Quantum Nonlocality and Communication Complexity

Richard Cleve
University of Waterloo

February 16,20,21,22,23 2006
(first 5 lectures) IHP, Paris

Quantum information can apparently be used to substantially reduce ***computation*** costs for a number of interesting problems, and to provide novel forms of ***cryptographic security***

We’ll explore this question:

How does quantum information affect the ***communication costs*** of information processing tasks?

Main Topics

1. Nonlocality à la Bell, CHSH, GHZ
2. Communication complexity
3. Nonlocal games

Contents of Lecture 1

- What quantum information ***cannot*** do
- The GHZ "paradox"
- The Bell inequality and its violation
  - Physicist's perspective
  - Computer scientist's perspective

- What quantum information ***cannot*** do
- The GHZ “paradox”
- The Bell inequality and its violation
  - Physicist’s perspective
  - Computer scientist’s perspective

How much classical information in n qubits?

$2^n - 1$ complex numbers apparently needed to ***specify*** an arbitrary n-qubit pure quantum state:

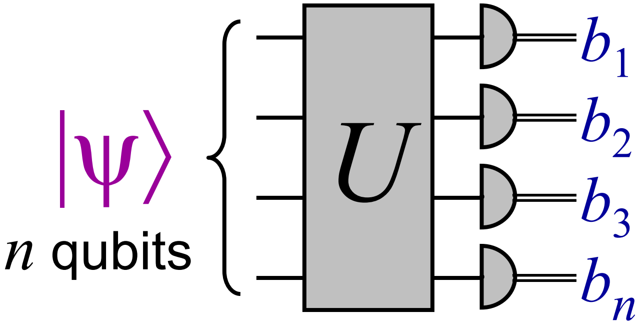
$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \ldots + \alpha_{111}|111\rangle$

Does this mean that an exponential amount of classical information is somehow ***stored*** in n qubits?

No! Holevo's Theorem [1973] implies: cannot convey more than n bits of information in n qubits

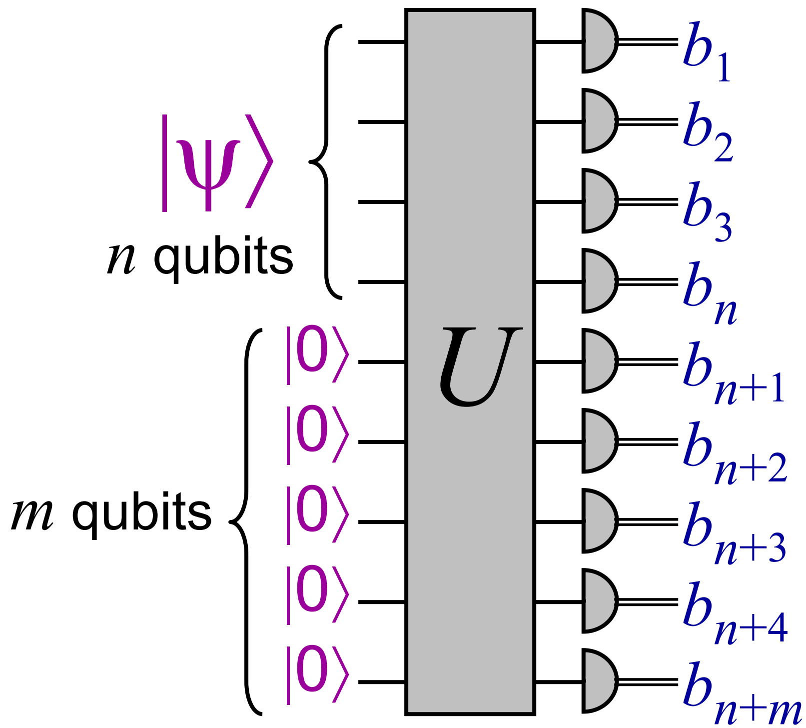
Holevo’s Theorem

Easy case:



$b_1 b_2 \ldots b_n$ cannot convey more than n bits!

Hard case (the general case):



(proof omitted here)

Entanglement and signaling

Recall that entangled states, such as $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$,

can be used to perform some intriguing feats, such as ***teleportation*** and ***superdense coding***

—but they ***cannot*** be used to "signal instantaneously"

Any operation performed on one system has no affect on the state of the other system (its reduced density matrix)

Basic communication scenario

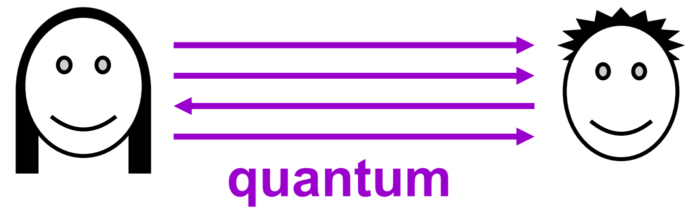
Goal: convey n bits from Alice to Bob

Basic communication scenario

Bit communication:

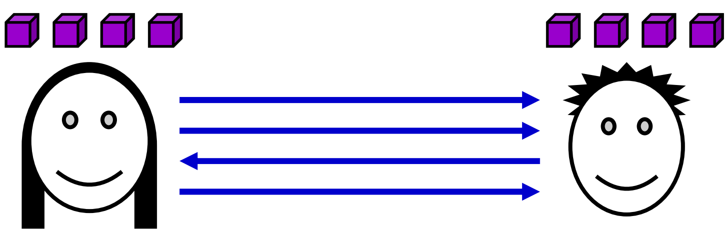
Cost: n

Qubit communication:



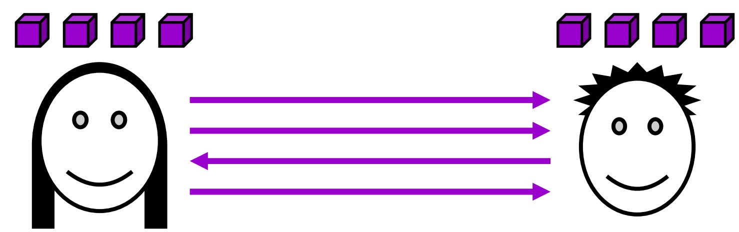
Cost: n [Holevo's Theorem, 1973]

Bit communication & prior entanglement:



Cost: n (can be deduced)

Qubit communication & prior entanglement:



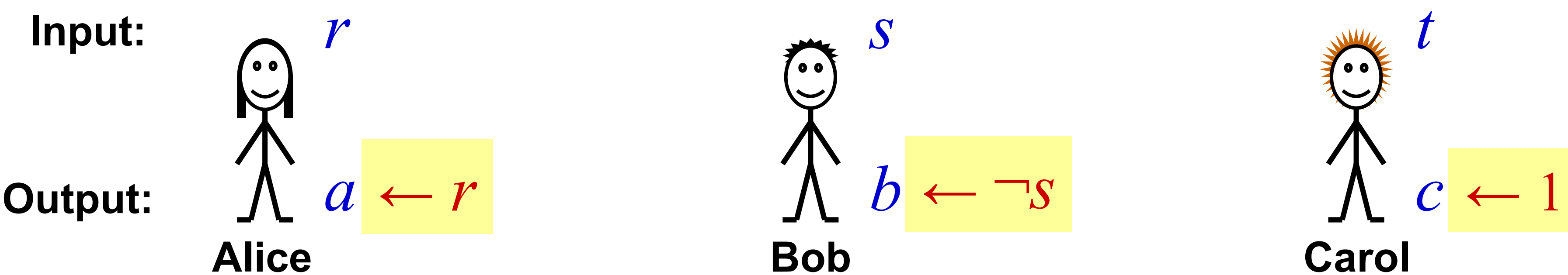
Cost: $n/2$ superdense coding

[Bennett & Wiesner, 1992]

- What quantum information ***cannot*** do
- The GHZ "paradox"
- The Bell inequality and its violation
  - Physicist's perspective
  - Computer scientist's perspective

GHZ scenario

[Greenberger, Horne, Zeilinger, 1980]

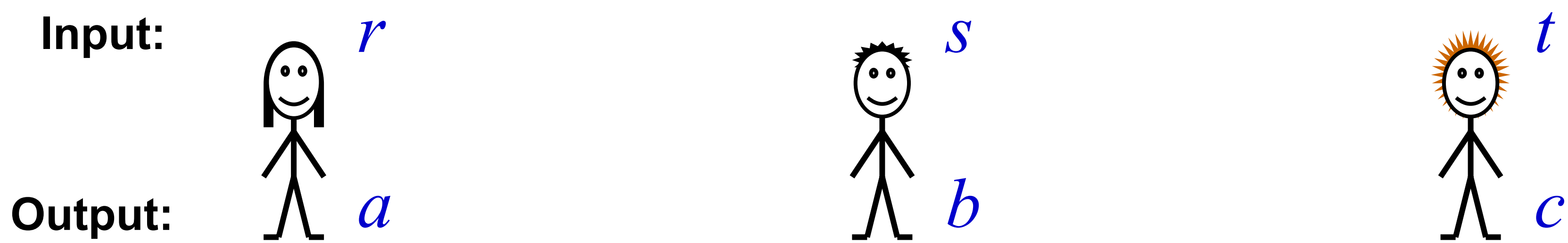


Rules of the game:

1. It is promised that $r \oplus s \oplus t = 0$
2. No communication after inputs received
3. They ***win*** if $a \oplus b \oplus c = r \vee s \vee t$

rst	$a \oplus b \oplus c$	abc
000	0	011
011	1	001
101	1	111
110	1	101

No perfect strategy for GHZ



rst	$a \oplus b \oplus c$
000	0
011	1
101	1
110	1

General deterministic strategy:

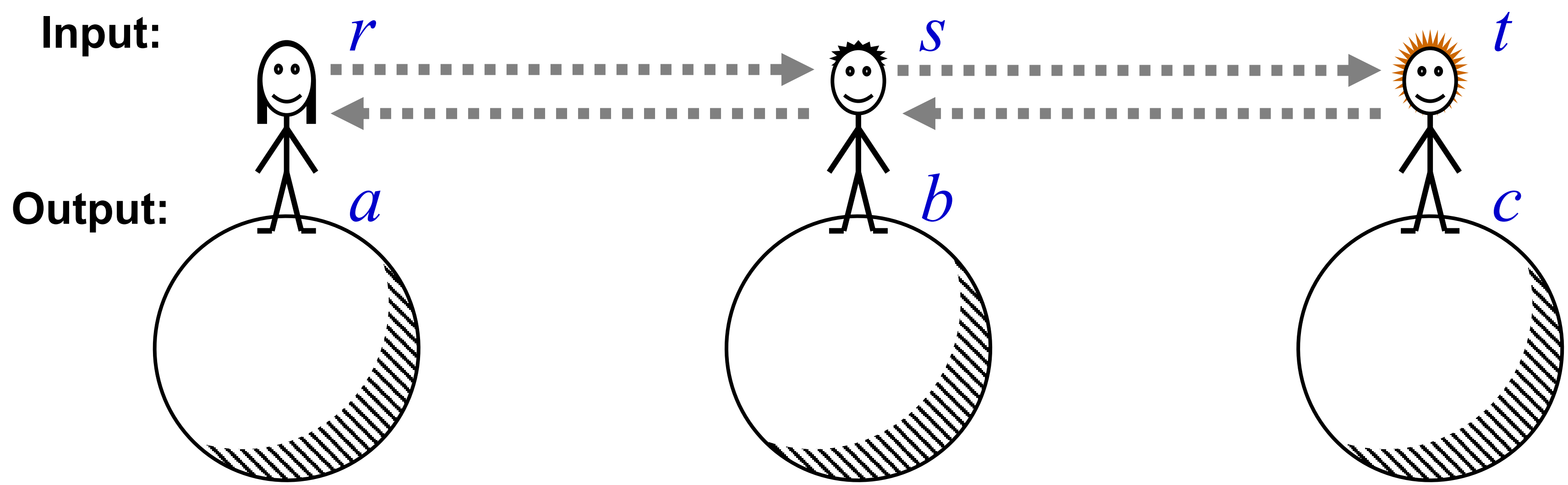
$a_0, a_1, b_0, b_1, c_0, c_1$

Winning conditions:

$$\begin{cases} a_0 \oplus b_0 \oplus c_0 = 0 \\ a_0 \oplus b_1 \oplus c_1 = 1 \\ a_1 \oplus b_0 \oplus c_1 = 1 \\ a_1 \oplus b_1 \oplus c_0 = 1 \end{cases}$$

Has no solution, thus no perfect strategy exists

GHZ: preventing communication

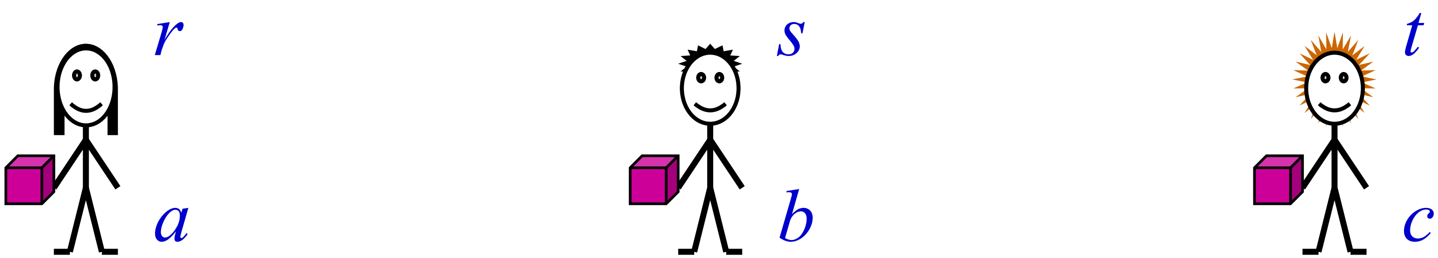


Input and output events can be ***space-like*** separated:
so signals at the speed of light are not fast enough for cheating

What if Alice, Bob, and Carol ***still*** keep on winning?

"GHZ Paradox" explained

Prior entanglement: $|\psi\rangle = |000\rangle - |011\rangle - |101\rangle - |110\rangle$



<u>Alice's strategy:</u>

1. if $r = 1$ then apply H to qubit
2. measure qubit and set a to result

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

<u>Bob's & Carol's strategies:</u> similar

Case 1 ($rst = 000$)**:** state is measured directly …

Case 2 ($rst = 011$)**:** new state $|001\rangle + |010\rangle - |100\rangle + |111\rangle$

(other cases similar by symmetry)

GHZ: conclusions

- For the GHZ game, any ***classical*** team succeeds with probability at most ¾
- Allowing the players to communicate would enable them to succeed with probability 1
- Entanglement cannot be used to communicate
- Nevertheless, allowing the players to have entanglement enables them to succeed with probability 1
- Thus, entanglement is a useful resource for the task of ***winning the GHZ game***

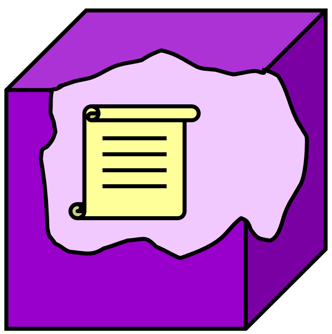
- What quantum information ***cannot*** do
- The GHZ "paradox"
- The Bell inequality and its violation
  - Physicist's perspective
  - Computer scientist's perspective

Bell's Inequality and its violation

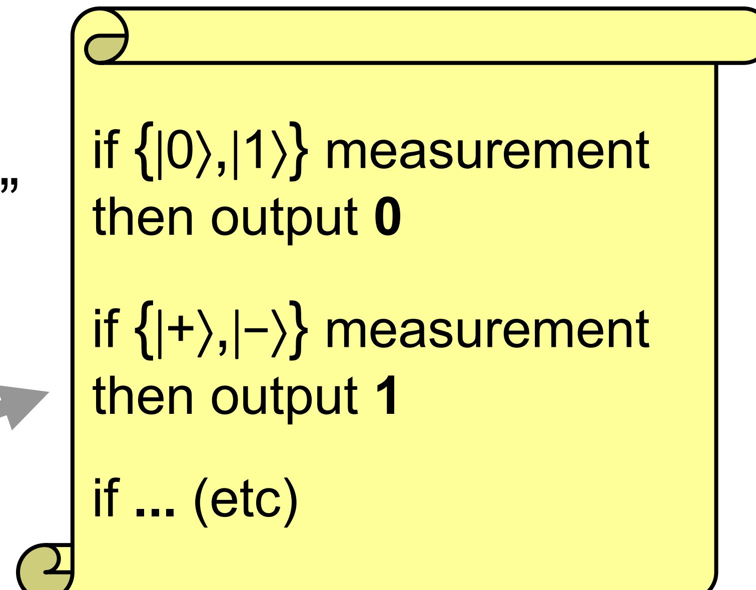
Part I: physicist's view:

Can a quantum state have ***pre-determined*** outcomes for each possible measurement that can be applied to it?

qubit:



where the "manuscript" is something like this:



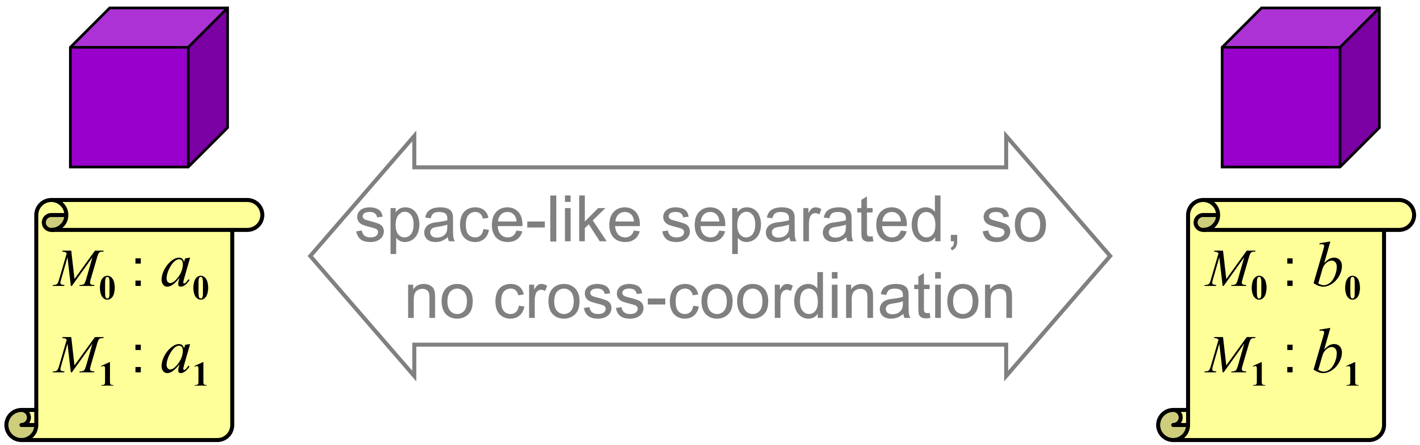
called ***hidden variables***

table could be implicitly given by some formula

[Bell, 1964]
[Clauser, Horne, Shimony, Holt, 1969]

Bell Inequality

Imagine a two-qubit system, where one of two measurements, called M_0 and M_1, will be applied to each qubit:



Define:

$A_0 = (-1)^{a_0}$

$A_1 = (-1)^{a_1}$

$B_0 = (-1)^{b_0}$

$B_1 = (-1)^{b_1}$

Claim: $A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \leq 2$

Proof: $A_0 (B_0 + B_1) + A_1 (B_0 - B_1) \leq 2$

one is ± 2 and the other is 0

Bell Inequality

$A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \leq 2$ is called a ***Bell Inequality****

Question: could one, in principle, design an experiment to check if this Bell Inequality holds for a particular system?

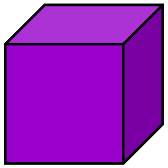
Answer 1: ***no, not directly***, because A_0, A_1, B_0, B_1 cannot all be measured (only ***one*** $A_s B_t$ term can be measured)

Answer 2: ***yes, indirectly***, by making many runs of this experiment: pick a random $st \in \{00, 01, 10, 11\}$ and then measure with M_s and M_t to get the value of $A_s B_t$

The ***average*** of $A_0 B_0$, $A_0 B_1$, $A_1 B_0$, $-A_1 B_1$ should be ≤ ½

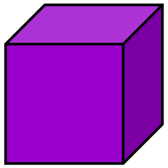
* also called CHSH Inequality

Violating the Bell Inequality



Two-qubit system in state

$|\phi\rangle = |00\rangle - |11\rangle$



Applying rotations θ_A and θ_B yields:

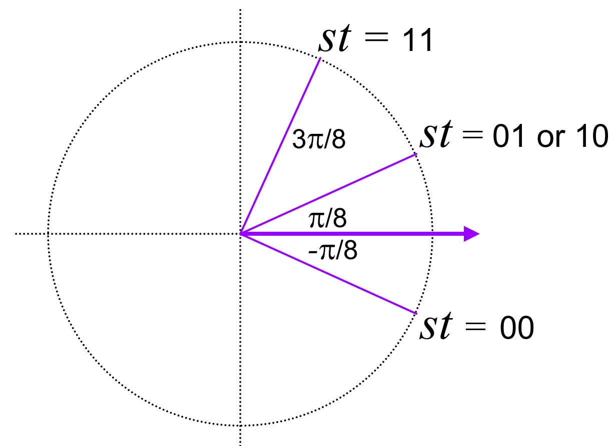
$$\cos(\theta_A + \theta_B)\,\underbrace{(|00\rangle - |11\rangle)}_{AB\,=\,+1} + \sin(\theta_A + \theta_B)\,\underbrace{(|01\rangle + |10\rangle)}_{AB\,=\,-1}$$

Define

M_0: rotate by $-\pi/16$ then measure

M_1: rotate by $+3\pi/16$ then measure

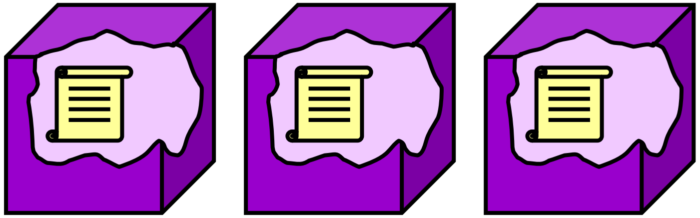
Then $A_0 B_0,\ A_0 B_1,\ A_1 B_0,\ -A_1 B_1$ all have expected value $\frac{1}{2}\sqrt{2}$, which ***contradicts*** the upper bound of ½



$\cos^2(\pi/8) = \frac{1}{2} + \frac{1}{4}\sqrt{2}$

Bell Inequality violation: summary

Assuming that quantum systems are governed by ***local hidden variables*** leads to the Bell inequality

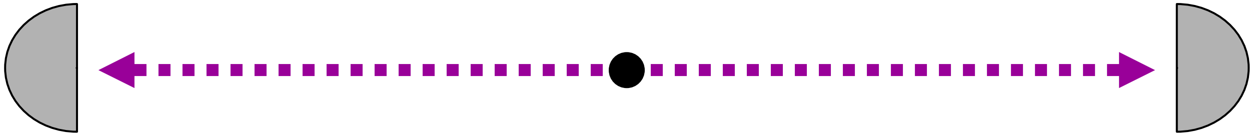


$$A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \leq 2$$

But this is ***violated*** in the case of Bell states (by a factor of $\sqrt{2}$)

Therefore, no such hidden variables exist

This is, in principle, experimentally verifiable, and experiments along these lines have actually been conducted



- What quantum information ***cannot*** do
- The GHZ “paradox”
- The Bell inequality and its violation
  - Physicist’s perspective
  - Computer scientist’s perspective

Bell’s Inequality and its violation

Part II: computer scientist’s view:

input: s t

output: a b

Rules: 1. No communication after inputs received

2. They ***win*** if $a \oplus b = s \wedge t$

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

With classical resources, $\Pr[a \oplus b = s \wedge t] \leq 0.75$

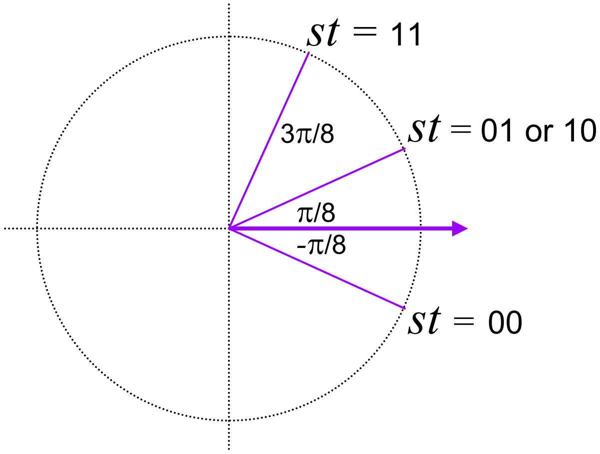
But, with prior entanglement state $|00\rangle - |11\rangle$,
$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = ½ + ¼\sqrt{2} = 0.853\ldots$

The quantum strategy

- Alice and Bob start with entanglement
  $|\phi\rangle = |00\rangle - |11\rangle$

- **Alice:** if $s = 0$ then rotate by $\theta_A = -\pi/16$ else rotate by $\theta_A = +3\pi/16$ and measure

- **Bob:** if $t = 0$ then rotate by $\theta_B = -\pi/16$ else rotate by $\theta_B = +3\pi/16$ and measure



$\cos(\theta_A - \theta_B)\,(|00\rangle - |11\rangle) + \sin(\theta_A - \theta_B)\,(|01\rangle + |10\rangle)$

Success probability:

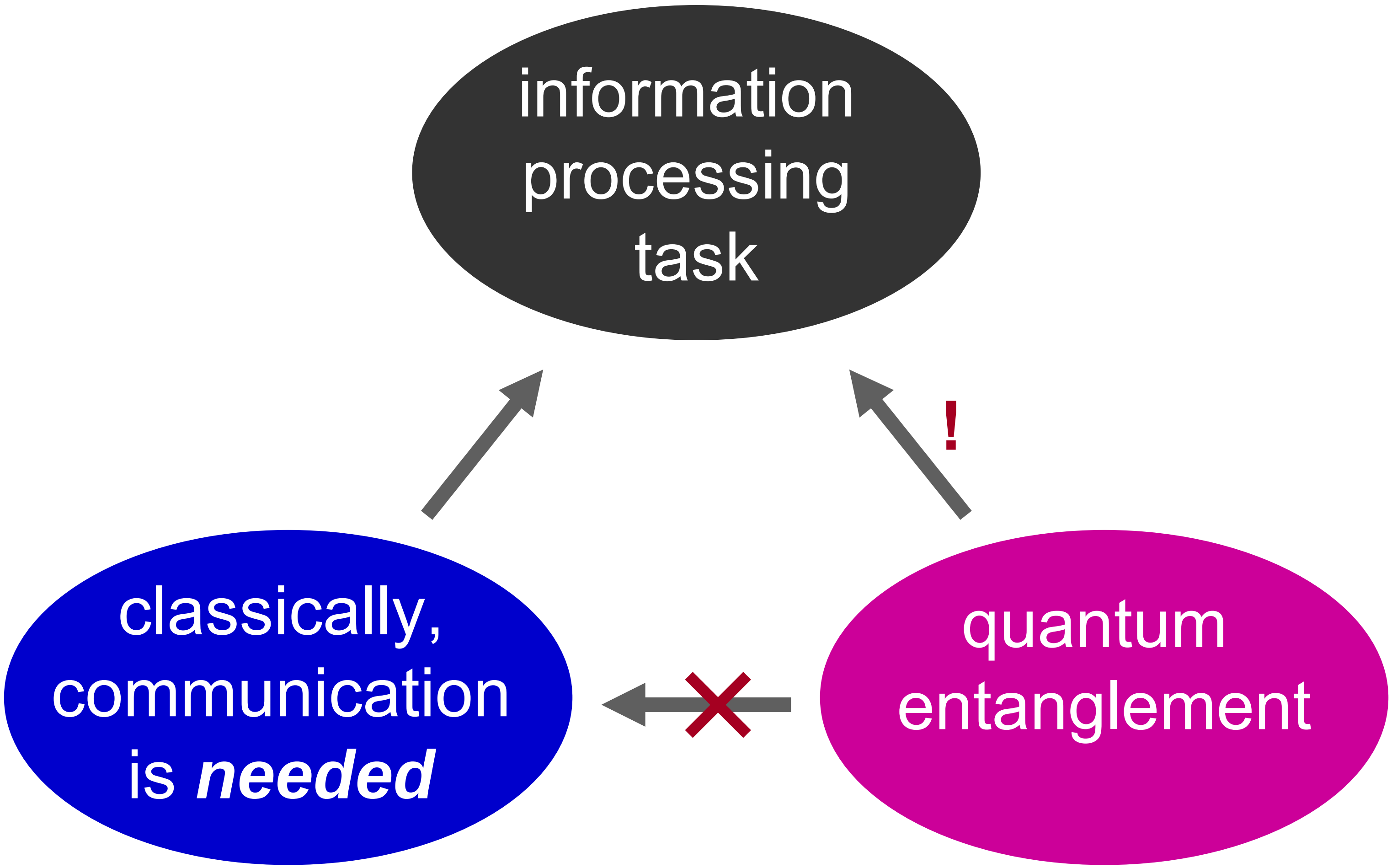
$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = ½ + ¼\sqrt{2} = 0.853\ldots$

The quantum strategy is optimal

Tsirelson [1980]: For ***any*** quantum strategy, the success probability is at most $\cos^2(\pi/8)$

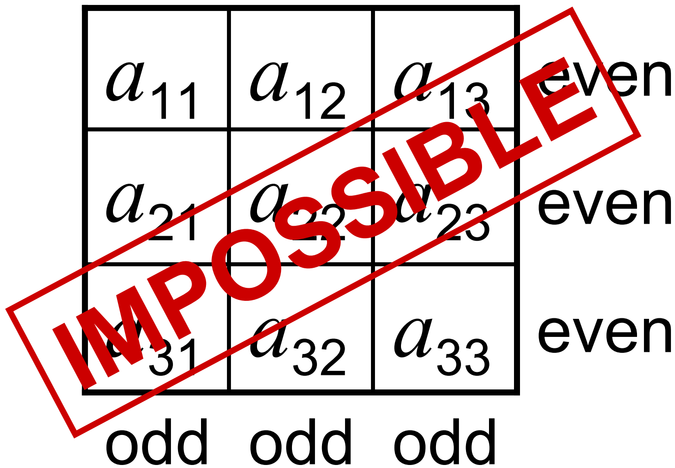
We'll prove this in a future lecture, when we get more deeply into ***nonlocal games***

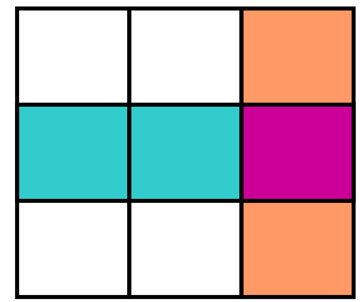
Nonlocality **in operational terms**



Preview: magic square game

Problem: fill in the matrix with bits such that each row has even parity and each column has odd parity





Game: ask Alice to fill in one row and Bob to fill in one column

They ***win*** iff parities are correct and bits agree at intersection

Success probabilities: $8/9$ classical and 1 quantum

[Aravind, 2002] (details omitted here)

THE END

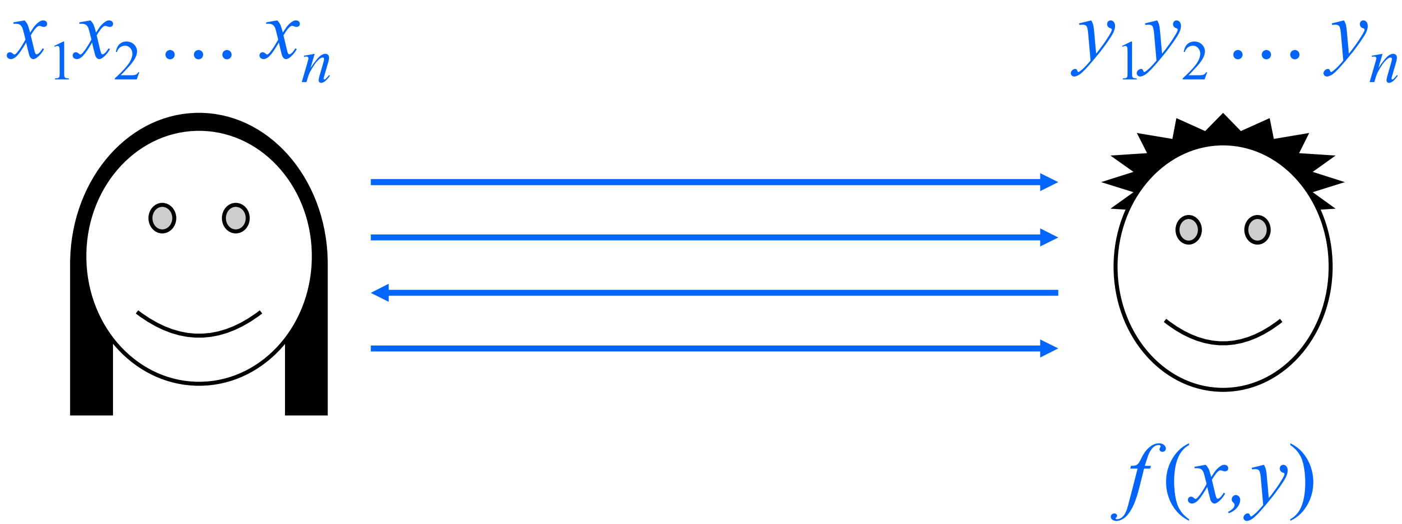
Contents of Lecture 2

- Communication complexity
  - Equality checking
  - Intersection (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
  - Simultaneous message passing & fingerprinting

- Communication complexity
  - Equality checking
  - Intersection (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
  - Simultaneous message passing & fingerprinting

Classical communication complexity

[Yao, 1979]



E.g. equality function: $f(x,y) = 1$ if $x = y$, and 0 if $x \neq y$

Question: can the communication be less than *n* bits?

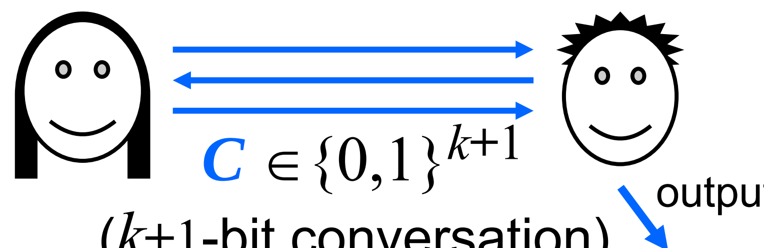
Deterministic cost is *n* bits (I)

Table of all values of $f(x,y)$:

	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	1	0
111	0	0	0	0	0	0	0	1

Suppose the communication complexity of f is k

Each input in the domain of f fixes a ***conversation***



(k+1-bit conversation)

Several inputs may lead to the same conversation ...

A ***rectangle*** is $R \subseteq \{0,1\}^n \times \{0,1\}^n$ of the form $R = R_A \times R_B$

Deterministic cost is *n* bits (II)

Table of all values of $f(x,y)$:

	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	1	0
111	0	0	0	0	0	0	0	1

In fact, the inputs leading to C ***must*** constitute a rectangle: if (x,y), (x',y') both lead to C then so do (x',y) and (x,y')

Since each conversation has a unique output, f is ***constant*** on each of these rectangles

Need at least 2^{n+1} rectangles to $\{0,1\}$-partition this table

Since this implies $\geq 2^{n+1}$ distinct conversations, $k \geq n$

Therefore, the deterministic communication complexity is n

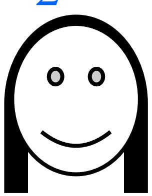
Probabilistic cost is $O(\log n)$ bits

Start with a "good" classical error-correcting code, which is a function $e:\{0,1\}^n \rightarrow \{0,1\}^{cn}$ such that, for all $x \neq y$,

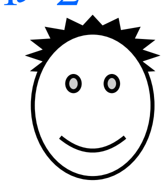
$\Delta(e(x), e(y)) \geq \delta cn$ (Δ means Hamming distance),

where c, δ are constants

$x_1 x_2 \ldots x_n$



$y_1 y_2 \ldots y_n$



randomly choose

$r \in \{1, 2, \ldots, cn\}$

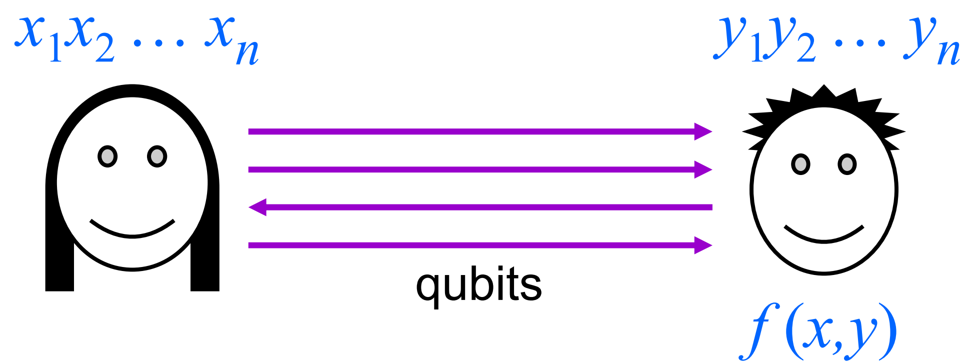
$(r, e(x)_r)$ →

output $\begin{cases} 1 \text{ if } e(y)_r = e(x)_r \\ 0 \text{ if } e(y)_r \neq e(x)_r \end{cases}$

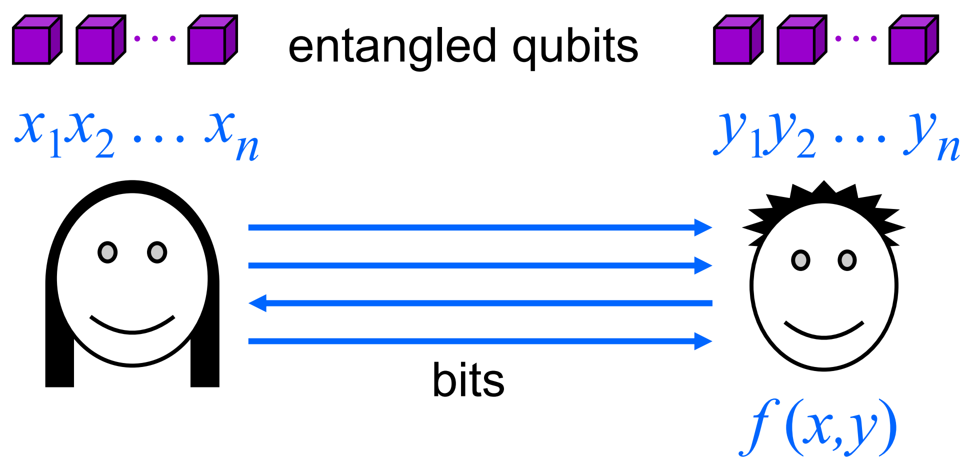
Can repeat to reduce error

Quantum communication complexity

Qubit communication



Prior entanglement



Question: can quantum beat classical in this context?

- Communication complexity
  - Equality checking
  - Intersection (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
  - Simultaneous message passing & fingerprinting

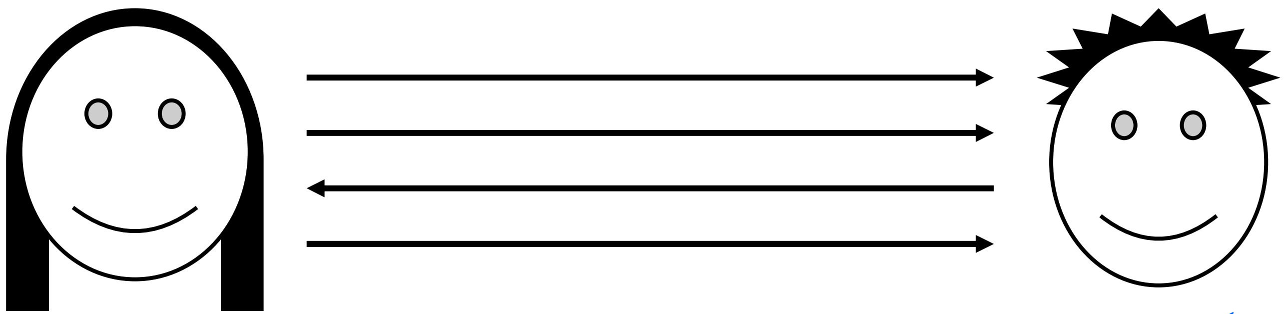
Appointment scheduling

1 2 3 4 5 . . . n

$x =$ 0 1 1 0 1 … 0

1 2 3 4 5 . . . n

$y =$ 1 0 0 1 1 … 1



$i \ \ (x_i = y_i = 1)$

Classically, $\Omega(n)$ **bits** necessary to succeed with prob. ≥ 3/4

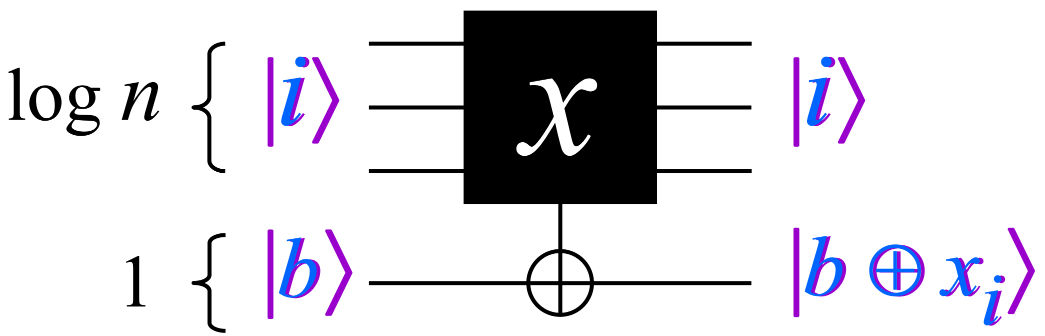
For all $\varepsilon > 0$, $O(n^{1/2} \log n)$ **qubits** sufficient for error prob. < ε

[KS ‘87] [BCW ‘98]

Search problem

1	2	3	4	5	6	...	n
0	0	0	0	1	0	...	1

Given: $x = $ 0 0 0 0 1 0 ... 1 accessible via ***queries***



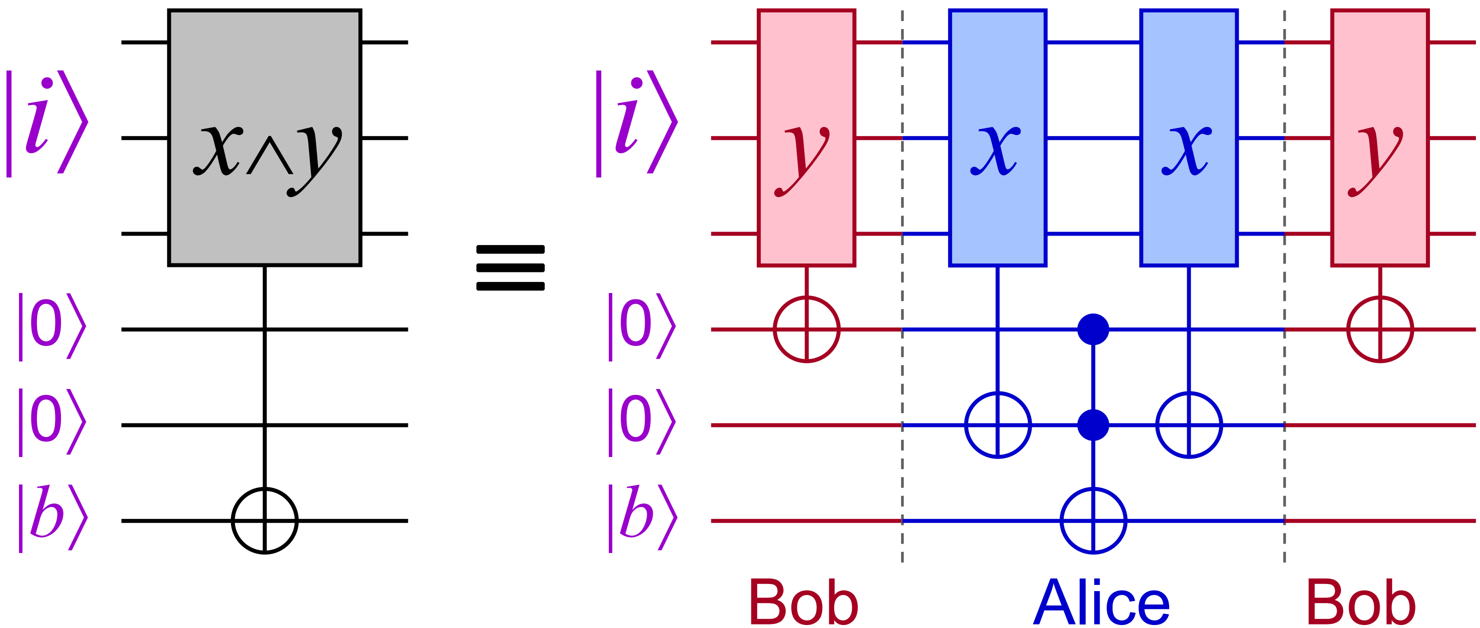
Goal: find $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$

Classically: $\Omega(n)$ queries are necessary

Quantum mechanically: $O(n^{1/2})$ queries are sufficient

[Grover, 1996]

		1	2	3	4	5	6	...	n
Alice	$x =$	0	1	1	0	1	0	...	0
Bob	$y =$	1	0	0	1	1	0	...	1
	$x \wedge y =$	0	0	0	0	1	0	...	0



Communication per $x \wedge y$-query: $2(\log n + 3) = O(\log n)$

Appointment scheduling: epilogue

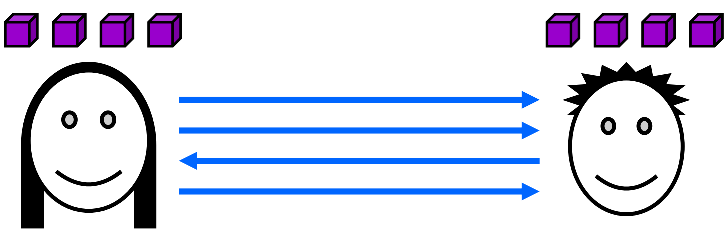
Bit communication:

Cost: $\theta(n)$

Qubit communication:

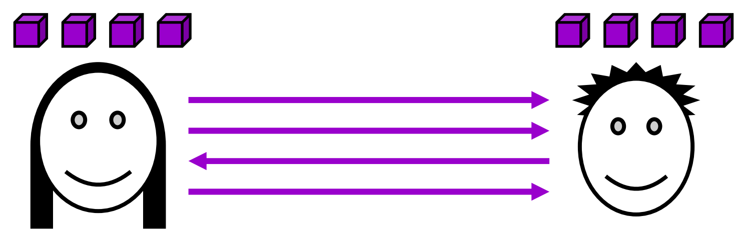
Cost: $\theta(n^{1/2})$ (with refinements)

Bit communication & prior entanglement:



Cost: $\theta(n^{1/2})$

Qubit communication & prior entanglement:



Cost: $\theta(n^{1/2})$

[R '02] [AA '03]

- Communication complexity
  - Equality checking
  - Intersection (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
  - Simultaneous message passing & fingerprinting

Restricted version of equality

Precondition (i.e. promise)**:** either $x = y$ or $\Delta(x,y) = n/2$

Hamming distance

(Distributed variant of “constant” vs. “balanced”)

Classically, $\Omega(n)$ bits communication are necessary ***for an exact solution***

Quantum mechanically, $O(\log n)$ qubits communication are sufficient ***for an exact solution***

[BCW ’98]

Classical lower bound

Theorem: If $S \subseteq \{0,1\}^n$ has the property that, for all $x, x' \in S$, their ***intersection*** size is ***not*** $n/4$ then $|S| < 1.99^n$

Let ***some*** protocol solve restricted equality with k bits comm.

- 2^k conversations of length k
- restrict to the $2^n/\sqrt{n}$ input pairs (x, x), where $\Delta(x) = n/2$

There are $2^n/2^k\sqrt{n}$ input pairs (x, x) that yield ***same*** conv. C

Define $S = \{x : \Delta(x) = n/2$ and (x, x) yields conv. $C\}$

For any $x, x' \in S$, input pair (x, x') ***also*** yields conversation C

Therefore, $\Delta(x, x') \neq n/2$, implying intersection size is ***not*** $n/4$

Theorem implies $2^n/2^k\sqrt{n} < 1.99^n$, so $k > 0.007n$

[Frankl and Rödl, 1987]

Quantum protocol

For each $x \in \{0,1\}^n$, define $|\psi_x\rangle = \sum_{j=1}^{n} (-1)^{x_j} |j\rangle$

Protocol:

1. Alice sends $|\psi_x\rangle$ to Bob ($\log n$ qubits)
2. Bob measures state in a basis that includes $|\psi_y\rangle$

Correctness of protocol:

If $x = y$ then Bob's result is definitely $|\psi_y\rangle$

If $\Delta(x,y) = n/2$ then $\langle\psi_x|\psi_y\rangle = 0$, so result is definitely ***not*** $|\psi_y\rangle$

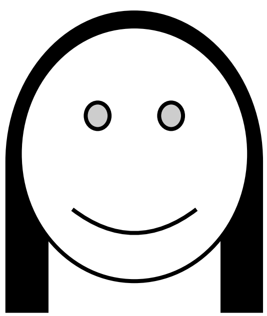
Question: How much communication if error ¼ is permitted?

Answer: Just 2 bits are sufficient!

Exponential quantum vs. classical separation in <u>bounded-error models</u>

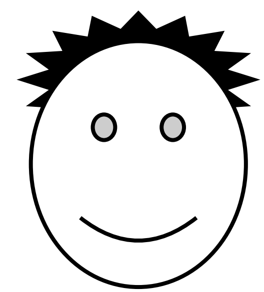
$O(\log n)$ quantum vs. $\Omega(n^{1/4} / \log n)$ classical communication

Classical description of
$|\psi\rangle$: a $\log(n)$-qubit state
$\boldsymbol{M}$: two-outcome measurement



Output: binary result
of applying $\boldsymbol{M}$ to $\boldsymbol{U}|\psi\rangle$

Classical description of
$\boldsymbol{U}$: $\log(n)$-qubit unitary op



[Raz, '99]

- Communication complexity
  - Equality checking
  - Intersection (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
  - Simultaneous message passing & fingerprinting

Inner product

$$\mathrm{IP}(x,y) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \bmod 2$$

Classically, $\Omega(n)$ bits of communication are required, even for bounded-error protocols

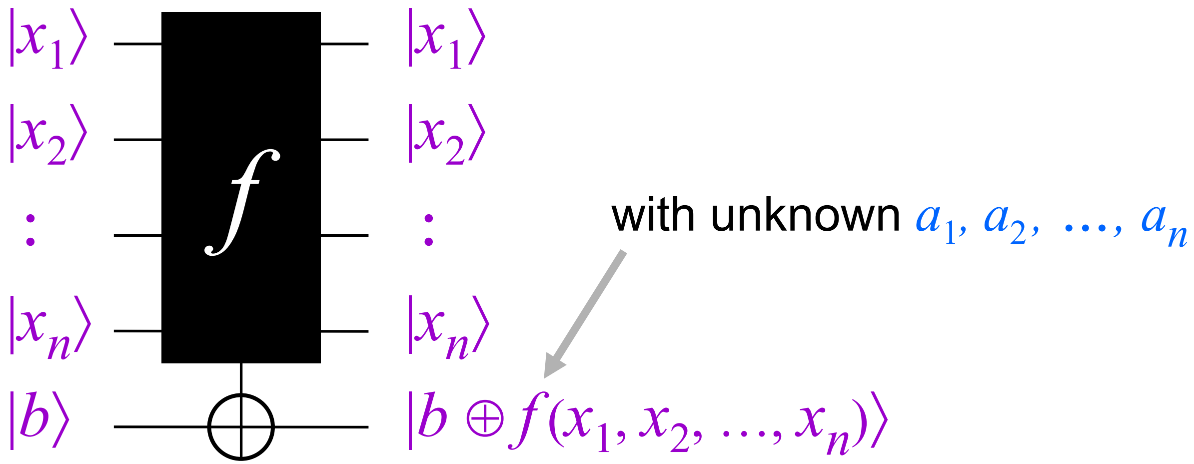
Quantum protocols ***also*** require $\Omega(n)$ communication

[KY ’95] [CNDT ’98] [NS ’02]

The Bernstein-Vazirani problem

Let $f(x_1, x_2, \ldots, x_n) = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \bmod 2$

Given:



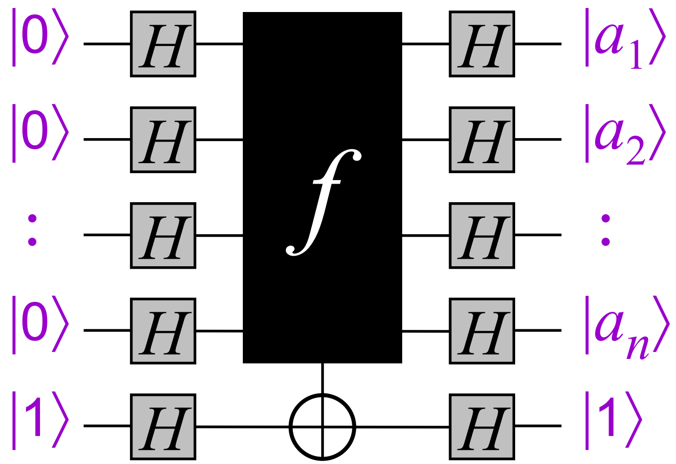
Goal: determine $a_1, a_2, \ldots, a_n$

Classically, n queries are necessary

The Bernstein-Vazirani problem

Let $f(x_1, x_2, \ldots, x_n) = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \bmod 2$

Given:



Goal: determine $a_1, a_2, \ldots, a_n$

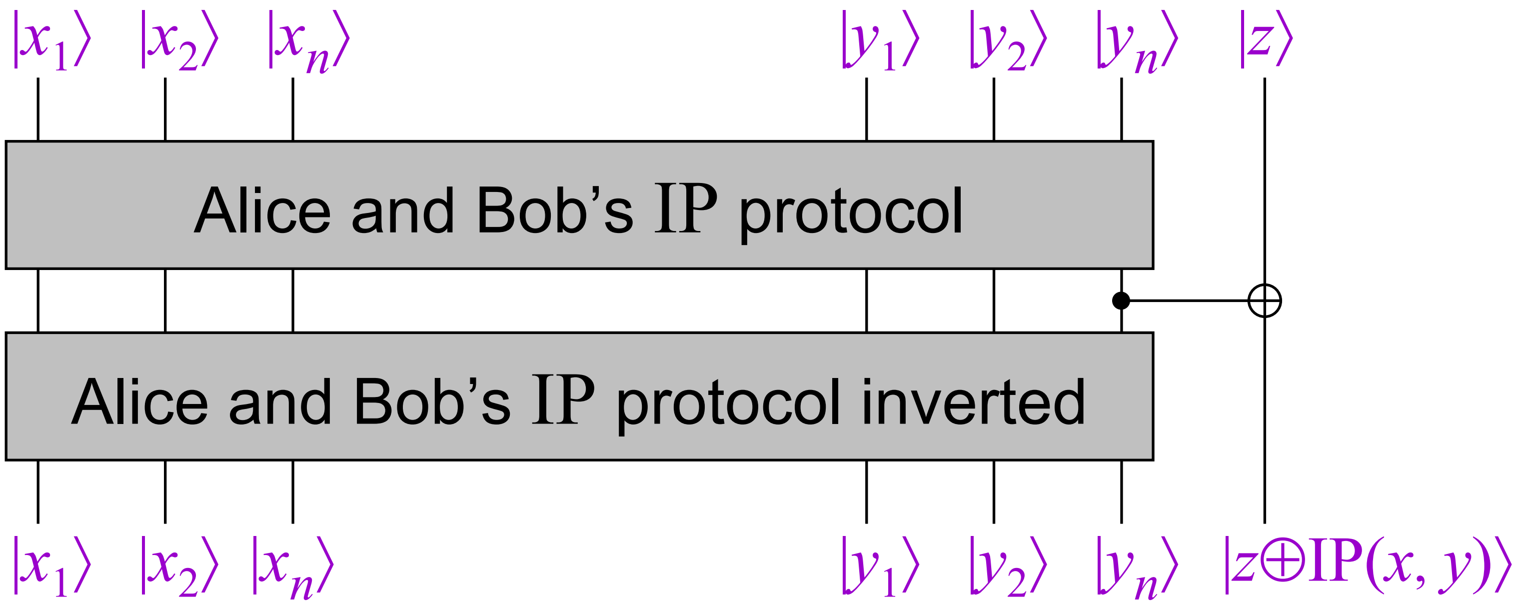
Classically, n queries are necessary

Quantum mechanically, 1 query is sufficient

Lower bound for inner product

$$\mathrm{IP}(x, y) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \bmod 2$$

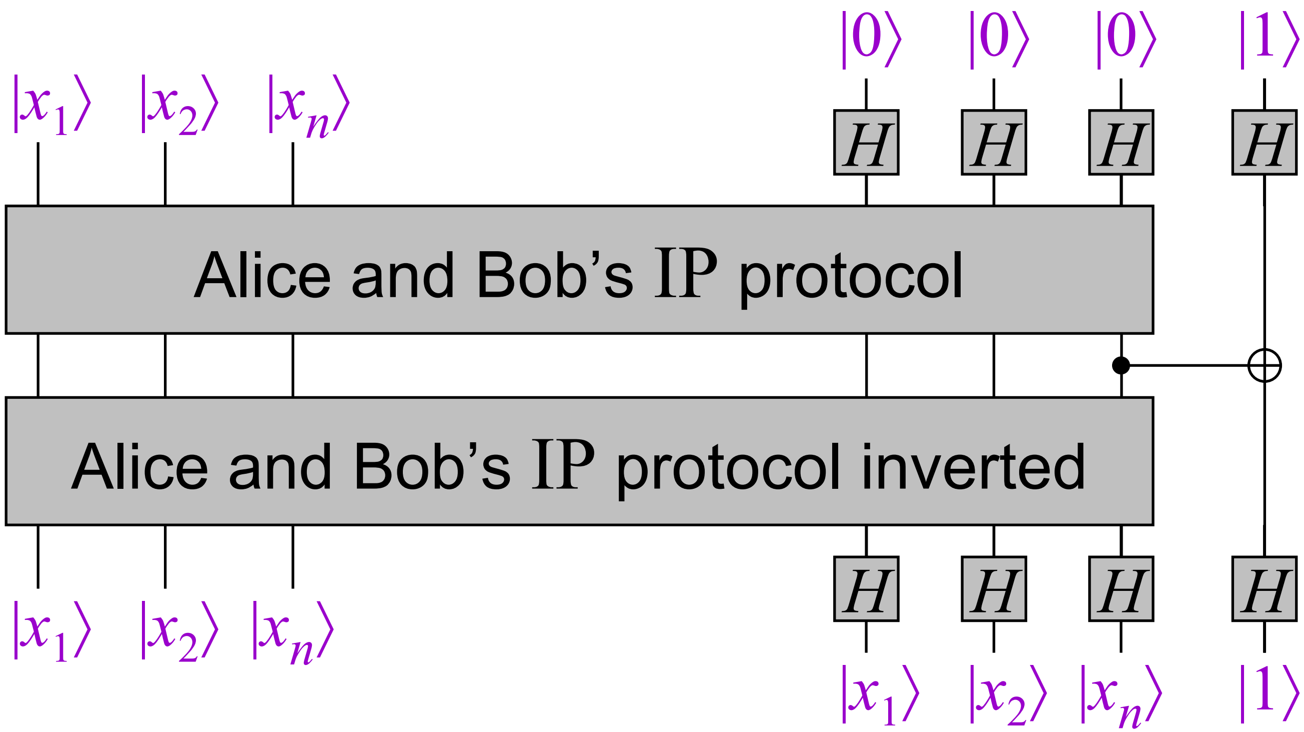
Proof:



Lower bound for inner product

$$\mathrm{IP}(x, y) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \bmod 2$$

Proof:



Since n bits are conveyed from Alice to Bob, n qubits communication necessary (by Holevo's Theorem)

THE END

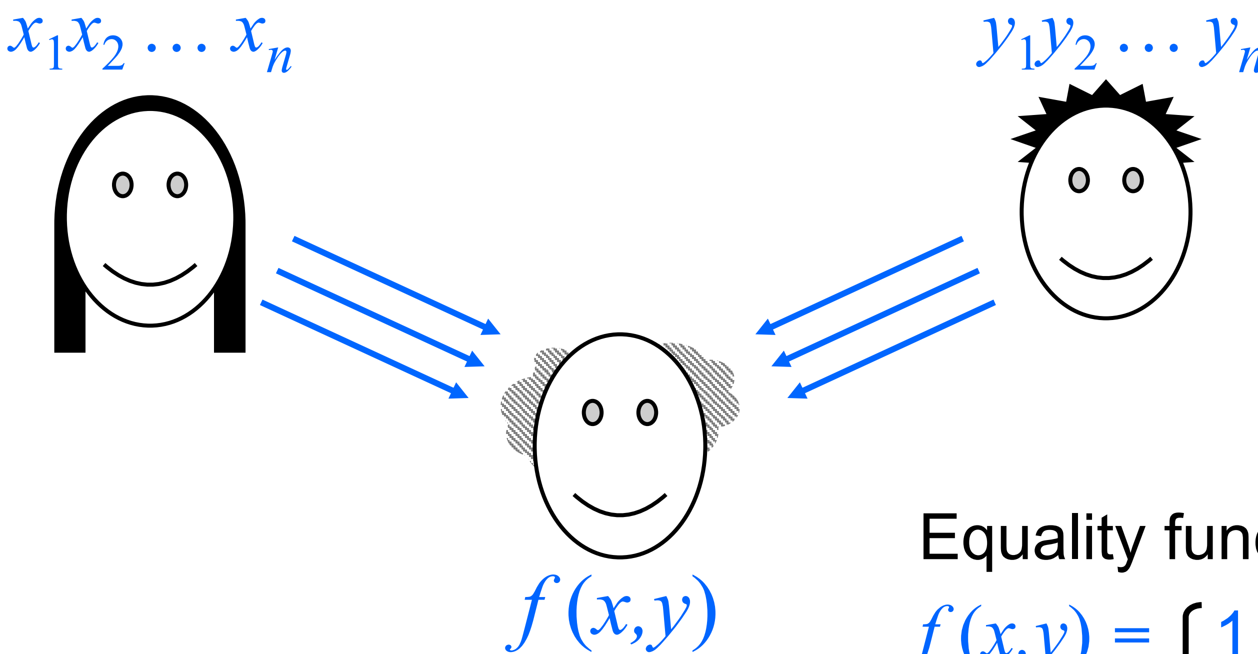
Contents of Lecture 3

- Quantum fingerprinting
- Hidden matching problem

- Quantum fingerprinting
- Hidden matching problem

Equality revisited

in simultaneous message model

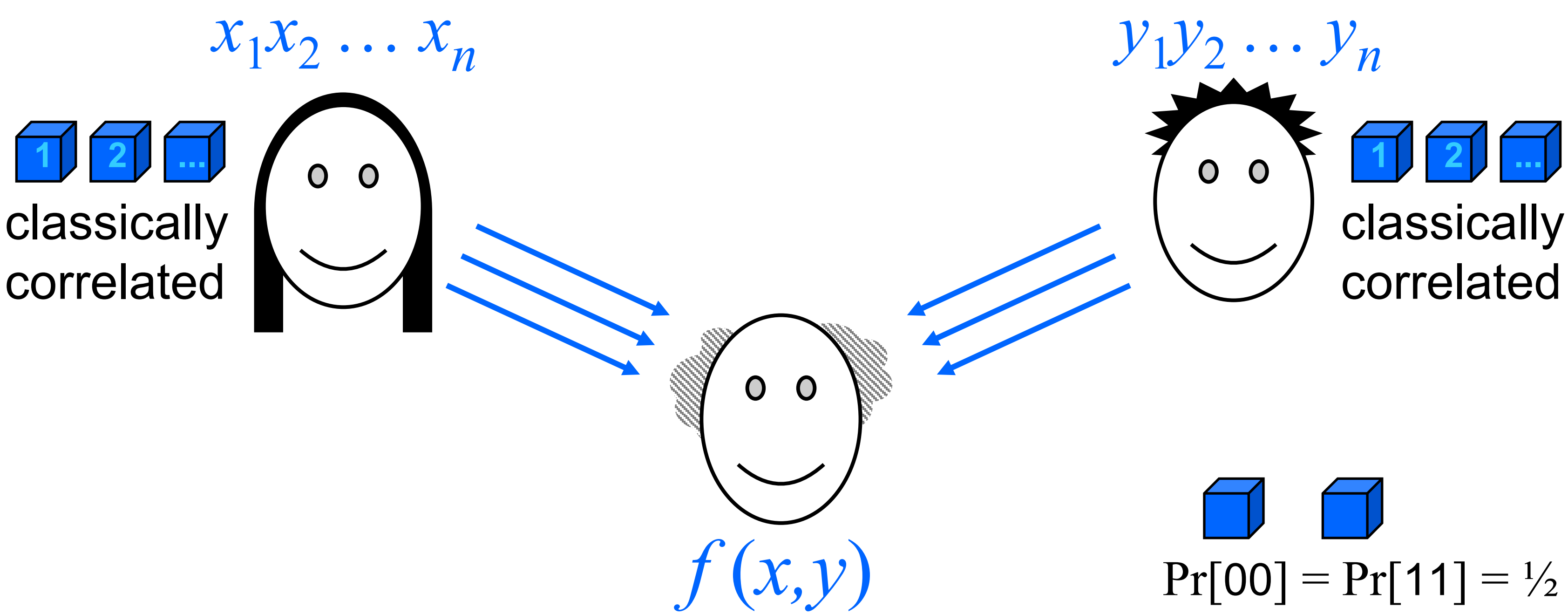


Equality function:

$$f(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

Exact protocols: require $2n$ bits communication

Equality revisited
in simultaneous message model



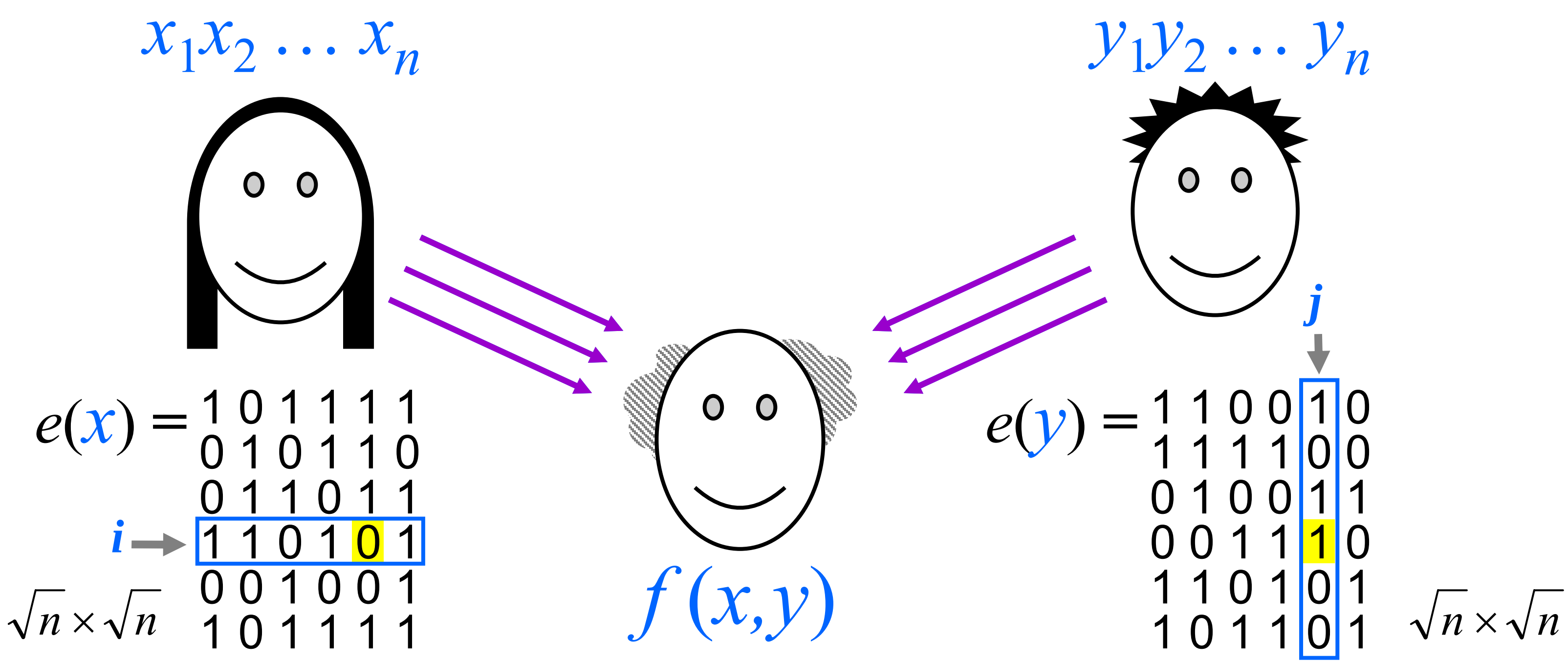
Bounded-error protocols with a shared random key: require only $O(1)$ bits communication

Error-correcting code: $e(x) =$ 1 0 1 1 1 1 0 1 0 1 1 0 0 1 1 0 0 1

$e(y) =$ 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0 1 0

random $\boldsymbol{k}$

Equality revisited
in simultaneous message model



Bounded-error protocols ***without*** a shared key:

Classical: $\theta(n^{1/2})$

Quantum: $\theta(\log n)$ using quantum fingerprints

[A '96] [NS '96] [BCWW '01]

Quantum fingerprints

Question 1: how many orthogonal states in m qubits?

Answer: 2^m

Let ε be an arbitrarily small positive constant

Question 2: how many ***almost orthogonal**** states in m qubits?

(* where $|\langle\psi_x|\psi_y\rangle| \leq \varepsilon$)

Answer: $2^{2^{am}}$, for some constant $0 < a < 1$

Construction of *almost* orthogonal states: start with a special classical error-correcting code, which is a function $e:\{0,1\}^n \rightarrow \{0,1\}^{cn}$ such that, for all $x \neq y$,

$$\delta cn \leq \Delta(e(x), e(y)) \leq (1-\delta)cn$$

(c, δ are constants)

Construction of *almost* orthogonal states

Set $|\psi_x\rangle = \frac{1}{\sqrt{cn}} \sum_{k=1}^{cn} (-1)^{e(x)_k} |k\rangle$ for each $x \in \{0,1\}^n$ ($\log(cn)$ qubits)

Then $\langle\psi_x|\psi_y\rangle = \frac{1}{cn} \sum_{k=1}^{cn} (-1)^{[e(x)\oplus e(y)]_k} |k\rangle = 1 - \frac{2\Delta(e(x),e(y))}{cn}$

Since $\delta cn \le \Delta(e(x),e(y)) \le (1-\delta)cn$, we have $|\langle\psi_x|\psi_y\rangle| \le 1-2\delta$

By duplicating each state, $|\psi_x\rangle\otimes|\psi_x\rangle\otimes \ldots \otimes|\psi_x\rangle$, the pairwise inner products can be made arbitrarily small: $(1-2\delta)^r \le \varepsilon$

Result: $m = r\log(cn)$ qubits storing $2^n = 2^{(1/c)2^{m/r}}$ different states

(as opposed to n qubits!)

What are these almost orthogonal states good for?

Question 3: can they be used to somehow store n bits using only $O(\log n)$ qubits?

Answer: *No*—recall that Holevo's theorem forbids this

Here's what we *can* do: given two states from an almost orthogonal set, we can distinguish between these two cases:

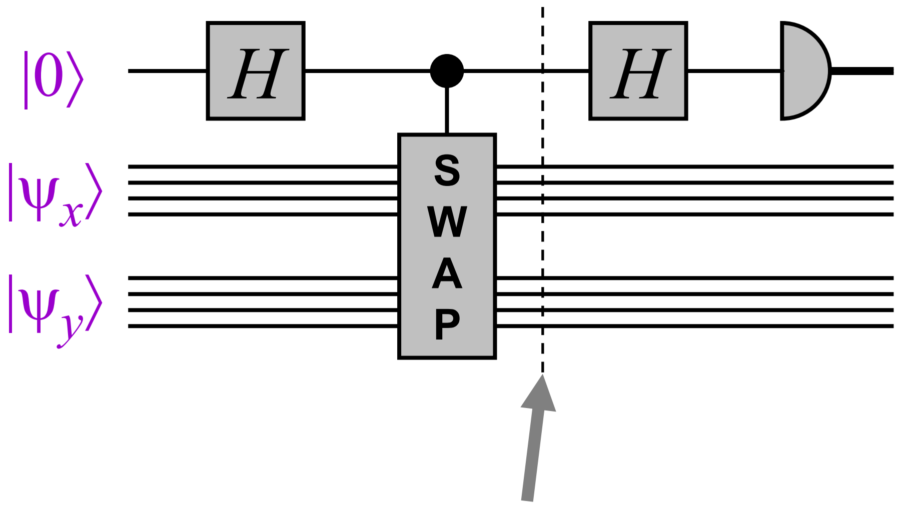
- they're both the same state
- they're almost orthogonal

Question 4: How?

Quantum fingerprints

Let $|\psi_{000}\rangle, |\psi_{001}\rangle, \ldots, |\psi_{111}\rangle$ be 2^n states on $O(\log n)$ qubits such that $|\langle\psi_x|\psi_y\rangle| \leq \varepsilon$ for all $x \neq y$

Given $|\psi_x\rangle|\psi_y\rangle$, one can check if $x = y$ or $x \neq y$ as follows:



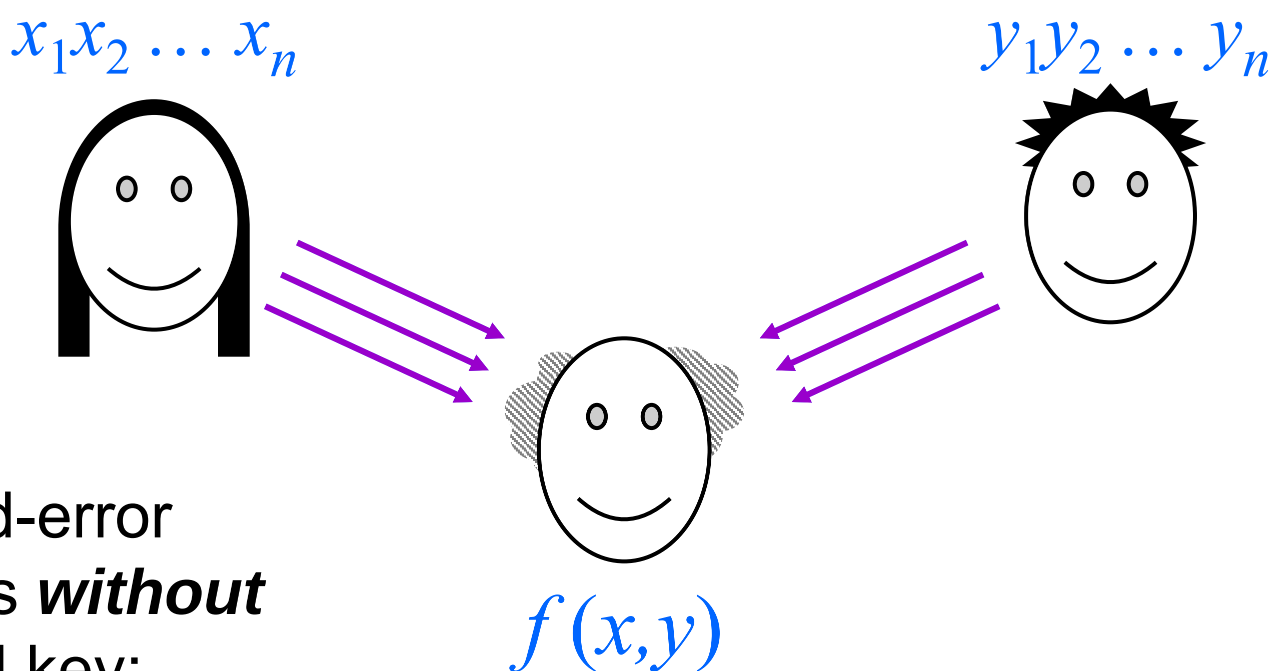
if $x = y$, $\Pr[\text{output} = 0] = 1$

if $x \neq y$, $\Pr[\text{output} = 0] = (1+ \varepsilon^2)/2$

Intuition: $|0\rangle|\psi_x\rangle|\psi_y\rangle + |1\rangle|\psi_y\rangle|\psi_x\rangle$

Note: error probability can be reduced to $((1+ \varepsilon^2)/2)^r$

Equality revisited
in simultaneous message model



Bounded-error
protocols ***without***
a shared key:

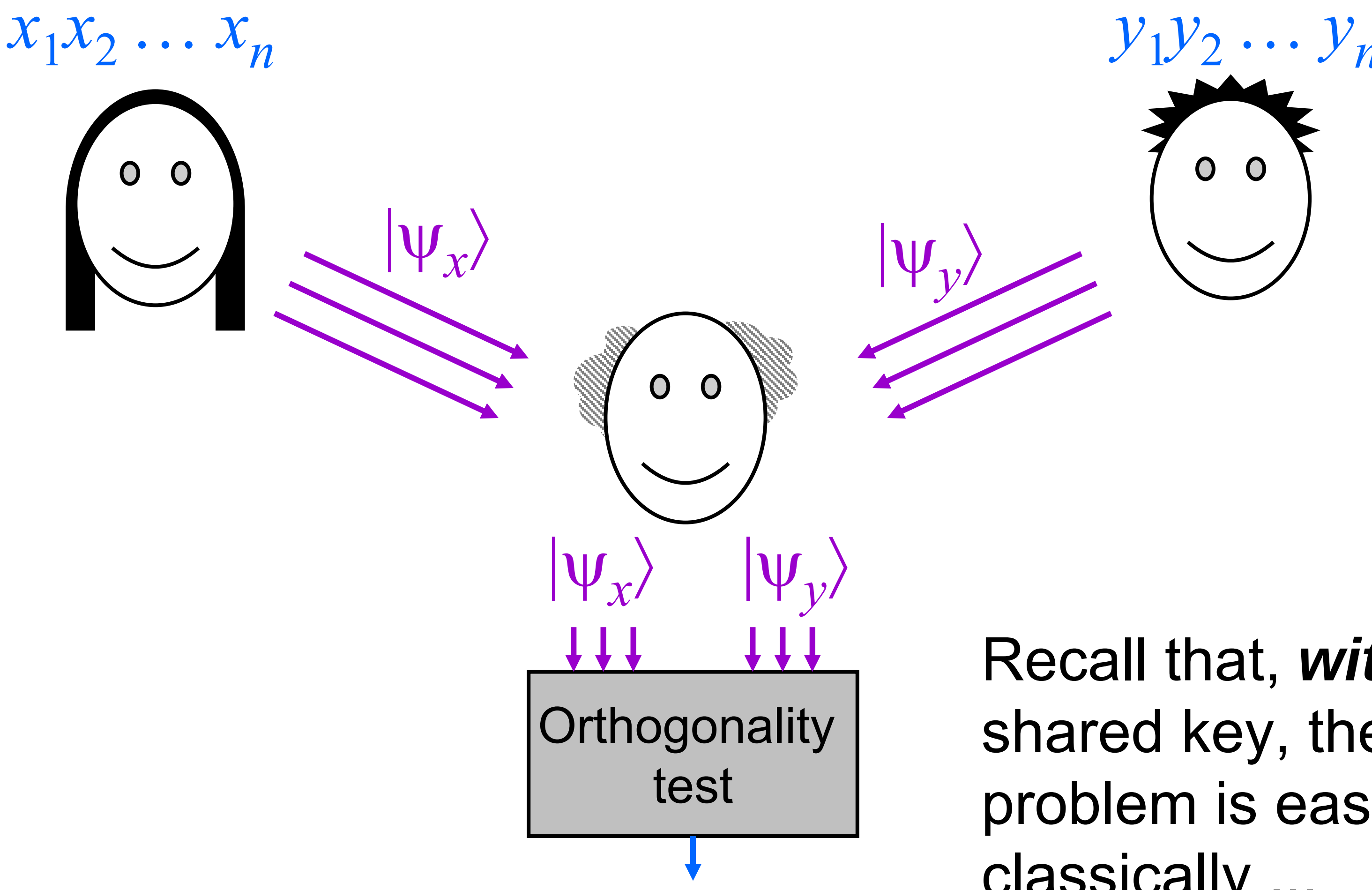
Classical: $\theta(n^{1/2})$

Quantum: $\theta(\log n)$

[A '96] [NS '96] [BCWW '01]

Quantum protocol for equality

in simultaneous message model



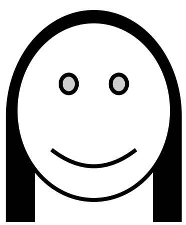
Recall that, ***with*** a shared key, the problem is easy classically ...

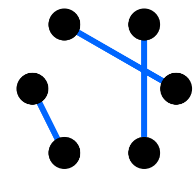
- Quantum fingerprinting
- Hidden matching problem

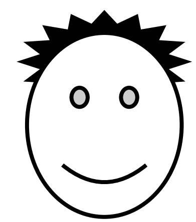
Hidden matching problem

For this problem, a quantum protocol is exponentially more efficient than any classical protocol—even with a shared key

Inputs: $x \in \{0,1\}^n$



$M =$  ***matching*** on $\{1, 2, \ldots, n\}$



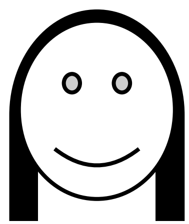
Output: $(i, j, x_i \oplus x_j)$, such that $(i, j) \in M$

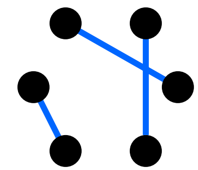
Only ***one-way*** communication (Alice to Bob) is permitted

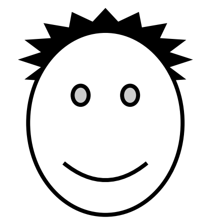
[Bar-Yossef, Jayram, Kerenidis, '04]

The hidden matching problem

Inputs: $x \in \{0,1\}^n$



$M =$  ***matching*** on $\{1,2, \ldots, n\}$



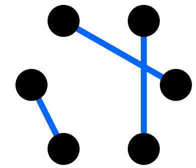
Output: $(i, j, x_i \oplus x_j)$, $(i, j) \in M$

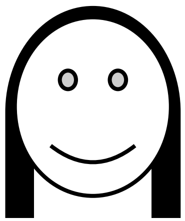
Classically, one-way communication is $\Omega(\sqrt{n})$, even with a shared classical key (the proof is omitted here)

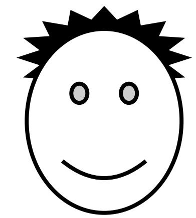
Rough intuition: Alice doesn't know which edges are in M, so she apparently has to send $\Omega(\sqrt{n})$ bits of the form $x_i \oplus x_j$ …

The hidden matching problem

Inputs: $x \in \{0,1\}^n$

$M =$  ***matching*** on $\{1,2, \ldots, n\}$





Output: $(i, j, x_i \oplus x_j)$, $(i, j) \in M$

Quantum protocol: Alice sends $\frac{1}{\sqrt{n}}\sum_{k=1}^{n}(-1)^{x_k}|k\rangle$ ($\log n$ qubits)

Bob measures in $|i\rangle \pm |j\rangle$ basis, $(i, j) \in M$, and uses the outcome's relative phase to determine $x_i \oplus x_j$

THE END

Contents of Lecture 4

- Interactive proof systems
- Two-prover interactive proof systems (**MIP**s)
  - Classical $\oplus$**-MIP** = **MIP** = **NEXP**
  - Quantum $\oplus$**-MIP*** $\subseteq$ **EXP**

joint work with:

Peter Høyer (Calgary)

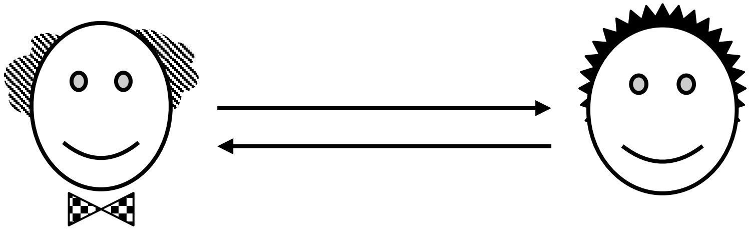
Ben Toner (Caltech)

John Watrous (Calgary)

- Interactive proof systems
- Two-prover interactive proof systems (**MIPs**)
  - Classical $\oplus$-**MIP** = **MIP** = **NEXP**
  - Quantum $\oplus$-**MIP*** $\subseteq$ **EXP**

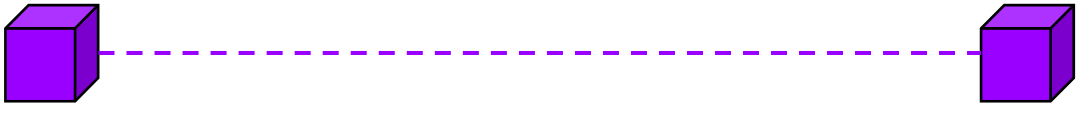
We'll consider connections between:

Computational proof systems: where one or more "provers" can efficiently convince a "verifier" of a mathematical truth



and …

Nonlocality: Bell inequalities and entangled systems that violate them



One conclusion: certain interactive proof systems become *weaker* with quantum information

What is the computational cost of the process of being *convinced* of something?

Consider an instance of **3SAT**:

$$f(x_1,\ldots,x_n) = (x_1 \vee \bar{x}_3 \vee x_4) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge \cdots \wedge (\bar{x}_1 \vee x_5 \vee \bar{x}_n)$$

$f(x_1,\ldots,x_n)$ is ***satisfiable*** iff there exists $b_1,\ldots,b_n \in \{0,1\}$ such that $f(b_1,\ldots,b_n) = 1$

Satisfiability is easy to ***verify***—if one is supplied with, say, a satisfying assignment

NP denotes the class of languages L whose positive instances have such “witnesses” that can be verified in polynomial time

"Complexity Theory 101"

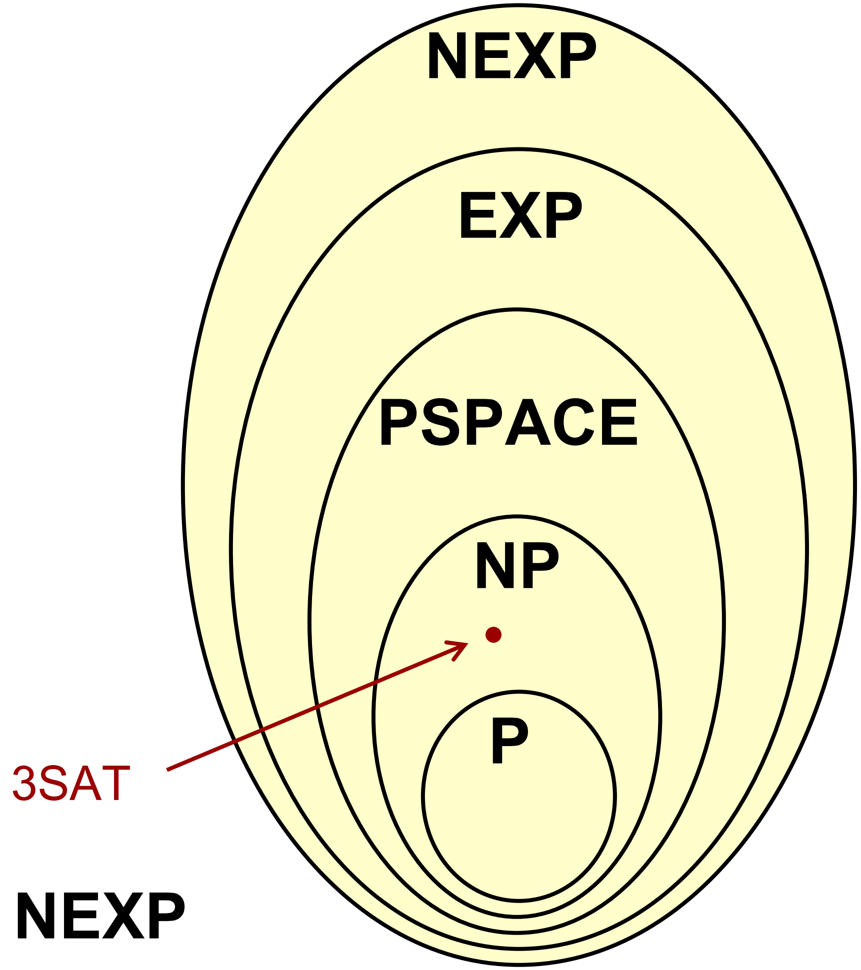
P: solvable in time $O(n^c)$

NP: positive instances verifiable in time $O(n^c)$

PSPACE: solvable with space $O(n^c)$

EXP: solvable in time $O(2^{n^c})$

NEXP: positive instances verifiable in time $O(2^{n^c})$

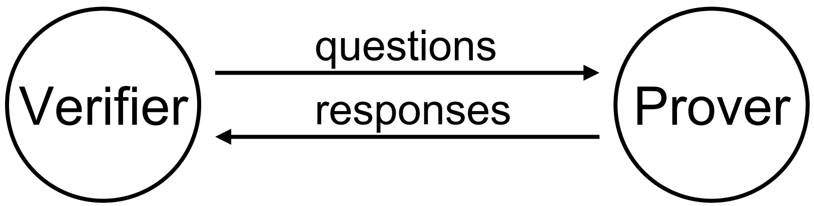


P $\subseteq$ **NP** $\subseteq$ **PSPACE** $\subseteq$ **EXP** $\subseteq$ **NEXP**

Interactive proof systems

If one can carry out a "dialog" with a prover then the expressive power increases from **NP** to **PSPACE**

is $x \in \boldsymbol{L}$?



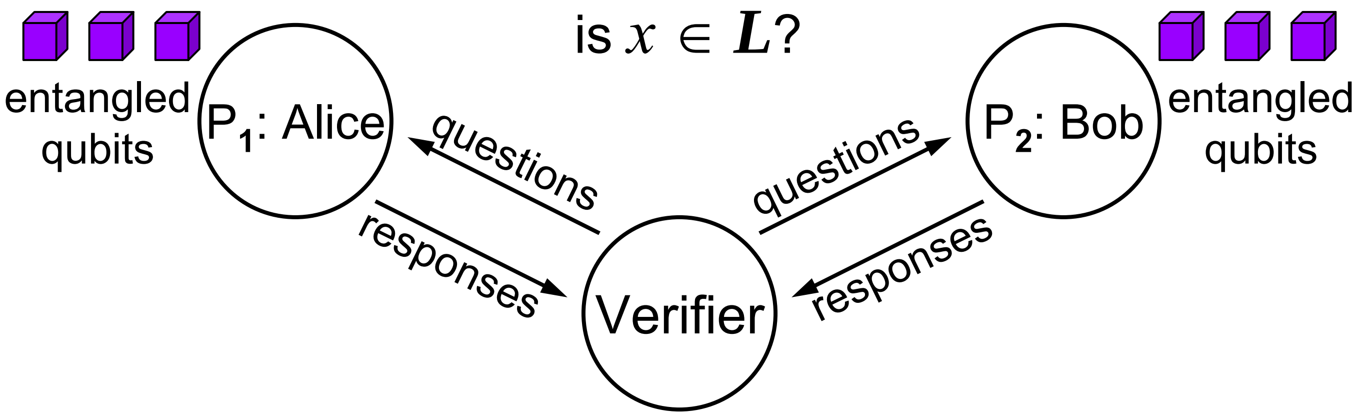
- The Verifier must be efficient (polynomial time), but the Prover is computationally unbounded
- **Soundness:** if $x \notin \boldsymbol{L}$, no Prover causes the Verifier to accept (small error probability is okay)
- **Completeness:** if $x \in \boldsymbol{L}$, there exists a Prover that causes the Verifier to accept (small error is okay)

[Lund, Fortnow, Karloff, Nisan 1990; Shamir 1990]

- Interactive proof systems
- Two-prover interactive proof systems (**MIP**s)
  - Classical $\oplus$-**MIP** = **MIP** = **NEXP**
  - Quantum $\oplus$-**MIP*** $\subseteq$ **EXP**

Two provers

With ***two*** provers, who cannot communicate with each other, the expressive power increases to **NEXP** (nondeterministic exponential-time)



- Again, the Verifier must be efficient (polynomial time), and the Provers are computationally unbounded
- The **NEXP** result assumes the provers are ***classical***
- With ***quantum*** strategies, provers can sometimes "cheat"

[Babai, Fortnow, Lund, 1991]

Sample protocol for 3SAT ...

Instance: $(x_1 \vee \overline{x}_3 \vee x_4) \wedge (\overline{x}_2 \vee x_3 \vee \overline{x}_5) \wedge (\overline{x}_1 \vee x_5 \vee \overline{x}_n)$

1. The Verifier randomly chooses a clause and a variable from that clause, and then sends the clause to Alice and the variable to Bob
2. Alice returns a valid truth assignment for the clause, and Bob must return a consistent value for the variable

E.g., for the above instance, the Verifier might send Alice "$(\overline{x}_2 \vee x_3 \vee \overline{x}_5)$" and send Bob "$x_5$"

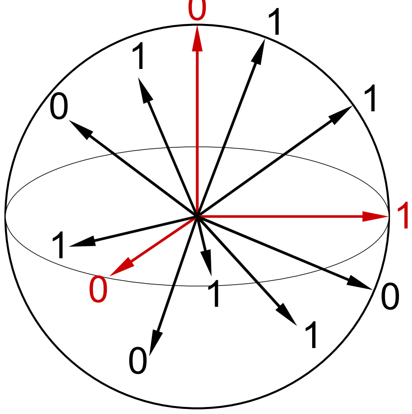
… and a valid response is Alice sends 1, 0, 0 (values for x_2, x_3, x_5 respectively), and Bob sends 0 (value for x_5)

... and how to cheat the protocol

Recall the

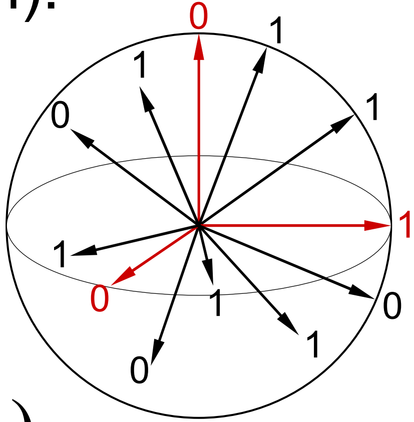
Kochen-Specker Theorem [1967]**:** there exists a finite set of vectors $v_1, v_2, \ldots, v_n$ in $\mathbb{R}^3$ that ***cannot*** be assigned labels from $\{0,1\}$ simultaneously satisfying:

- For any two orthogonal vectors, they are not both labeled 1
- For any three mutually orthogonal vectors, at least one of them is labeled 1



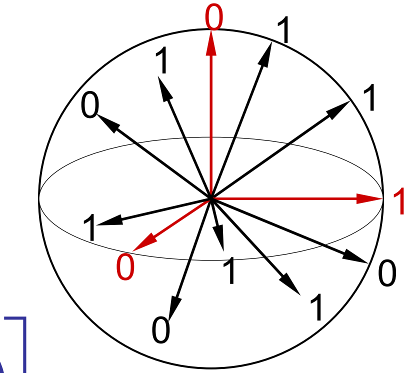
Kochen-Specker "nonlocality"

Game (essentially a Bell-inequality violation):



- The Verifier sends Alice a triple of orthogonal vectors (v_i, v_j, v_k) and Bob one vector v_m from that triple
- Alice returns a valid labeling for (v_i, v_j, v_k), and Bob returns a label for v_m
- The verifier ***accepts*** iff the labels are consistent
- By the Kochen-Specker Theorem, the ***classical*** success probability is less than one
- There is a perfect quantum strategy using entanglement $|\psi\rangle = |00\rangle + |11\rangle + |22\rangle$

Cheating the protocol for 3SAT



For an instance of the Kochen-Specker Theorem, the orthogonality conditions can be expressed by the formula

$$f(x_1,\ldots,x_n) = \left[\bigwedge_{v_i \perp v_j} \left(\overline{x}_i \vee \overline{x}_j \right) \right] \wedge \left[\bigwedge_{v_i \perp v_j \perp v_k} \left(x_i \vee x_j \vee x_k \right) \right]$$

- By the Kochen-Specker Theorem, this formula is unsatisfiable—therefore, for classical Provers, the Verifier accepts with probability ***less than one***
- But, using the quantum strategy for the KS game, the Provers can cause the Verifier to ***always*** accept

MIP

- **Definition: MIP** is the class of languages accepted by ***classical*** two-prover interactive proof systems

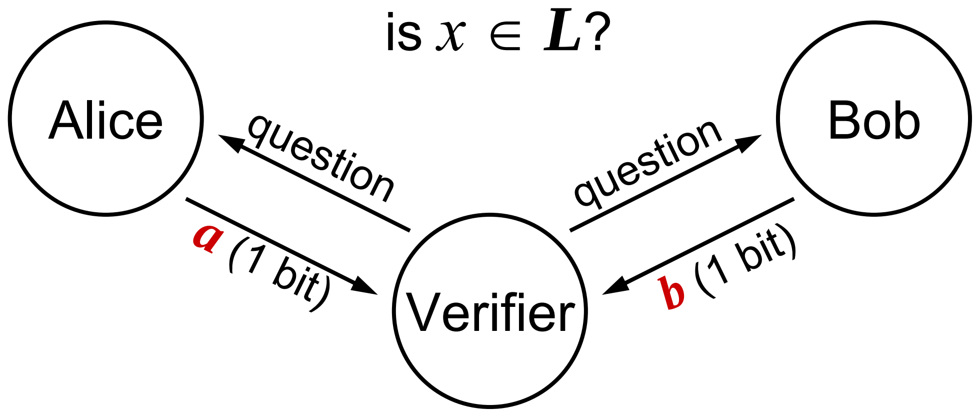
- **Theorem** [Fortnow, Rompel, Sipser, 1988; Babai, F, Lund, 1991]**:**
  MIP = **NEXP**

- **Definition: MIP*** is the class of languages accepted by ***quantum*** two-prover interactive proof systems

- **Open questions:**

  Is **NEXP** $\subseteq$ **MIP***?
  Is **MIP*** $\subseteq$ **NEXP**?

⊕-MIP and ⊕-MIP*



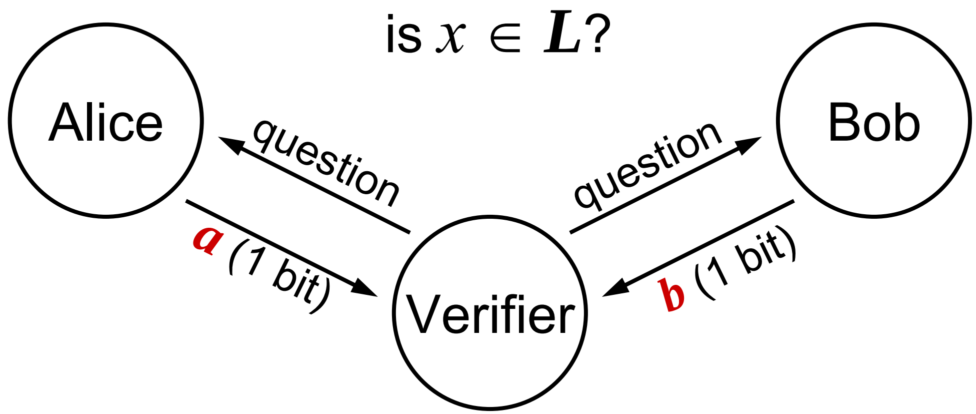
Restricted protocols that are ***one-round*** and where:

- Alice and Bob's responses, a and b, are ***single bits***
- The Verifier's decision is a function of $a \oplus b$ and his questions only
- Any constant gap between the soundness and the completeness success probability is okay

Recall the CHSH version of Bell: $a \oplus b = s \wedge t$

$$a_0 \oplus b_0 = 0$$
$$a_0 \oplus b_1 = 0$$
$$a_1 \oplus b_0 = 0$$
$$a_1 \oplus b_1 = 1$$

⊕-MIP vs ⊕-MIP*



Theorem 1: ⊕-MIP $=$ **NEXP** ($=$ **MIP**)

Theorem 2: ⊕-MIP* $\subseteq$ **EXP**

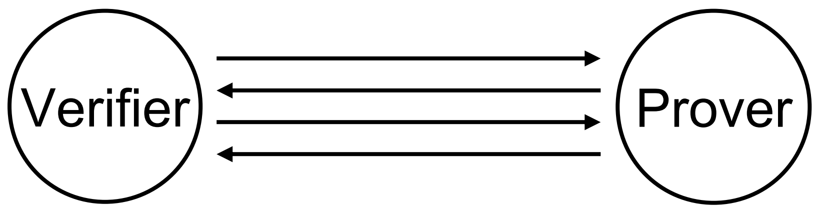
Therefore, ⊕**-MIP*** is strictly weaker than ⊕**-MIP** (unless **EXP** $=$ **NEXP**)

- Interactive proof systems
- Two-prover interactive proof systems (**MIP**s)
  - Classical $\oplus$-**MIP** = **MIP** = **NEXP**
  - Quantum $\oplus$-**MIP*** $\subseteq$ **EXP**

Proof that NEXP $\subseteq$ $\oplus$-MIP (I)

A ***probabilistically checkable proof*** (***PCP***) system is:

A single-prover interactive proof system where the prover is not adaptive (i.e., behaves like an oracle)



Equivalently, each proof is bit-string, and the verifier accesses a bounded number of bits of the string (of his choosing)

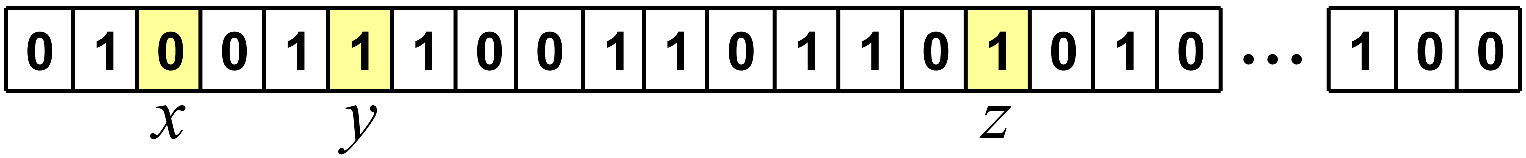
0	1	1	0	1	0	1	0	0	1	1	0	1	0	1	0	0	1	1

Theorem: NP $=$ $\oplus$-**PCP**$_{1/2+\varepsilon,\,1}\,[O(\log n),\, \mathbf{3}]$

[Håstad ’01][Bellare, Goldreich, Sudan ’98]

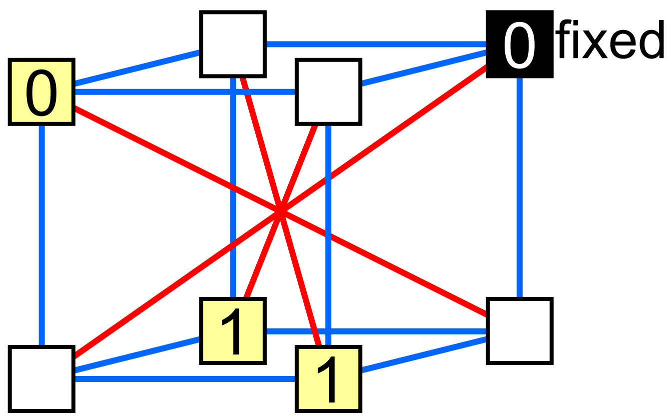
Proof that NEXP ⊆ ⊕-MIP (II)

Corollary: NEXP $= \oplus$**-PCP**$_{1/2+\varepsilon,\,1}[n^{O(1)}, \mathbf{3}]$



Lemma: NEXP $= \oplus$**-PCP**$_{11/16+\varepsilon,\,1}[n^{O(1)}, \mathbf{2}]$

A test for $x \oplus y \oplus z = 0$



If $x \oplus y \oplus z =$ **0** then it is is possible to satisfy 12/16 edges

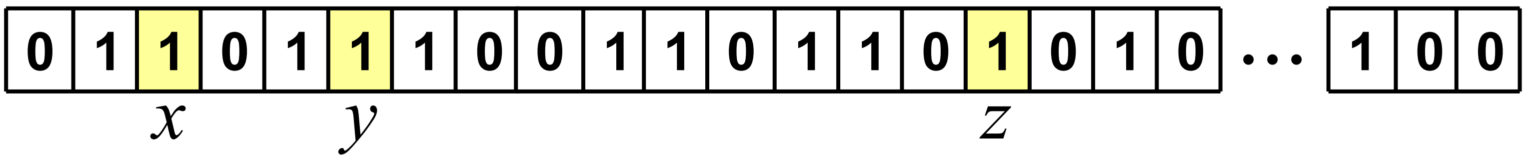
—— $a \oplus b = 1$ (different)

—— $a \oplus b = 0$ (same)

[H '01][BGS '98]

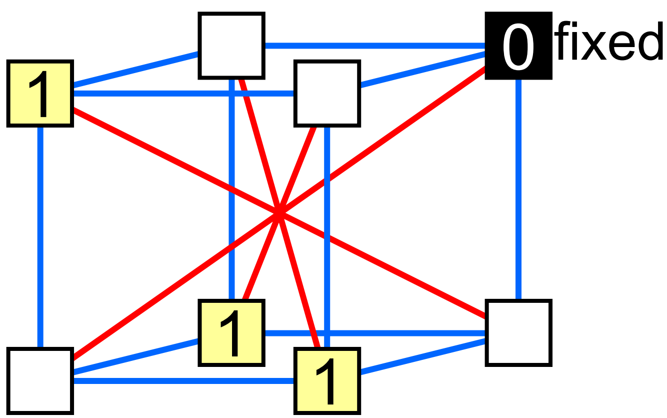
Proof that NEXP ⊆ ⊕-MIP (III)

Corollary: NEXP $= \oplus$**-PCP**$_{1/2+\varepsilon,\,1}\,[n^{O(1)},\, \mathbf{3}]$



Lemma: NEXP $= \oplus$**-PCP**$_{11/16+\varepsilon,\,1}\,[n^{O(1)},\, \mathbf{2}]$

A test for $x \oplus y \oplus z = 0$



If $x \oplus y \oplus z$ = **1** then it is is possible to satisfy at most 10/16 edges

To test $x \oplus y \oplus z = 1$, set fixed bit to 1 (or switch incident edge colors)

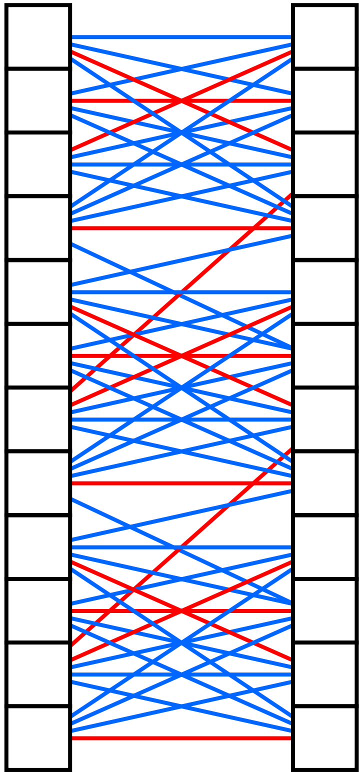
—— $a \oplus b$ = 1 (different)

—— $a \oplus b$ = 0 (same)

Finally, can “unfix” fixed bit

Proof that NEXP $\subseteq$ ⊕-MIP (IV)

In the ⊕-**PCP**$_{1/2+\varepsilon,\,1}[n^{O(1)}, \mathbf{2}]$ construction, the underlying graph is ***bipartite***, so each bit can be queried to a separate prover

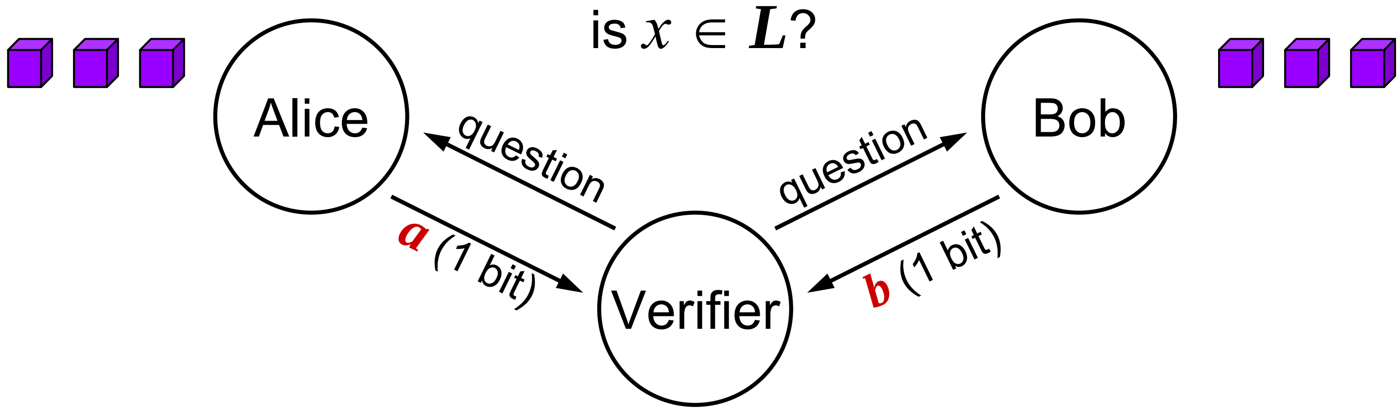


What follows is a ⊕-**MIP**$_{\mathbf{0.6875\,+\varepsilon,\ 0.75}}$ proof system for **NEXP**

Therefore **NEXP** $\subseteq$ ⊕-**MIP**

- Interactive proof systems
- Two-prover interactive proof systems (**MIP**s)
  - Classical $\oplus$-**MIP** = **MIP** = **NEXP**
  - Quantum $\oplus$-**MIP*** $\subseteq$ **EXP**

⊕-MIP* ⊆ EXP

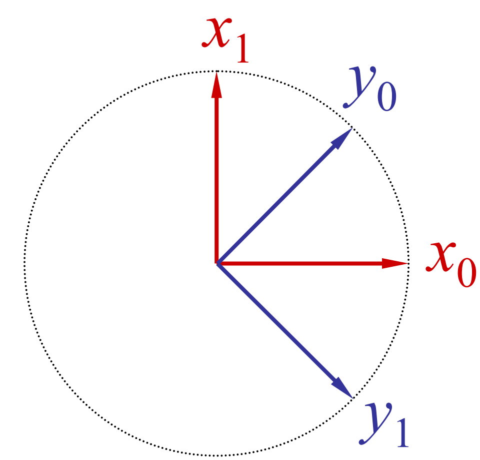


⊕-MIP* ⊆ EXP (I)

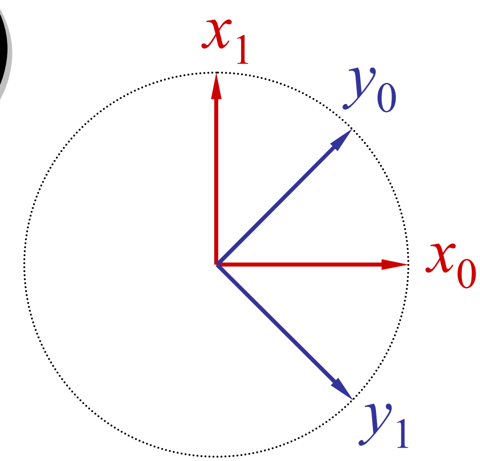
Theorem [Tsirelson, 1987]**:** every ***quantum*** ⊕-type protocol corresponds to sets of unit vectors $\{x_s : s \in S\}$ & $\{y_t : t \in T\}$ in $\mathbb{R}^n$ such that, for questions $(s,t) \in S \times T$, the responses satisfy

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

Example: vectors in $\mathbb{R}^2$ for the CHSH game:



⊕-MIP* ⊆ EXP (II)



Example: vectors in $\mathbb{R}^2$ for the CHSH game:

Overall success probability:

$$\frac{1}{4}\left(\frac{1+x_0\cdot y_0}{2}\right)+\frac{1}{4}\left(\frac{1+x_0\cdot y_1}{2}\right)+\frac{1}{4}\left(\frac{1+x_1\cdot y_0}{2}\right)+\frac{1}{4}\left(\frac{1-x_1\cdot y_1}{2}\right)$$

Tsirelson's Theorem implies that finding the best quantum ⊕-type protocol reduces to finding a set of vectors optimizing an expression of the form $\sum_{st} p_{st}\, x_s \cdot y_t$

Efficient algorithms (polynomial-time in $|S|$ and $|T|$) are known for this kind of problem, using semidefinite programming

Proof of Tsirelson's Theorem (I)

Converting a protocol into a vector system:

Start with a quantum ⊕-type protocol using entanglement $|\psi\rangle$

This can be described in terms of a set of binary observables (Hermitian operators with eigenvalues in $\{+1,-1\}$)
$\{A_s : s \in S\}$ and $\{B_t : t \in T\}$, which correspond to Alice and Bob's respective actions on input $(s,t) \in S{\times}T$

The expected outcome is:

$$\langle\psi|A_s{\otimes}B_t|\psi\rangle = (\langle\psi|A_s{\otimes}I\,)\,(I{\otimes}B_t|\psi\rangle)$$

which is an inner product of two (complex) vectors

These vectors can be embedded into $\mathbb{R}^d$

Proof of Tsirelson's Theorem (II)

Converting a vector system into a protocol:

For any k, there exists a set of k binary observables $M_1, M_2, \ldots, M_k$ such that, for all $i \neq j$, $M_i M_j = -M_j M_i$

They act on a d-dimensional space (where $d = 2^{(k-1)/2}$)

Convert each vector $v = (v_1, v_2, \ldots, v_k)$ into the observable
$M^v = v_1 M_1 + v_2 M_2 + \ldots + v_k M_k$

Then $(1/d)\mathrm{Tr}\left(M^v M^w\right) = v \cdot w$

It follows from this that, setting $|\psi\rangle = |1\rangle|1\rangle + |2\rangle|2\rangle + \ldots + |d\rangle|d\rangle$ yields the desired protocol

Open questions

- **MIP*** versus **MIP**?
- What happens with more than two provers?
- *Quantum* communication between the provers and a quantum verifier?
- There are interesting “spinoffs” from classical **MIP** (e.g. a theory of hardness of approximation problems)—what about for **MIP***?
- How does “parallel repetition” work for quantum strategies?

THE END

Contents of Lecture 5

- $\oplus$-**MIP*** vs one-prover systems
- Nonlocal games (CHSH, KS)
- Quantum versus classical XOR games
- Odd Cycle game (blackboard)
- Magic Square game (blackboard)

joint work with:

Peter Høyer (Calgary)

Ben Toner (Caltech)

John Watrous (Calgary)

- $\oplus$-**MIP*** vs one-prover systems
- Nonlocal games (CHSH, KS)
- Quantum versus classical XOR games
- Odd Cycle game (blackboard)
- Magic Square game (blackboard)

⊕-MIP* vs one-prover systems

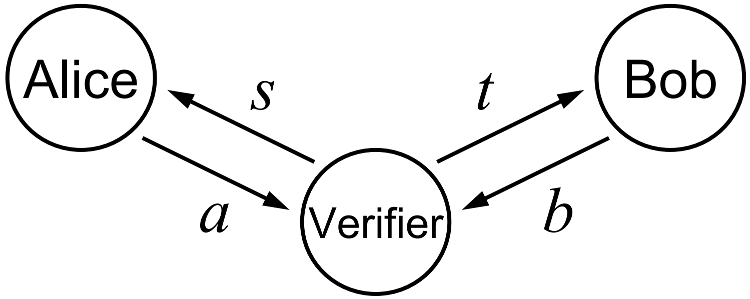
QIP(2) is all langauges accepted by ***single-prover*** interactive proof systems with ***one round of quantum communication*** between prover and verifier (who must now be quantum)

Theorem [Wehner ’05]**:** for $0 \leq s < c \leq 1$, **⊕-MIP*** $_{s,c} \subseteq$ **QIP** $_{s,c}$(2)

Theorem [Kitaev, Watrous ’00]**: QIP** $_{s,c}$(2) $\subseteq$ **EXP**

- ⊕-**MIP*** vs one-prover systems
- Nonlocal games (CHSH, KS)
- Quantum versus classical XOR games
- Odd Cycle game (blackboard)
- Magic Square game (blackboard)

Nonlocality game framework

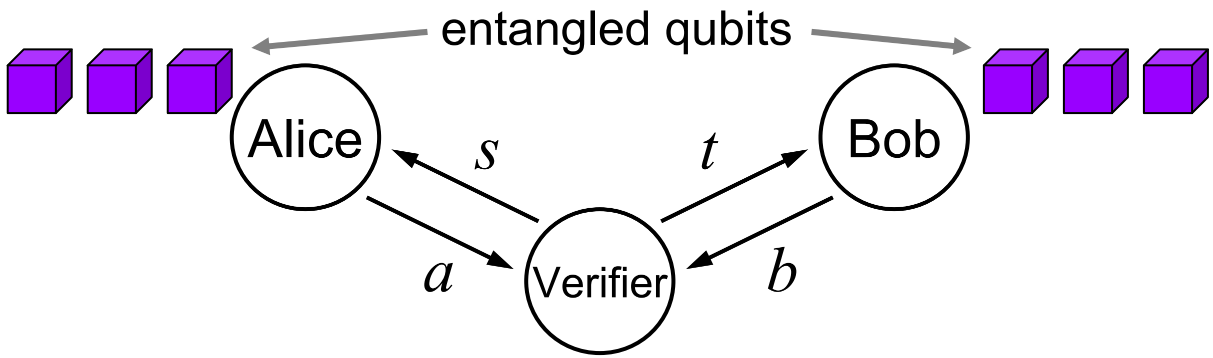


- A ***nonlocality game*** G consists of four sets A, B, S, T, a probability distribution π on $S \times T$, and a predicate $V : A \times B \times S \times T \rightarrow \{0,1\}$

- Verifier chooses $(s,t) \in S \times T$ according to π and, after receiving (a,b), ***accepts*** iff $V(a,b,s,t) = 1$

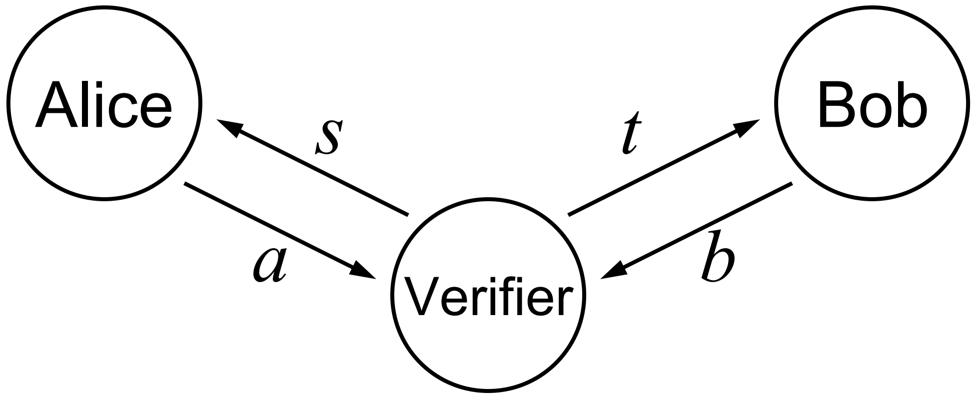
- The ***classical value*** of G, denoted as $\omega_c(G)$, is the maximum acceptance probability, over all classical strategies of Alice and Bob

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***

CHSH game



π uniform distribution on $\{0,1\}\times\{0,1\}$, and

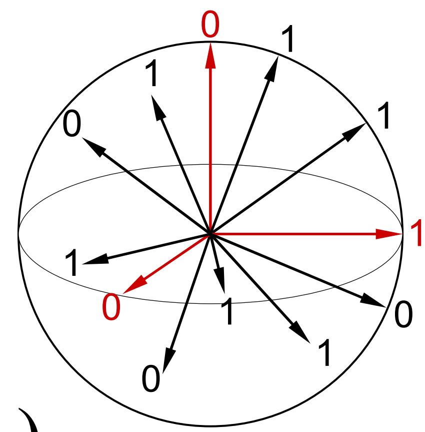
$V(a,b,s,t) = 1$ iff $a \oplus b = s \wedge t$

$$a_0 \oplus b_0 = 0$$
$$a_0 \oplus b_1 = 0$$
$$a_1 \oplus b_0 = 0$$
$$a_1 \oplus b_1 = 1$$

$\omega_c(G) = \frac{3}{4} = \frac{1}{2}\left(1 + \frac{1}{2}\right)$

$\omega_q(G) \geq \cos^2(\pi/8) = \frac{1}{2}\left(1 + \frac{1}{2}\sqrt{2}\right)$

Kochen-Specker game



- The Verifier sends Alice a triple of orthogonal vectors $s = (v_i, v_j, v_k)$ and Bob one vector $t = v_m$ from the triple
- Alice returns a, a valid labeling for (v_i, v_j, v_k), and Bob returns b, a label for v_m
- The verifier accepts iff the labels are consistent
- By the Kochen-Specker Theorem, $\omega_c(G) < 1$
- There is a perfect quantum strategy using entanglement $|\psi\rangle = |00\rangle + |11\rangle + |22\rangle$, therefore $\omega_q(G) = 1$

- ⊕-**MIP*** vs one-prover systems
- Nonlocal games (CHSH, KS)
- Quantum versus classical XOR games
- Odd Cycle game (blackboard)
- Magic Square game (blackboard)

XOR Games

- An ***XOR game*** is a nonlocality game where:
  - Alice and Bob's messages, a and b, are bits
  - The Verifier's decision is a function of s, t, $a \oplus b$
- **Example:** the CHSH game is an XOR game

ω_q vs ω_c for XOR games (I)

Theorem: for $\gamma \approx 0.72$ (formally, where a line through the origin meets the function $x \mapsto \sin^2(\pi x/2)$), for any XOR game,

$$\begin{cases} \omega_q(G) \le \sin^2\left(\frac{\pi}{2}\omega_c(G)\right) & \text{if } \omega_c(G) > \gamma, \\ \omega_q(G) \le \lambda \omega_c(G) & \text{if } \omega_c(G) \le \gamma, \end{cases}$$

where $\lambda = \pi \sin(\pi\gamma)/2 \approx 1.14$

Informally: for small ε, if $\omega_c(G) = 1 - \varepsilon$ then $\omega_q(G) \le 1 - c\varepsilon^2$, where $c \approx \pi^2/4 \approx 2.46$

Corollary: for the CHSH game, $\omega_q(G) \le \cos^2(\pi/8)$

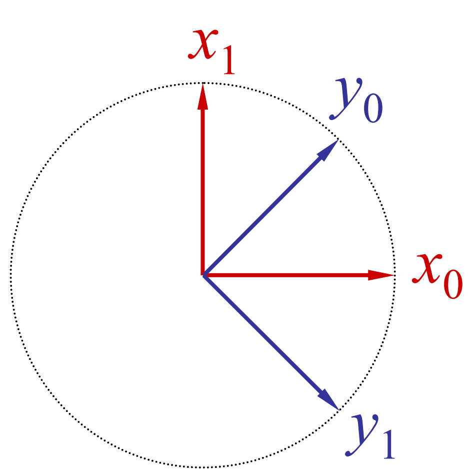
ω_q vs ω_c for XOR games (II)

To prove the theorem, we make use of

Theorem [Tsirelson '87]**:** for any XOR games, it's quantum strategies can be characterized by sets of 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:

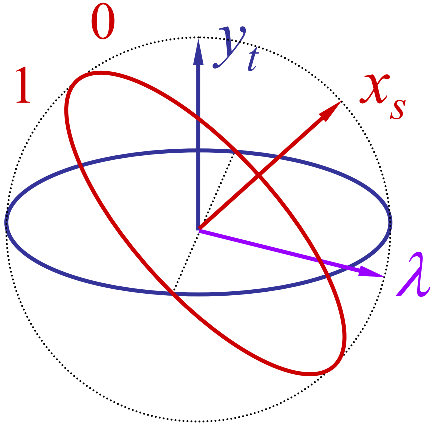


ω_q vs ω_c for XOR games (III)

Contrapositive: $\omega_q(G) > 1 - c\varepsilon^2$ implies $\omega_c(G) > 1 - \varepsilon$

For a quantum strategy, we have $\{x_s : s \in S\}$, $\{y_t : t \in T\}$

Classical strategy:



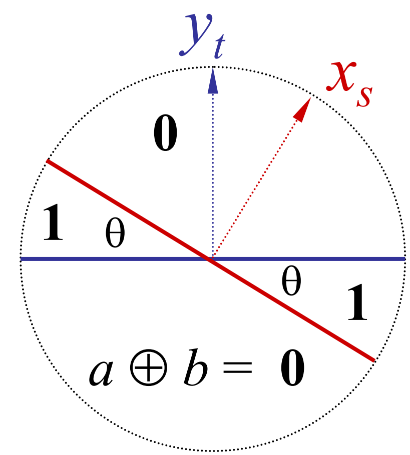
- Alice and Bob share a random vector $\lambda \in \mathbb{R}^n$
- On input s, Alice outputs 0 if $x_s \cdot \lambda \geq 0$ and 1 otherwise
- On input t, Bob outputs 0 if $y_t \cdot \lambda \geq 0$ and 1 otherwise

ω_q vs ω_c for XOR games (IV)

- **Classical protocol:**
  $p_c = \Pr[a \oplus b = 1] = \theta/\pi$

- **Quantum protocol:**
  $p_q = \Pr[a \oplus b = 1] = (1 - \cos(\theta))/2$

- Therefore, $p_q = (1 - \cos(\pi\, p_c))/2$
  $= \sin^2(\pi\, p_c/2)$



$\cos(\theta) = x_s \cdot y_t$

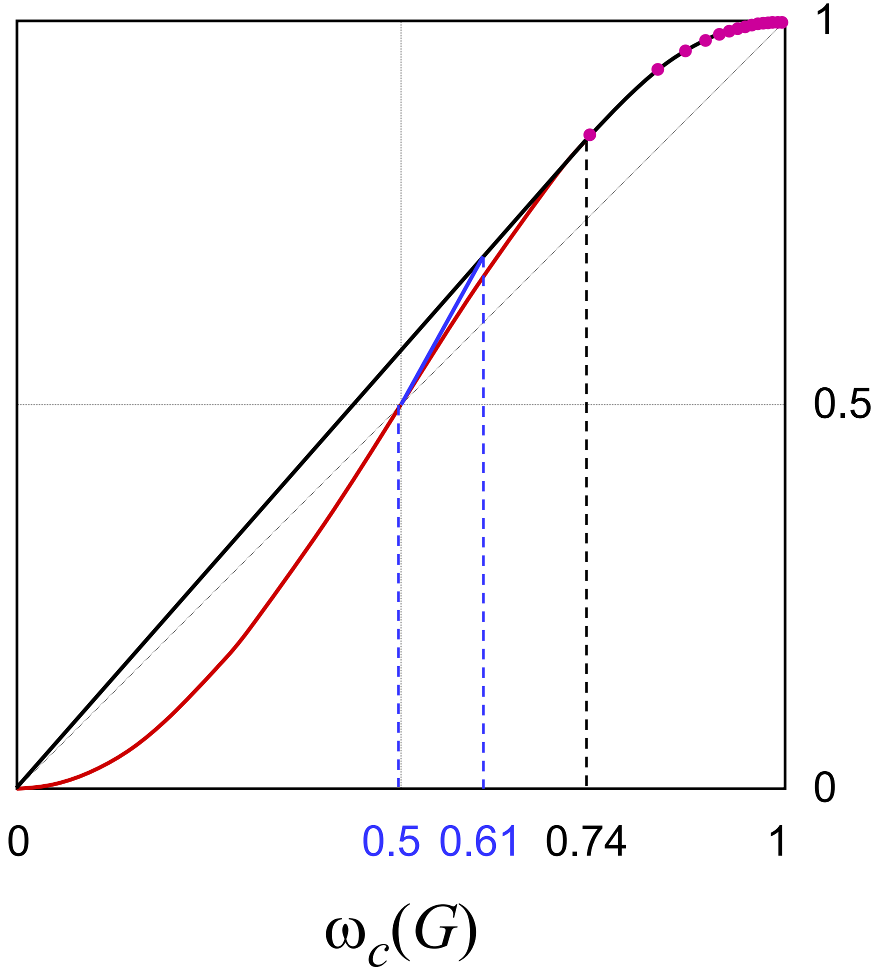
The quantum success probability is a convex combination of probabilities of the above form (averaged over all possible questions $(s,t) \in S \times T$)

ω_q vs ω_c for XOR games (V)

Upper bound of $\omega_q(G)$ in terms of $\omega_c(G)$ for XOR games

Tight bound for Odd Cycle games and Chained Bell Inequality games [Braunstein, Caves, 1990]

For ***nondegenerate*** XOR games, better bound when $0.5 \leq \omega_c(G) < 0.61$



Binary nonlocality games

Binary: $|A| = |B| = 2$ (but not necessarily XOR)

Theorem 2: for any binary game G, if $\omega_c(G) < 1$ then $\omega_q(G) < 1$

Note: no corresponding result if "binary" is relaxed to "ternary-binary": $|A| = 3$ and $|B| = 2$

Example: the Kochen-Specker game is ternary-binary with $\omega_c(G) < 1$ and $\omega_q(G) = 1$

- $\oplus$-**MIP*** vs one-prover systems
- Nonlocal games (CHSH, KS)
- Quantum versus classical XOR games
- Odd Cycle game (blackboard)
- Magic Square game (blackboard)

- $\oplus$-**MIP*** vs one-prover systems
- Nonlocal games (CHSH, KS)
- Quantum versus classical XOR games
- Odd Cycle game (blackboard)
- Magic Square game (blackboard)

THE END