y_i = z_i + x_i \mod 2$

The Nonlocal Game G_k:

Fix $k \geq 1$.

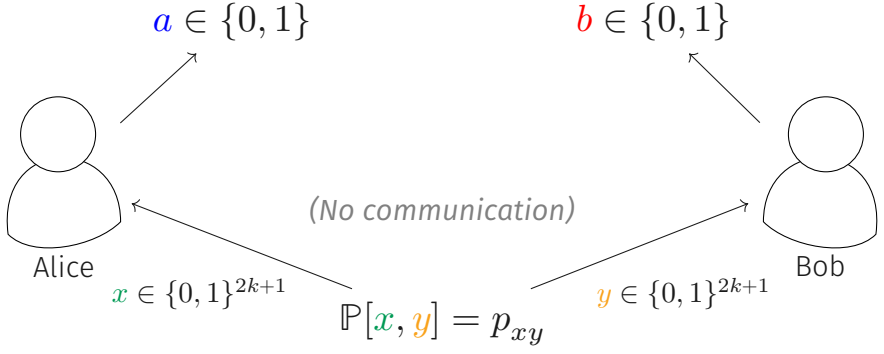
The Nonlocal Game G_k:

Fix $k \geq 1$.



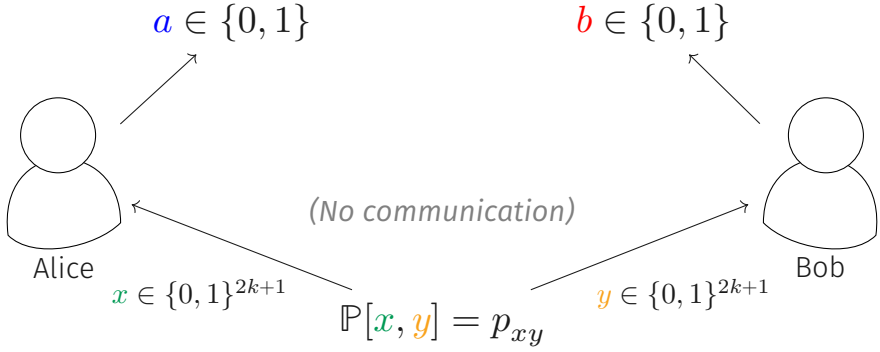
The Nonlocal Game G_k:

Fix $k \geq 1$.



The Nonlocal Game G_k:

Fix $k \geq 1$.



Players Win if $\mathrm{Maj}_{2k+1}(x+y) = a+b$

For some choice of p_{xy}, any $\mathbb{P}[\text{win } G_k]$ above quantum implies that AliceBob is an amplifier away from $1/2$.

For some choice of p_{xy}, any $\mathbb{P}[\text{win } G_k]$ above quantum implies that AliceBob is an amplifier away from $1/2$.

There is also an AliceBob NOT gate, so by Theorem 2 there is fault tolerant computation by AliceBob circuits.

For some choice of p_{xy}, any $\mathbb{P}[\text{win } G_k]$ above quantum implies that AliceBob is an amplifier away from $1/2$.

There is also an AliceBob NOT gate, so by Theorem 2 there is fault tolerant computation by AliceBob circuits.

Alice and Bob can simulate arbitrary circuits of AliceBob gates with constant communication using shared random coins.

For some choice of p_{xy}, any $\mathbb{P}[\text{win } G_k]$ above quantum implies that AliceBob is an amplifier away from $1/2$.

There is also an AliceBob NOT gate, so by Theorem 2 there is fault tolerant computation by AliceBob circuits.

Alice and Bob can simulate arbitrary circuits of AliceBob gates with constant communication using shared random coins.

This implies that communication complexity is trivial for such Alice and Bob.

How to modify nonlocal game to have quantum advantage:

How to modify nonlocal game to have quantum advantage:

$$G \longrightarrow qG + (1-q)\text{Magic}$$


Gilles Brassard, Harry Buhrman, Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger.
Limit on nonlocality in any world in which communication complexity is not trivial.
Physical Review Letters, 96(25):250401, 2006.


John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt.
Proposed experiment to test local hidden-variable theories.
Physical review letters, 23(15):880, 1969.


Richard Cleve.
personal communication.


William Evans and Nicholas Pippenger.
On the maximum tolerable noise for reliable computation by formulas.
IEEE Transactions on Information Theory, 44(3):1299–1305, 1998.

William S Evans and Leonard J Schulman.
Signal propagation and noisy circuits.
IEEE Transactions on Information Theory, 45(7):2367–2373, 1999.

Nicholas Pippenger.
Reliable computation by formulas in the presence of noise.
IEEE Transactions on Information Theory, 34(2):194–197, 1988.

Noah Shutty, Mary Wootters, and Patrick Hayden.
Tight limits on nonlocality from nontrivial communication complexity; aka reliable computation with asymmetric gate noise.
In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 206–217. IEEE, 2020.

Falk Unger.
Noise threshold for universality of 2-input gates.
In *IEEE International Symposium on Information Theory (ISIT)*, pages 1901–1905. IEEE, 2007.

Wim van Dam.
Implausible consequences of superstrong nonlocality.
Natural Computing, 12(1):9–12, 2013.

Thank you for listening.

arXiv/1809.09748