Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 467 / Phys 767
C&O 481 / C&O 681

Lecture 17 (2005)

Richard Cleve
DC 3524
cleve@cs.uwaterloo.ca

Course web site at:
http://www.cs.uwaterloo.ca/~cleve/courses/cs467

Contents

- Communication complexity
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting
- Hidden matching problem
- Nonlocality revisited

- Communication complexity
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting
- Hidden matching problem
- Nonlocality revisited

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

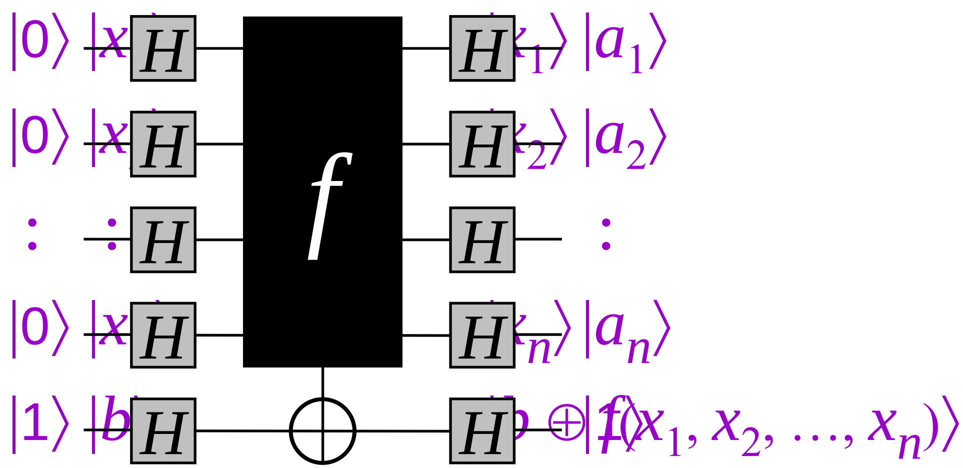
[KY '95] [CNDT '98] [NS '02]

The BV black-box problem

Bernstein & Vazirani

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 $a_1, a_2, \ldots, a_n$

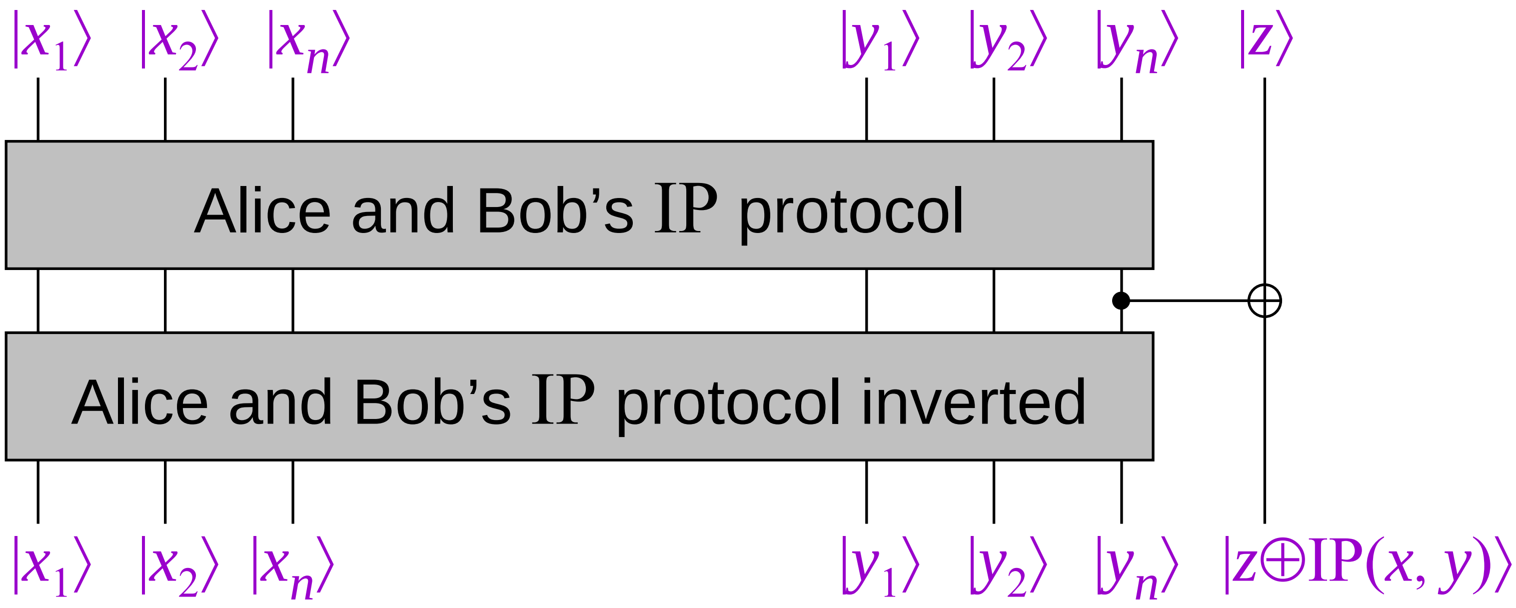
Classically, n queries are necessary

Quantum mechanically, 1 query is sufficient

Lower bound for inner product

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

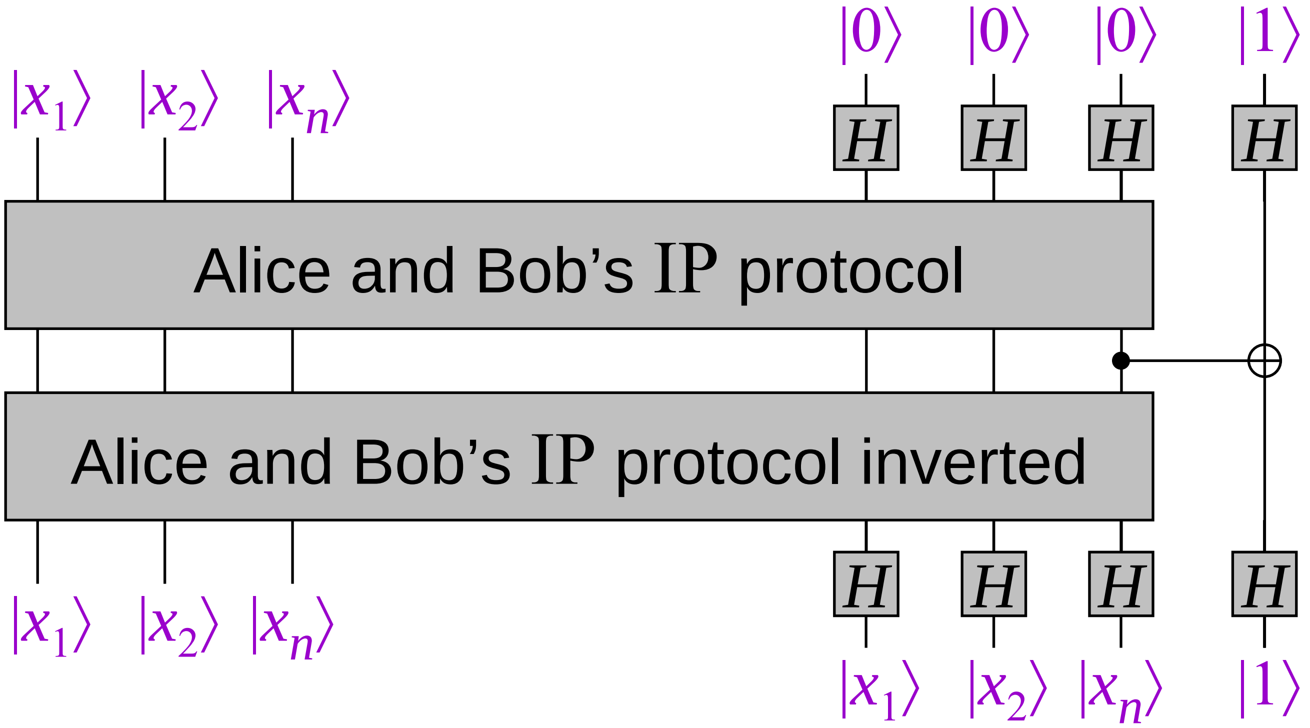
Proof:



Lower bound for inner product

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

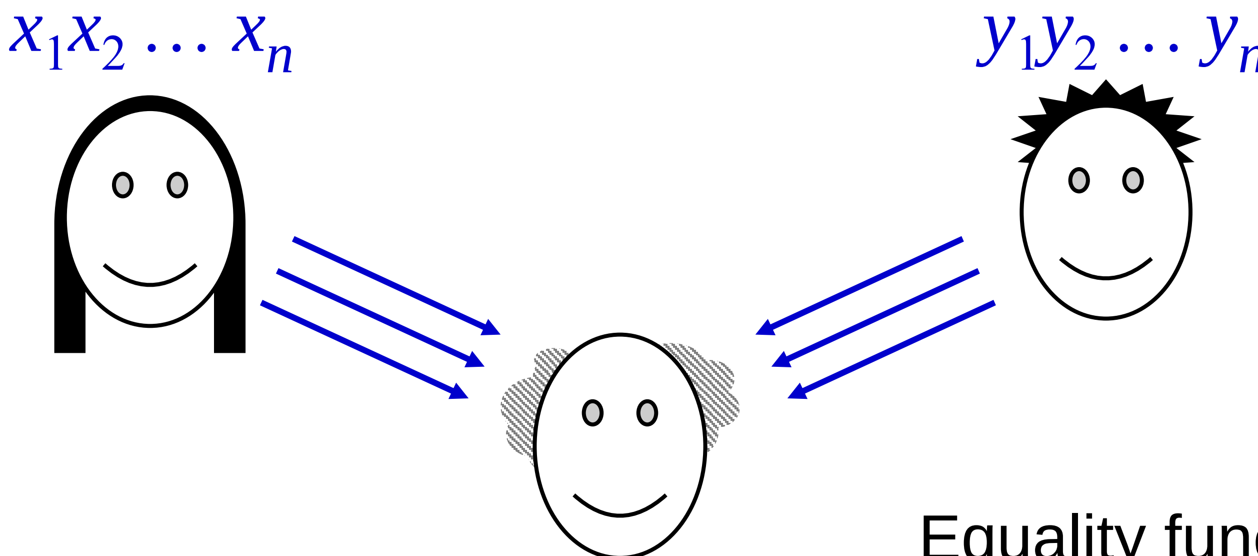
Proof:



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

- Communication complexity
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting
- Hidden matching problem
- Nonlocality revisited

Equality revisited
in simultaneous message model



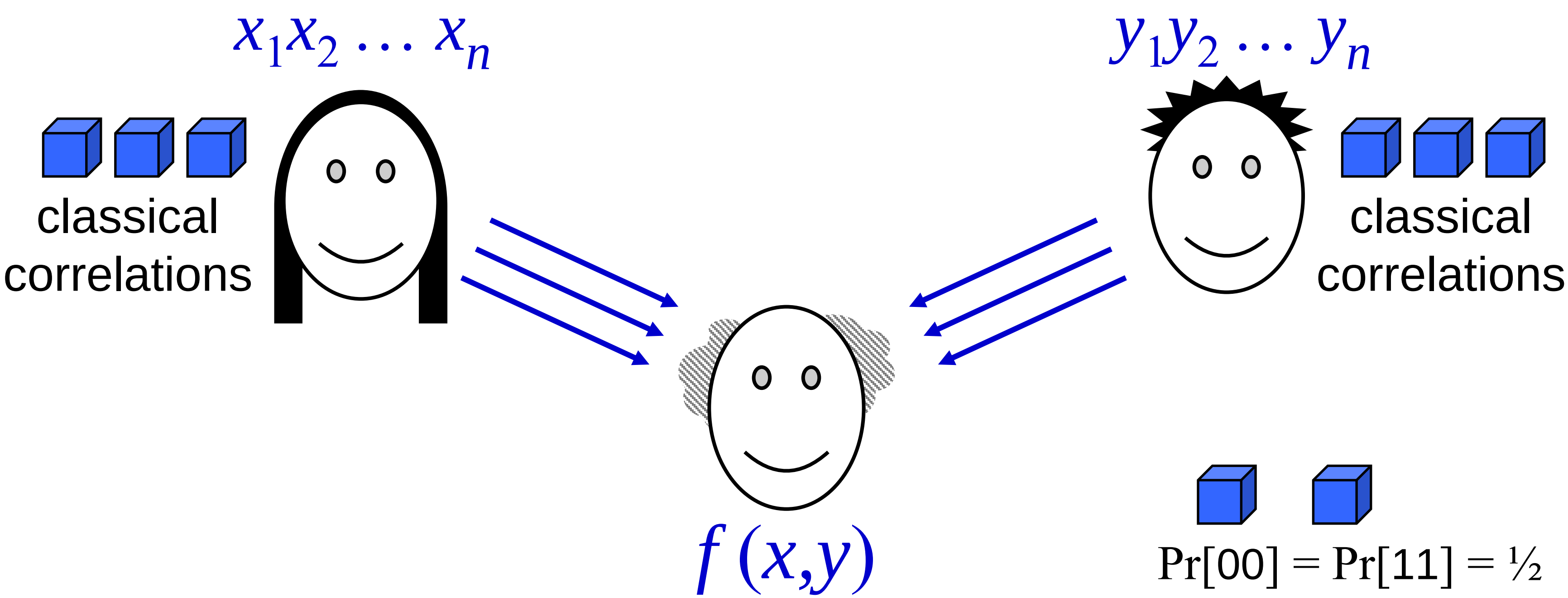
$f(x,y)$

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

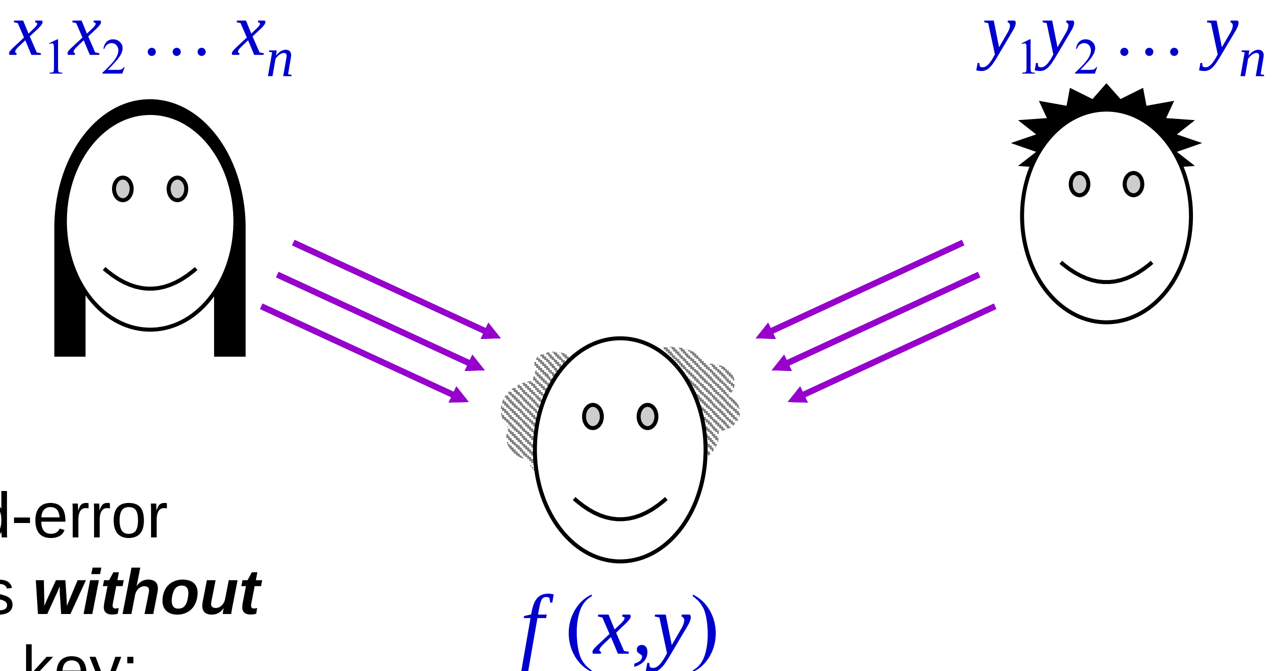
Error-correcting code: $e(x) = 1\ 0\ 1\ 1\ 1\ \boxed{1}\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1$

$e(y) = 0\ 1\ 1\ 0\ 1\ \boxed{0}\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0$

random $\boldsymbol{k}$

Equality revisited

in simultaneous message model



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

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

Quantum: $\theta(\log n)$

[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 $a > 0$

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

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

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: $(1-2d)^r \leq \varepsilon$

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

(as opposed to n qubits!)

What are 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

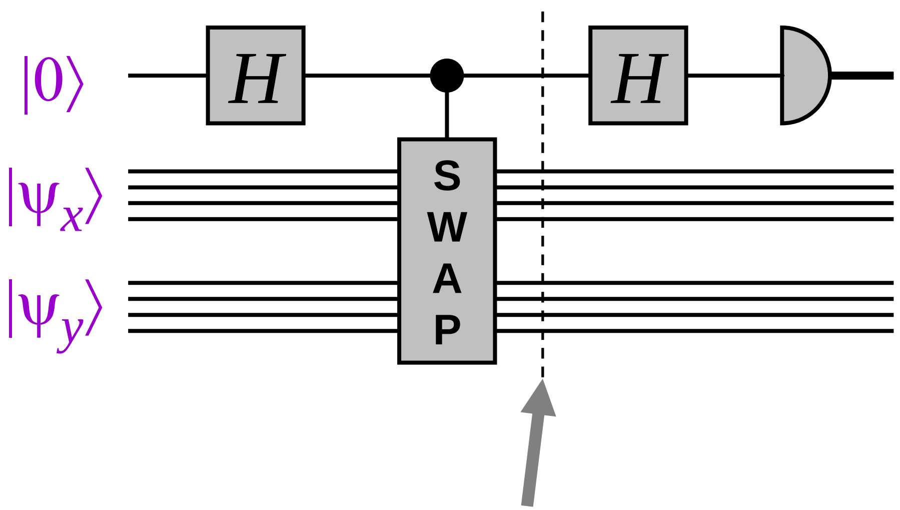
Here's what we *can* do: given two states from an almost orthogonal set, we can distinguish between these two cases:
- they're both the same state
- they're almost orthogonal

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:



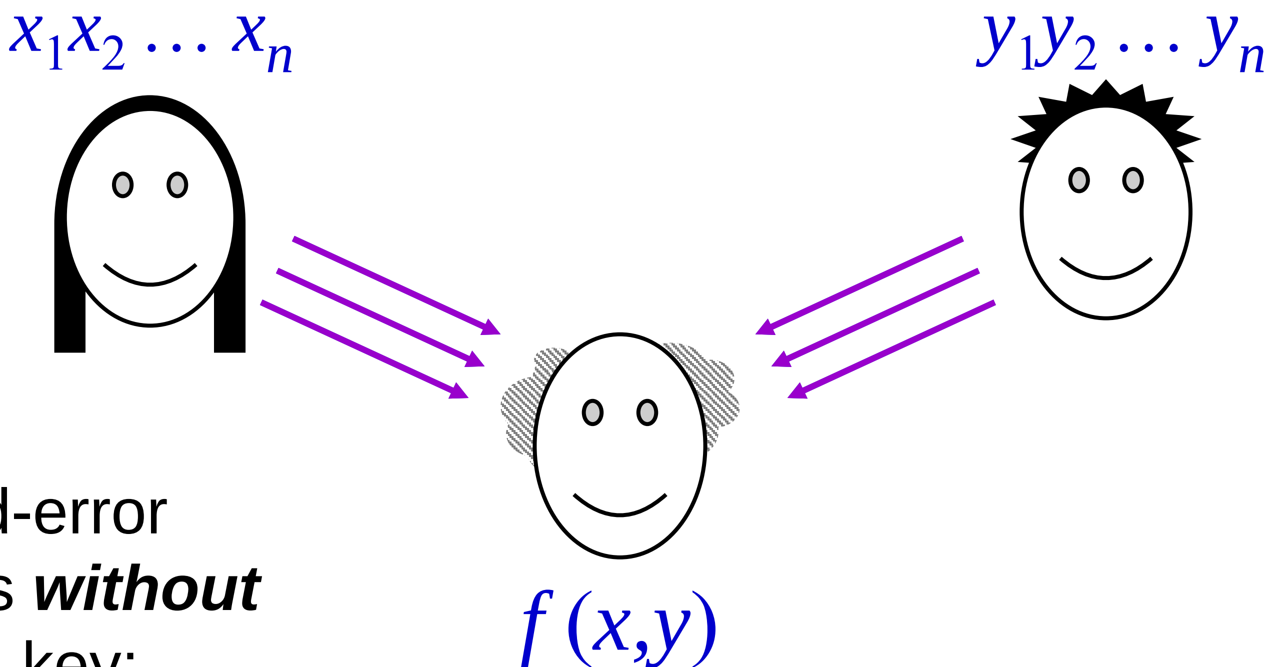
if $x = y$, $\Pr[\text{output} = 0] = 1$

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



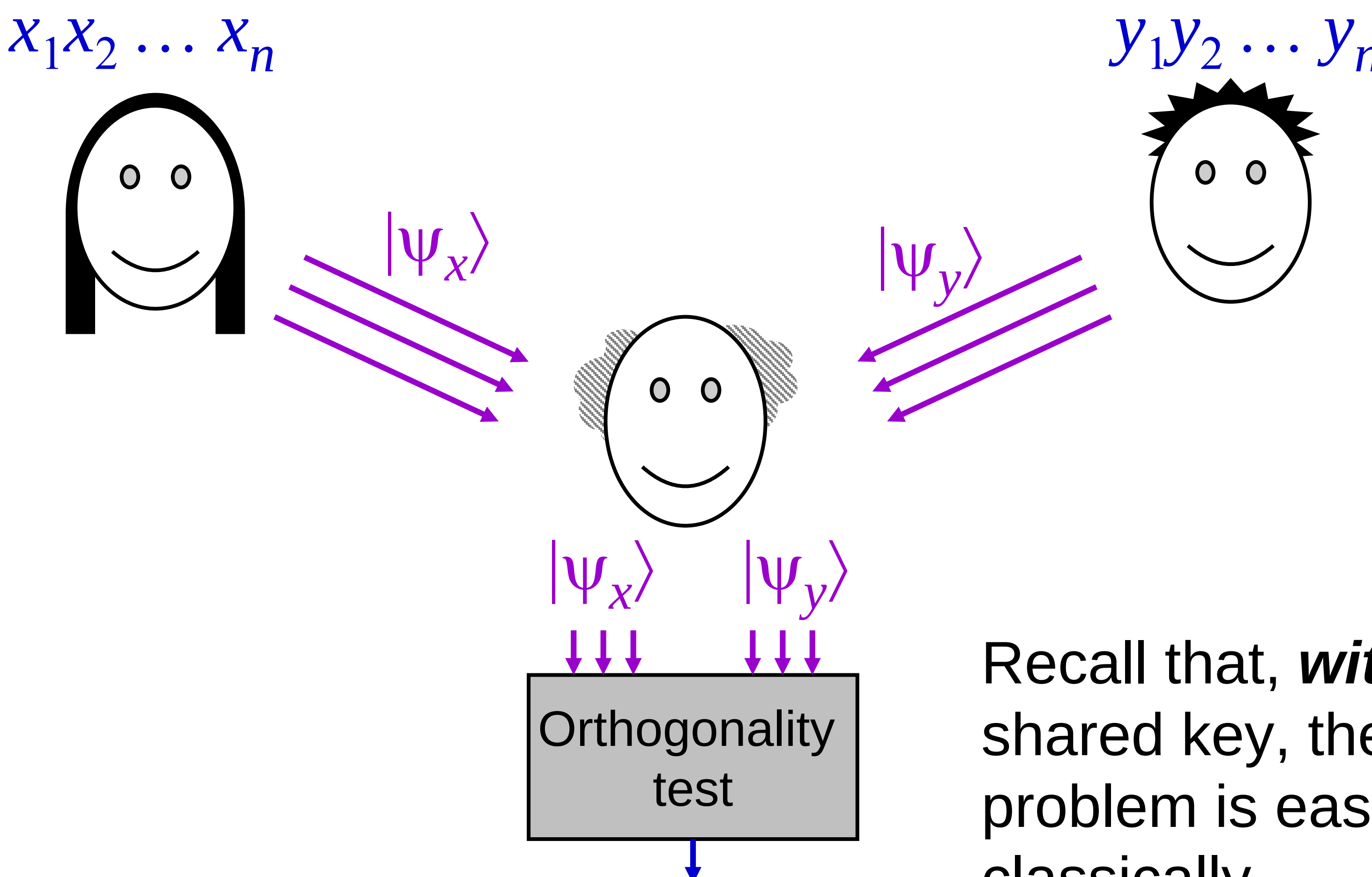
Bounded-error protocols ***without*** a shared key:

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

Quantum: $\theta(\log n)$

[A ’96] [NS ’96] [BCWW ’01]

Quantum protocol for equality
in simultaneous message model



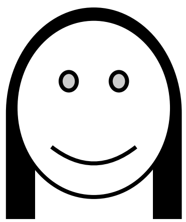
Recall that, ***with*** a shared key, the problem is easy classically ...

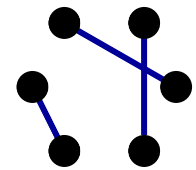
- Communication complexity
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting
- Hidden matching problem
- Nonlocality revisited

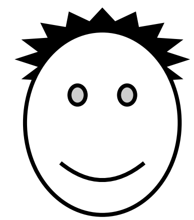
Hidden matching problem

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 $\{1, 2, \ldots, n\}$



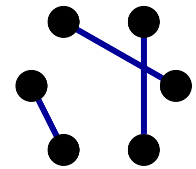
Output: $(i, j, x_i \oplus x_j)$, such that $(i, j) \in M$

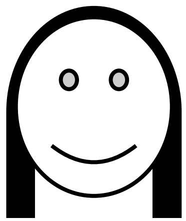
Only ***one-way*** communication (Alice to Bob) is permitted

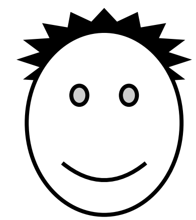
[Bar-Yossef, Jayram, Kerenidis, 2004]

The hidden matching problem

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

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





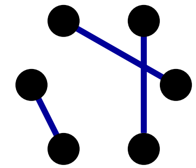
Output: $(i, j, x_i \oplus x_j)$, $(i, j) \in M$

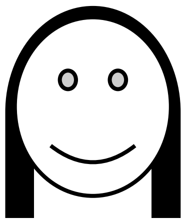
Classically, one-way communication is $\Omega(\sqrt{n})$, even with a shared classical key (the proof is omitted here)

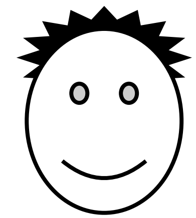
Rough intuition: Alice doesn't know which edges are in M, so she apparently has to send $\Omega(\sqrt{n})$ bits of the form $x_i \oplus x_j$ …

The hidden matching problem

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

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





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

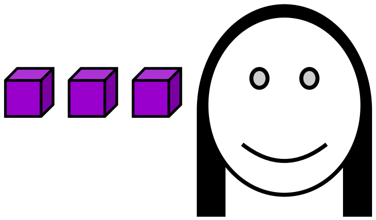
Quantum protocol: Alice sends $\frac{1}{\sqrt{n}}\sum_{k=1}^{n}(-1)^{x_k}|k\rangle$ ($\log n$ qubits)

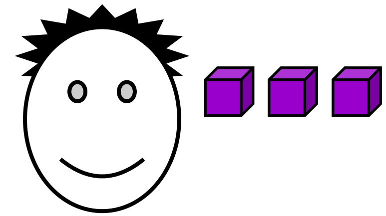
Bob measures in $|i\rangle \pm |j\rangle$ basis, $(i, j) \in M$, and uses the outcome's relative phase to determine $x_i \oplus x_j$

- Communication complexity
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting
- Hidden matching problem
- Nonlocality revisited

Restricted-equality nonlocality

inputs: x (n bits) y (n bits)





outputs: a ($\log n$ bits) b ($\log n$ bits)

Precondition: either $x = y$ or $\Delta(x,y) = n/2$

Required postcondition: $a = b$ iff $x = y$

With classical resources, $\Omega(n)$ bits of communication needed ***for an exact solution****

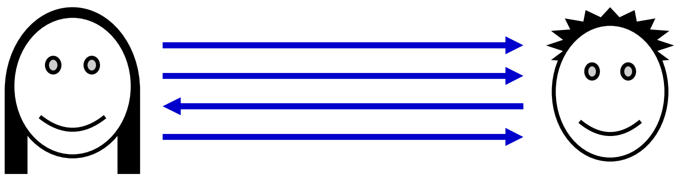
With $(|00\rangle + |11\rangle)^{\otimes \log n}$ prior entanglement, no communication is needed at all*

$\ast$ Technical details similar to restricted equality of Lecture 17

[BCT '99]

Restricted-equality nonlocality

Bit communication:

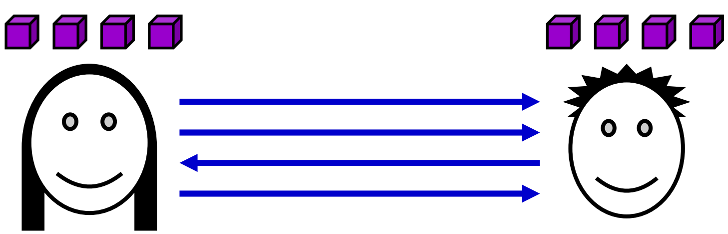


Cost: $\theta(n)$

Qubit communication:

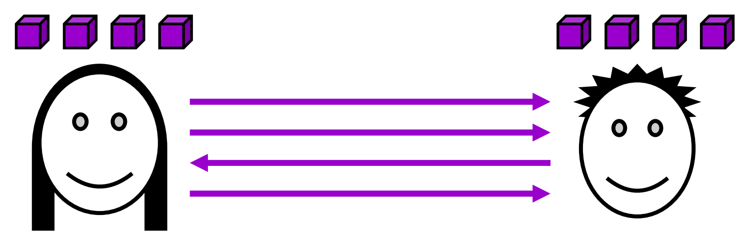
Cost: $\log n$

Bit communication & prior entanglement:



Cost: zero

Qubit communication & prior entanglement:



Cost: zero

Nonlocality and communication complexity conclusions

- Quantum information affects communication complexity in interesting ways
- There is a rich interplay between quantum communication complexity and:
  - quantum algorithms
  - quantum information theory
  - other notions of complexity theory …

THE END