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:

$$|\psi\rangle$$

$n$ qubits

$$U$$

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

Hard case (the general case):

$$U$$

$$|\psi\rangle$$

$n$ qubits

$$|0\rangle$$

$m$ qubits

(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 \textit{teleportation} and \textit{superdense coding}.

—but they \textit{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

$x_1 x_2 \ldots x_n$

Alice

Resources

$x_1 x_2 \ldots x_n$

Bob
Basic communication scenario

Bit communication:
- **Classical**
  - Cost: $n$

Bit communication & prior entanglement:
- (can be deduced)
  - Cost: $n$

Qubit communication:
- **Quantum**
  - Cost: $n$ [Holevo’s Theorem, 1973]

Qubit communication & prior entanglement:
- $n/2$ 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]

Input: $r$

Output: $a \leftarrow r$

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 $a \oplus b \oplus c = r \lor s \lor t$

<table>
<thead>
<tr>
<th>$rst$</th>
<th>$a \oplus b \oplus c$</th>
<th>$abc$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0 [green]</td>
<td>011</td>
</tr>
<tr>
<td>011</td>
<td>1 [lightgreen]</td>
<td>001</td>
</tr>
<tr>
<td>101</td>
<td>1 [lightgreen]</td>
<td>111</td>
</tr>
<tr>
<td>110</td>
<td>1 [red]</td>
<td>101</td>
</tr>
</tbody>
</table>
No perfect strategy for GHZ

General deterministic strategy:
\[ a_0, a_1, b_0, b_1, c_0, c_1 \]

Winning conditions:
\[ \begin{align*}
     a_0 \oplus b_0 \oplus c_0 &= 0 \\
     a_0 \oplus b_1 \oplus c_1 &= 1 \\
     a_1 \oplus b_0 \oplus c_1 &= 1 \\
     a_1 \oplus b_1 \oplus c_0 &= 1 
\end{align*} \]

Has no solution, thus no perfect strategy exists.
Input and output events can be \textit{space-like} separated: so signals at the speed of light are not fast enough for cheating.

What if Alice, Bob, and Carol \textit{still} keep on winning?
“GHZ Paradox” explained

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

Alice’s strategy:
1. if $r = 1$ then apply $H$ to qubit
2. measure qubit and set $a$ to result

Bob’s & Carol’s strategies: 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 $\frac{3}{4}$

• 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:

![Table with quantum states and outcomes](image)

called *hidden variables*

[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 $\pm 2$ and the other is 0

space-like separated, so no cross-coordination
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* *also called CHSH 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 $\leq \frac{1}{2}$

*also called CHSH Inequality*
Violating the Bell Inequality

Two-qubit system in state
\[ |\phi\rangle = |00\rangle - |11\rangle \]

Applying rotations \( \theta_A \) and \( \theta_B \) yields:
\[
\begin{align*}
    |\phi\rangle &= \cos(\theta_A + \theta_B) (|00\rangle - |11\rangle) + \sin(\theta_A + \theta_B) (|01\rangle + |10\rangle) \\
    AB &= +1 \\
    AB &= -1
\end{align*}
\]

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 \text{contradicts} the upper bound of \( \frac{1}{2} \)

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

output: $a$  $b$

Rules: 1. No communication after inputs received  
2. They win if $a \oplus b = s \wedge t$

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

But, with prior entanglement state $|00\rangle - |11\rangle$,  
$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = \frac{1}{2} + \frac{1}{4}\sqrt{2} = 0.853\ldots$
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:
\[
\Pr[a \oplus b = s \land t] = \cos^2(\pi/8) = \frac{1}{2} + \frac{1}{4}\sqrt{2} = 0.853\ldots
\]
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

- Information processing task
- Classically, communication is needed
- Quantum entanglement
Preview: magic square game

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

$$
\begin{array}{ccc}
\begin{array}{ccc}
11 & 12 & 13 \\
21 & 22 & 23 \\
31 & 32 & 33 \\
\end{array}
\end{array}
$$

**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:** $\frac{8}{9}$ 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]

\[ f(x, y) \]

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 $f(x,y)$:

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>101</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>111</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Suppose the communication complexity of $f$ is $k$

Each input in the domain of $f$ fixes a conversation $C \in \{0,1\}^{k+1}$ (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 $f(x,y)$:

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>101</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>111</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

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 $x \neq y$,

$$\Delta(e(x),e(y)) \geq \delta cn$$

(\Delta means Hamming distance), where $c, \delta$ are constants

$x_1 x_2 \ldots x_n$ $y_1 y_2 \ldots y_n$

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

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

Classically, $\Omega(n)$ bits necessary to succeed with prob. $\geq \frac{3}{4}$

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

[KS ‘87] [BCW ‘98]
Search problem

Given: \( x = \begin{array}{cccccccc}
0 & 0 & 0 & 0 & 1 & 0 & \ldots & 1
\end{array} \)

accessible via queries

\[
\log n \left\{ \begin{array}{c}
|i\rangle \\
1
\end{array} \right\} \xrightarrow{x} \left\{ \begin{array}{c}
|i\rangle \\
|b\rangle \oplus x_i\rangle
\end{array} \right\}
\]

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]
Alice: \[ x = \begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
0 & 1 & 1 & 0 & 1 & 0 \\
\end{array} \ldots 0 \]

Bob: \[ y = \begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
1 & 0 & 0 & 1 & 1 & 0 \\
\end{array} \ldots 1 \]

\[ x \wedge y = \begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
0 & 0 & 0 & 0 & 1 & 0 \\
\end{array} \ldots 0 \]

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 \( \Delta(x, y) = n/2 \)

(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 \( \frac{1}{4} \) is permitted?
Answer: Just 2 bits are sufficient!
Exponential quantum vs. classical separation in bounded-error models

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

**Classical** description of

$|\psi\rangle$: a $\log(n)$-qubit state

$M$: two-outcome measurement

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

**Classical** description of

$U$: $\log(n)$-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

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

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

Quantum protocols *also* require $\Omega(n)$ communication.
The Bernstein-Vazirani problem

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

Given:

\[
\begin{align*}
|b\rangle & \quad \quad |b\rangle \\
|b \oplus f(x_1, x_2, \ldots, x_n)\rangle & \quad \quad |b \oplus f(x_1, x_2, \ldots, x_n)\rangle \\
|x_1\rangle & \quad \quad |x_1\rangle \\
|x_2\rangle & \quad \quad |x_2\rangle \\
\vdots & \quad \quad \vdots \\
|x_n\rangle & \quad \quad |x_n\rangle
\end{align*}
\]

with unknown \( a_1, a_2, \ldots, a_n \)

Goal: determine \( a_1, a_2, \ldots, a_n \)

Classically, \( n \) queries are necessary
The Bernstein-Vazirani problem

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

Given:

\[
\begin{align*}
|0\rangle & \quad H \quad H \quad |a_1\rangle \\
|0\rangle & \quad H \quad H \quad |a_2\rangle \\
: & \quad H \quad H \quad : \\
|0\rangle & \quad H \quad H \quad |a_n\rangle \\
|1\rangle & \quad H \quad H \quad |1\rangle
\end{align*}
\]

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

\[ \text{IP}(x, y) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \mod 2 \]

Proof:

Alice and Bob’s IP protocol

Alice and Bob’s IP protocol inverted

Proof:
Lower bound for inner product

\[ \text{IP}(x, y) = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \mod 2 \]

Proof:

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

\[ x_1 x_2 \ldots x_n \quad y_1 y_2 \ldots y_n \]

classically correlated

\[ f(x,y) \]

Pr[00] = Pr[11] = \( \frac{1}{2} \)

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 \( k \)
Equality revisited in simultaneous message model

\[ x_1 x_2 \ldots x_n \]

\[ y_1 y_2 \ldots y_n \]

Bounded-error protocols \textit{without} a shared key:

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

\textbf{Quantum:} \( \theta(\log n) \) using quantum fingerprints

\[ f(x,y) \]

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

Question 1: how many orthogonal states in $m$ qubits?

Answer: $2^m$

Let $\varepsilon$ 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: $2^{2am}$, 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 $x \neq y$,

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

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

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: $(1-2\delta)^r \leq \epsilon$

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 $|\psi_{000}\rangle$, $|\psi_{001}\rangle$, ..., $|\psi_{111}\rangle$ 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

$\begin{align*}
& x_1 x_2 \ldots x_n \\
& y_1 y_2 \ldots y_n
\end{align*}$

Bounded-error protocols \textit{without} a shared key:

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

\textbf{Quantum: } $\theta(\log n)$

[A '96] [NS '96] [BCWW '01]
Quantum protocol for equality in simultaneous message model

\[ x_1 x_2 \ldots x_n \]

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

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: \( x \in \{0,1\}^n \)

\[ M = \begin{array}{c}
\text{matching on} \\
\{1,2, \ldots, n\}
\end{array} \]

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: \( x \in \{0,1\}^n \)

\[ M = \begin{array}{ccc}
\text{matching on} & \{1,2, \ldots, n\} \\
\end{array} \]

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 (MIPs)
  – 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:

\[ f(x_1, \ldots, x_n) = (x_1 \lor \overline{x}_3 \lor x_4) \land (\overline{x}_2 \lor x_3 \lor \overline{x}_5) \land \cdots \land (\overline{x}_1 \lor x_5 \lor \overline{x}_n) \]

\( f(x_1, \ldots, x_n) \) 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

\[ \textbf{NP} \] denotes the class of languages \( L \) whose positive instances have such “witnesses” that can be verified in polynomial time
“Complexity Theory 101”

\( \mathbf{P} \): solvable in time \( O(n^c) \)

\( \mathbf{NP} \): positive instances verifiable in time \( O(n^c) \)

\( \mathbf{PSPACE} \): solvable with space \( O(n^c) \)

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

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

\( \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP} \subseteq \mathbf{NEXP} \)
Interactive proof systems

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

is $x \in L$?

Verifier \quad \text{questions} \quad \text{responses} \quad \text{Prover}

- The Verifier must be efficient (polynomial time), but the Prover is computationally unbounded
- **Soundness**: if $x \notin L$, no Prover causes the Verifier to accept (small error probability is okay)
- **Completeness**: if $x \in L$, 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 (MIPs)
  – Classical \( \oplus\text{-MIP} = \text{MIP} = \text{NEXP} \)
  – Quantum \( \oplus\text{-MIP}^* \subseteq \text{EXP} \)
Two provers

With two provers, who cannot communicate with each other, the expressive power increases to $\text{NEXP}$ (nondeterministic exponential-time)

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

[Babai, Fortnow, Lund, 1991]
Sample protocol for 3SAT ...

Instance: \((x_1 \lor \overline{x}_3 \lor x_4) \land (\overline{x}_2 \lor x_3 \lor \overline{x}_5) \land (\overline{x}_1 \lor x_5 \lor \overline{x}_n)\)

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 “\((\overline{x}_2 \lor x_3 \lor \overline{x}_5)\)” 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

\[ f(x_1, \ldots, x_n) = \left[ \bigwedge_{v_i \perp v_j} (\overline{x_i} \lor \overline{x_j}) \right] \land \left[ \bigwedge_{v_i \perp v_j \perp v_k} (x_i \lor x_j \lor x_k) \right] \]

- By the Kochen-Specker Theorem, this formula is unsatisfiable—therefore, for classical Provers, the Verifier accepts with probability \textit{less than one}

- But, using the quantum strategy for the KS game, the Provers can cause the Verifier to \textit{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]:
  \( \text{MIP} = \text{NEXP} \)

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

• Open questions:
  \( \text{Is } \text{NEXP} \subseteq \text{MIP}^*? \)
  \( \text{Is } \text{MIP}^* \subseteq \text{NEXP}? \)
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: $a \oplus b = s \land t$
Theorem 1: $\oplus$-MIP = NEXP (= MIP)

Theorem 2: $\oplus$-MIP* ⊆ EXP

Therefore, $\oplus$-MIP* is strictly weaker than $\oplus$-MIP (unless EXP = NEXP)
• Interactive proof systems

• Two-prover interactive proof systems (MIPs)
  – Classical \( \oplus \text{-MIP} = \text{MIP} = \text{NEXP} \)
  – Quantum \( \oplus \text{-MIP}^* \subseteq \text{EXP} \)
Proof that $\text{NEXP} \subseteq \oplus\text{-MIP}$ (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)

![Diagram of verifier and prover interaction](image)

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

\[0110101001101010011\]

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

[Håstad ’01][Bellare, Goldreich, Sudan ’98]
Proof that \( \text{NEXP} \subseteq \oplus\text{-MIP} \) (II)

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

\[
\begin{array}{cccccccccc}
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & \ldots & 1 & 0 & 0 \\
x & y & z
\end{array}
\]

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

A test for \( x \oplus y \oplus z = 0 \)

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

\[
\begin{array}{cccc}
0 & \text{fixed} & & \\
& 1 & \text{fixed} & \\
& & 1 & \text{fixed} \\
\end{array}
\]

\( a \oplus b = 1 \) (different)

\( a \oplus b = 0 \) (same)

[H ’01][BGS ’98]
Proof that $\text{NEXP} \subseteq \oplus\text{-MIP (III)}$

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

$\begin{array}{ccccccccccc}
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & \ldots & 1 & 0 & 0
\end{array}$

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

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

If $x \oplus y \oplus z = 1$ then it 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)

Finally, can “unfix” fixed bit

---

$a \oplus b = 1$ (different)

$a \oplus b = 0$ (same)
Proof that $\text{NEXP} \subseteq \oplus\text{-MIP (IV)}$

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

What follows is a $\Theta\text{-MIP}_{0.6875 + \varepsilon, 0.75}$ proof system for $\text{NEXP}$.

Therefore $\text{NEXP} \subseteq \Theta\text{-MIP}$.
• Interactive proof systems

• Two-prover interactive proof systems (MIPs)
  – Classical $\oplus\text{-MIP} = \text{MIP} = \text{NEXP}$
  – Quantum $\oplus\text{-MIP}^* \subseteq \text{EXP}$
⊕-MIP* ⊆ EXP

is \( x \in L? \)

Alice \( \rightarrow \) question \( a \) (1 bit) \( \leftarrow \) Bob

Verifier

question \( b \) (1 bit)
\( \Theta \text{-MIP}^* \subseteq \text{EXP (I)} \)

**Theorem** [Tsirelson, 1987]: every *quantum* \( \Theta \)-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

\[
\Pr[a \oplus b = 0] = \frac{1 + x_s \cdot y_t}{2}
\]

**Example:** vectors in \( \mathbb{R}^2 \) for the CHSH game:
$$\oplus\text{-MIP}^* \subseteq \text{EXP (II)}$$

**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 $\oplus$-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 \( \Theta \)-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:

\[
\langle \psi | A_s \otimes B_t | \psi \rangle = (\langle \psi | A_s \otimes I \rangle ) (I \otimes B_t | \psi \rangle)
\]

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 $M_1, M_2, ..., M_k$ 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 $v = (v_1, v_2, ..., v_k)$ into the observable $M^v = v_1 M_1 + v_2 M_2 + ... + v_k M_k$

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

It follows from this that, setting $|\psi\rangle = |1\rangle|1\rangle + |2\rangle|2\rangle + ... + |d\rangle|d\rangle$ 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 languages 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
• $\oplus$-MIP* vs one-prover systems
• Nonlocal games (CHSH, KS)
• Quantum versus classical XOR games
• Odd Cycle game (blackboard)
• Magic Square game (blackboard)
A nonlocality game $G$ consists of four sets $A$, $B$, $S$, $T$, a probability distribution $\pi$ 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 $\pi$ 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**.
\[ V(a, b, s, t) = 1 \text{ iff } a \oplus b = s \land t \]
\[ \omega_c(G) = \frac{3}{4} = \frac{1}{2} \left( 1 + \frac{1}{2} \right) \]
\[ \omega_q(G) \geq \cos^2(\pi/8) = \frac{1}{2} \left( 1 + \frac{1}{2}\sqrt{2} \right) \]
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 \( \omega_q(G) = 1 \)
• $\oplus$-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
  - TheVerifier’s decision is a function of $s, t, a \oplus b$

- **Example**: the CHSH game is an XOR game
\( \omega_q \text{ vs } \omega_c \text{ for XOR games (I)} \)

**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,

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

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

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

**Corollary:** for the CHSH game, \( \omega_q(G) \leq \cos^2(\pi/8) \)
$\omega_q \textit{ vs } \omega_c \textit{ for XOR games (II)}$

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 $(s,t) \in S \times T$,

$$\Pr[a \oplus b = 0] = \frac{1 + x_s \cdot y_t}{2}$$

E.g., vectors in $\mathbb{R}^2$ for the CHSH game:
ω_q vs ω_c for XOR games (III)

Contrapositive: ω_q(G) > 1 – cε² implies ω_c(G) > 1 – ε

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
\( \omega_q \text{ vs } \omega_c \text{ for XOR games (IV)} \)

- Classical protocol:
  \[ p_c = \Pr[a \oplus b = 1] = \frac{\theta}{\pi} \]

- Quantum protocol:
  \[ p_q = \Pr[a \oplus b = 1] = \frac{1 - \cos(\theta)}{2} \]

- Therefore,
  \[ p_q = \frac{1 - \cos(\pi p_c)}{2} = \sin^2\left(\frac{\pi p_c}{2}\right) \]

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