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

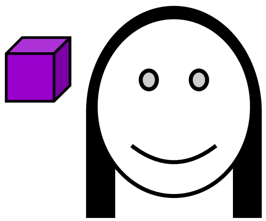
- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting

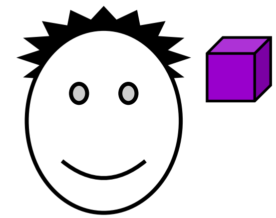
- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting

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 $|00\rangle - |11\rangle$,

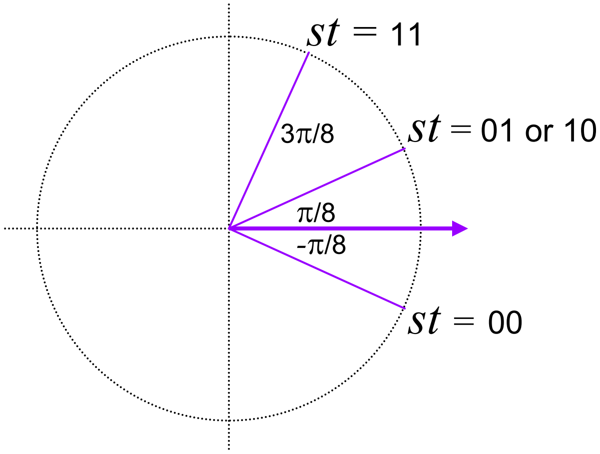
$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = ½ + ¼\sqrt{2} = 0.853\ldots$

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

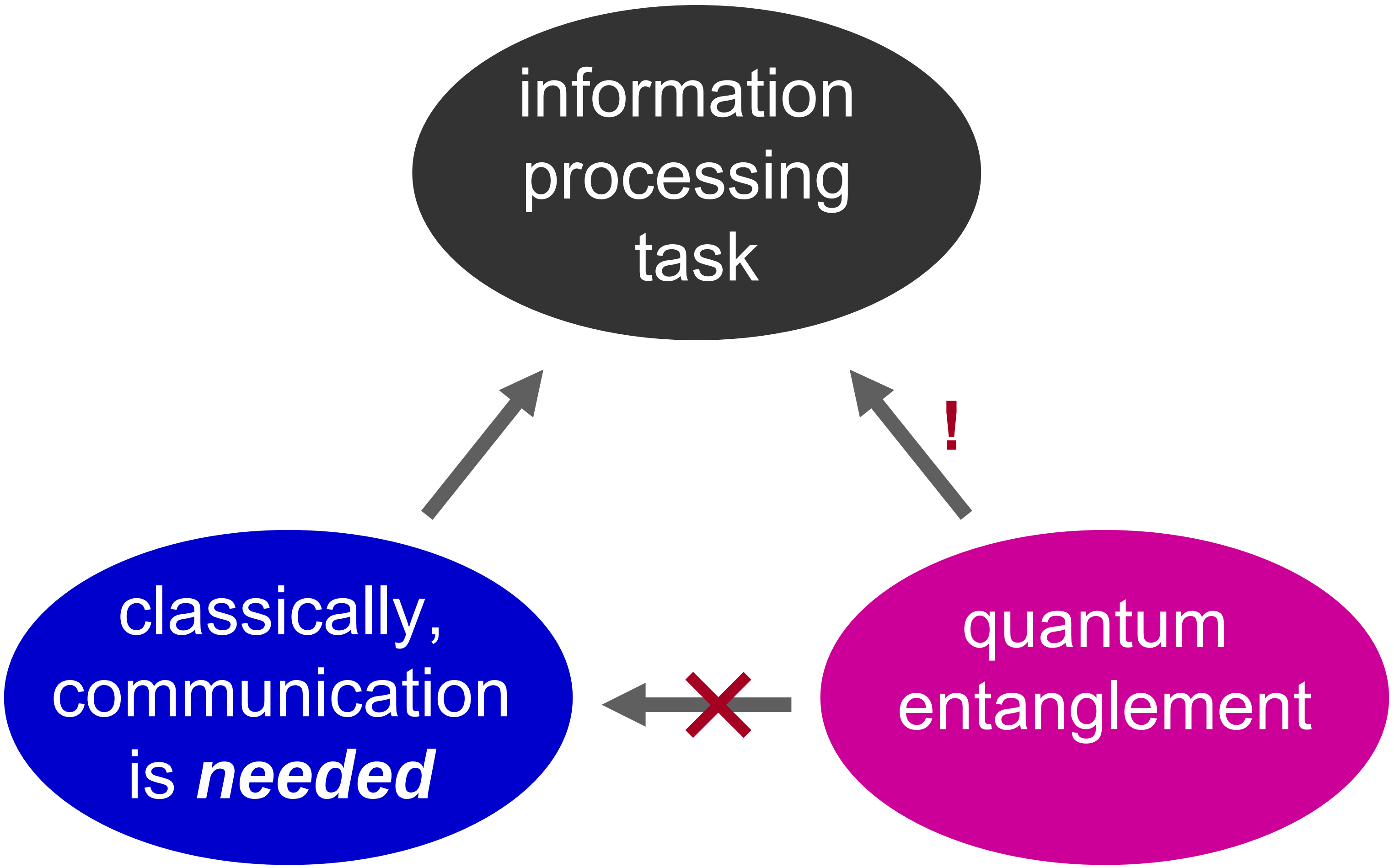


$$\cos(\theta_A - \theta_B)\,(|00\rangle - |11\rangle) + \sin(\theta_A - \theta_B)\,(|01\rangle + |10\rangle)$$

Success probability:

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

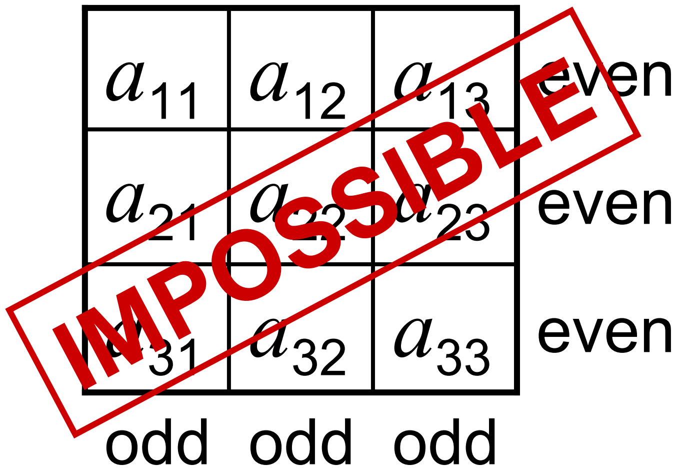
Nonlocality in operational terms

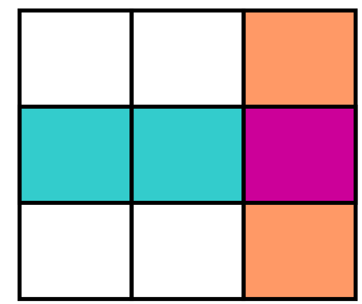


- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting

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

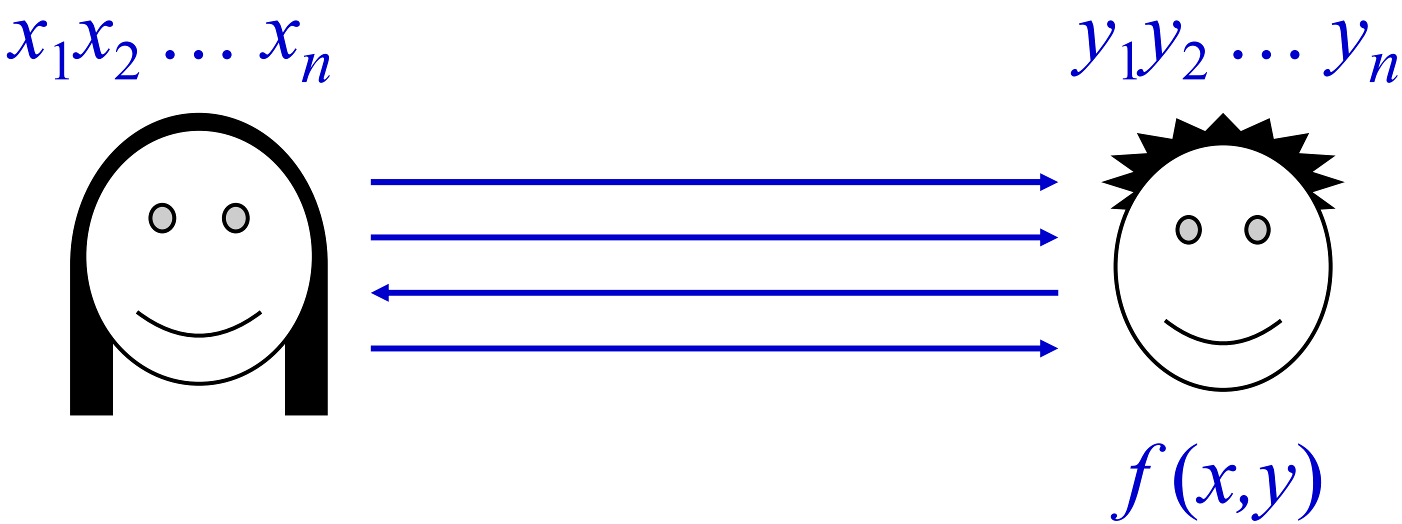
Success probabilities: $8/9$ classical and 1 quantum

[Aravind, 2002] (details omitted here)

- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting

Classical communication complexity

[Yao, 1979]



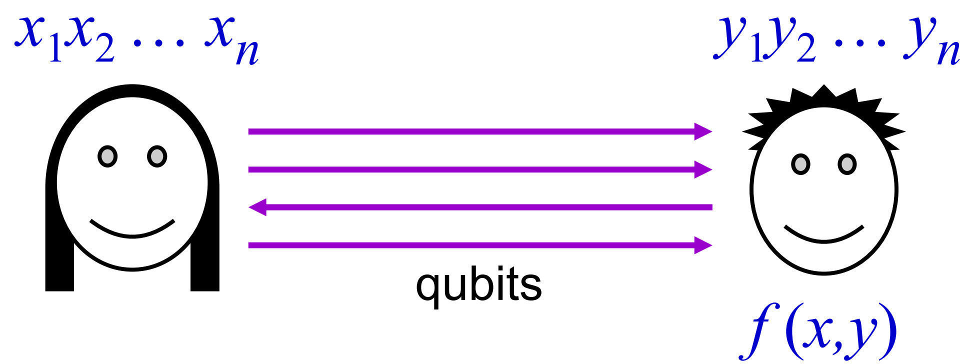
E.g. equality function: $f(x,y) = 1$ if $x = y$, and 0 if $x \neq y$

Any ***deterministic*** protocol requires n bits communication

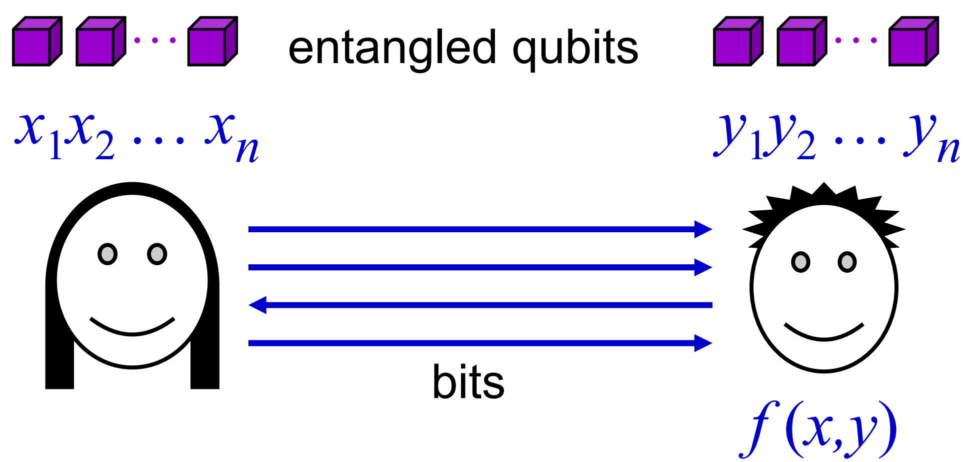
Probabilistic protocols can solve with only $O(\log(n/\varepsilon))$ bits communication (error probability ε), via random hashing

Quantum communication complexity

Qubit communication



Prior entanglement



- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting

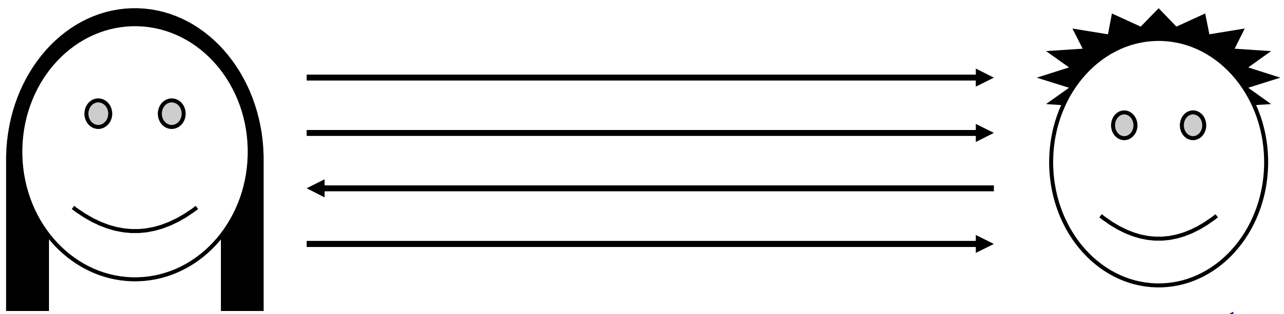
Appointment scheduling

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. $\geq 3/4$

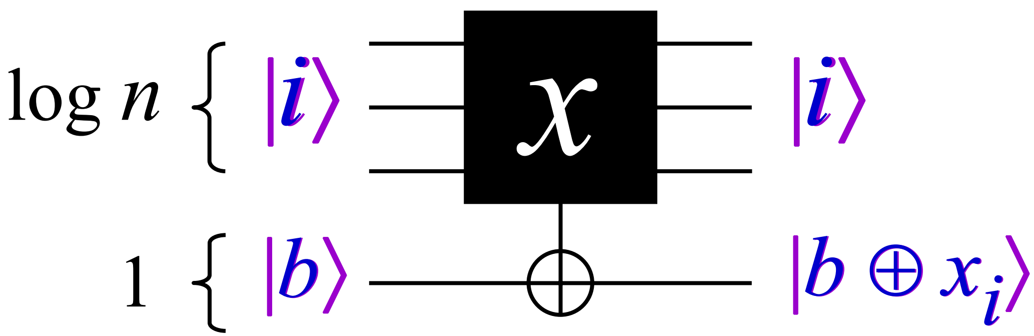
For all $\varepsilon > 0$, $O(n^{1/2} \log n)$ **qubits** sufficient for error prob. $< \varepsilon$

[KS ‘87] [BCW ‘98]

Search problem

1 2 3 4 5 6 . . . n

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



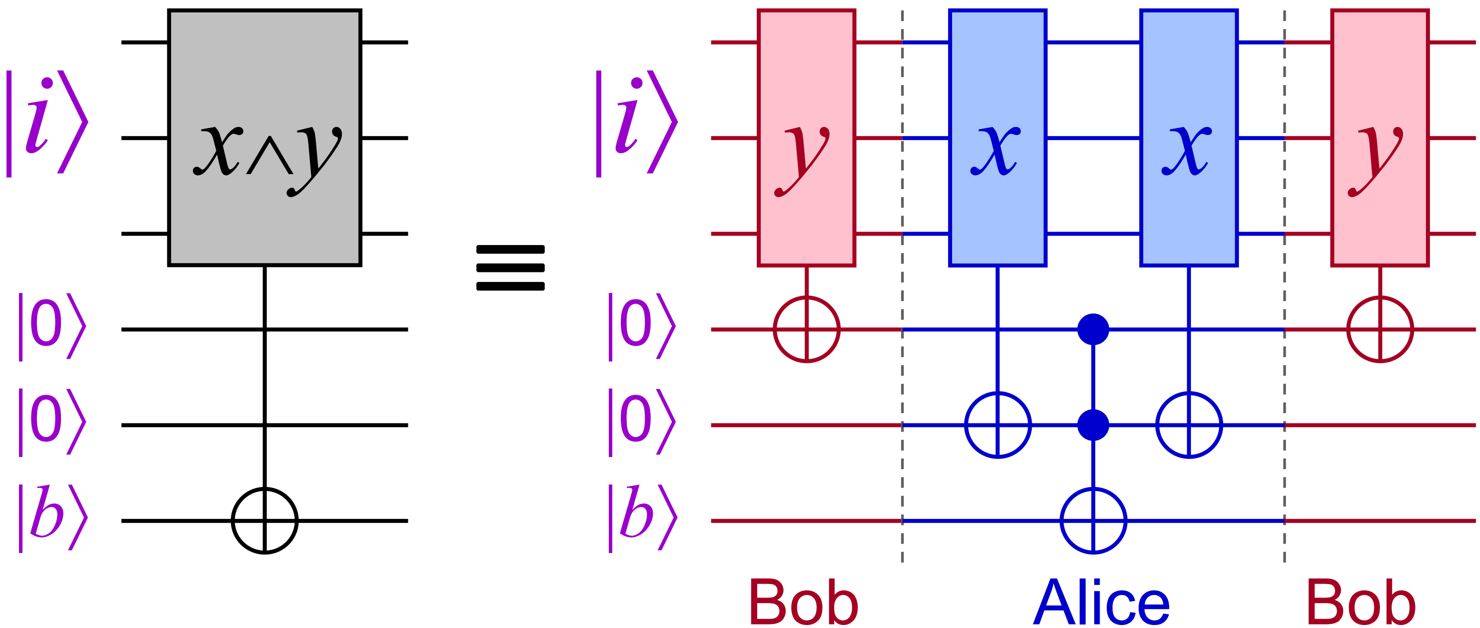
Goal: find $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$

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

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

[Grover, 1996]

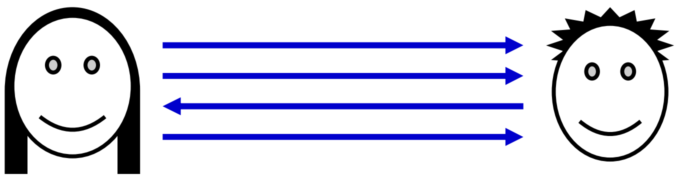
		1	2	3	4	5	6	...	n
Alice	$x =$	0	1	1	0	1	0	...	0
Bob	$y =$	1	0	0	1	1	0	...	1
	$x \wedge y =$	0	0	0	0	1	0	...	0



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

Appointment scheduling: epilogue

Bit communication:

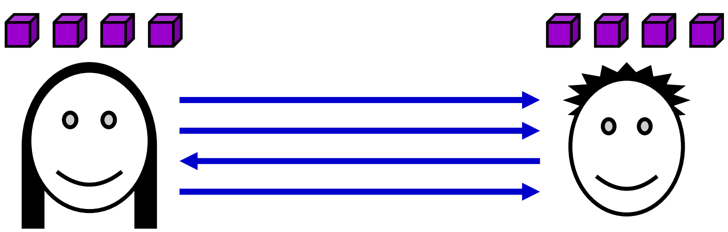


Cost: $\theta(n)$

Qubit communication:

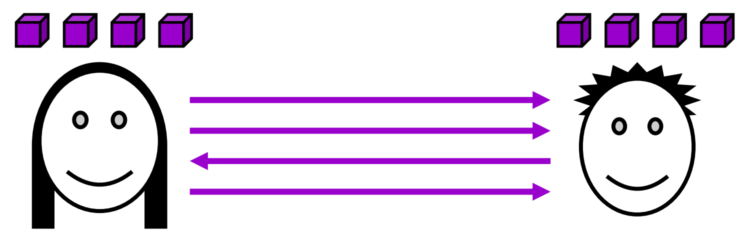
Cost: $\theta(n^{1/2})$ (with refinements)

Bit communication & prior entanglement:



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

Qubit communication & prior entanglement:



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

[R ‘02] [AA ‘03]

- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and 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
- approximately $2^n/\sqrt{n}$ input pairs (x, x), where $\Delta(x) = n/2$

Therefore, $2^n/2^k\sqrt{n}$ 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?

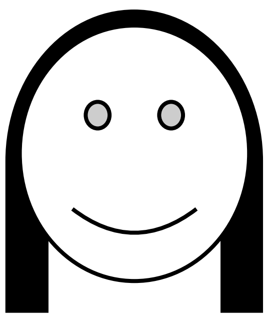
Answer: just 2 bits are sufficient!

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

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

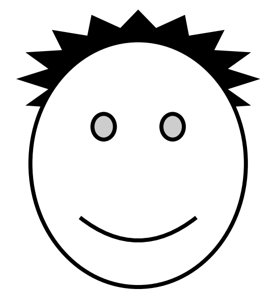
$|\psi\rangle$: a $\log(n)$-qubit state (described ***classically***)

$\boldsymbol{M}$: two-outcome measurement



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

$\boldsymbol{U}$: unitary operation on $\log(n)$ qubits



[Raz, 1999]

- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and 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

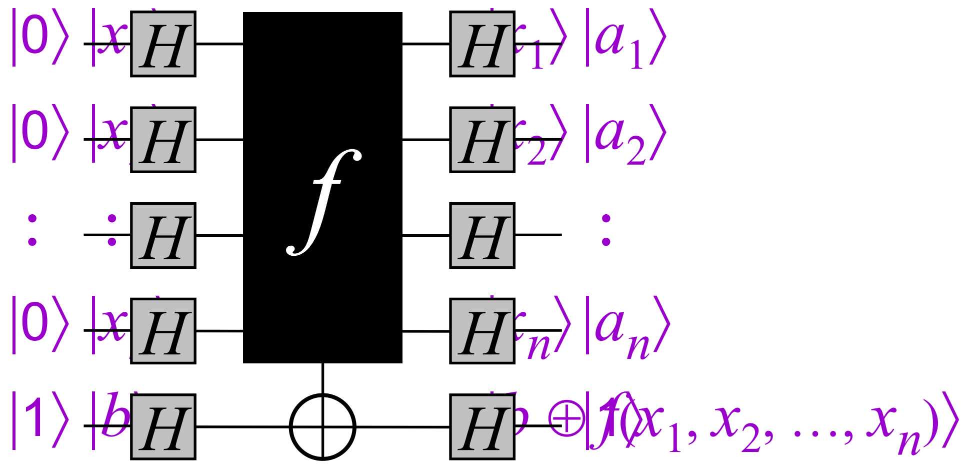
Quantum protocols ***also*** require $\Omega(n)$ communication

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

Recall the BV 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 $a_1, a_2, \ldots, a_n$

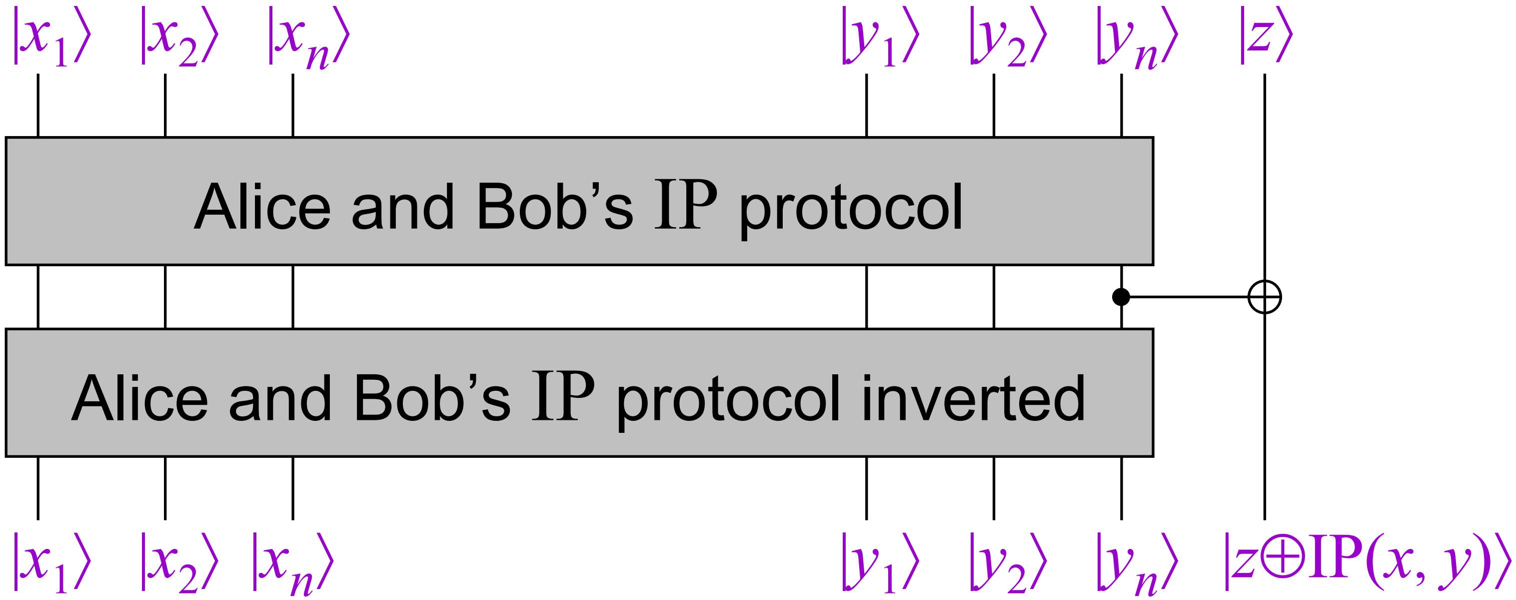
Classically, n queries are necessary

Quantum mechanically, 1 query is sufficient

Lower bound for inner product

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

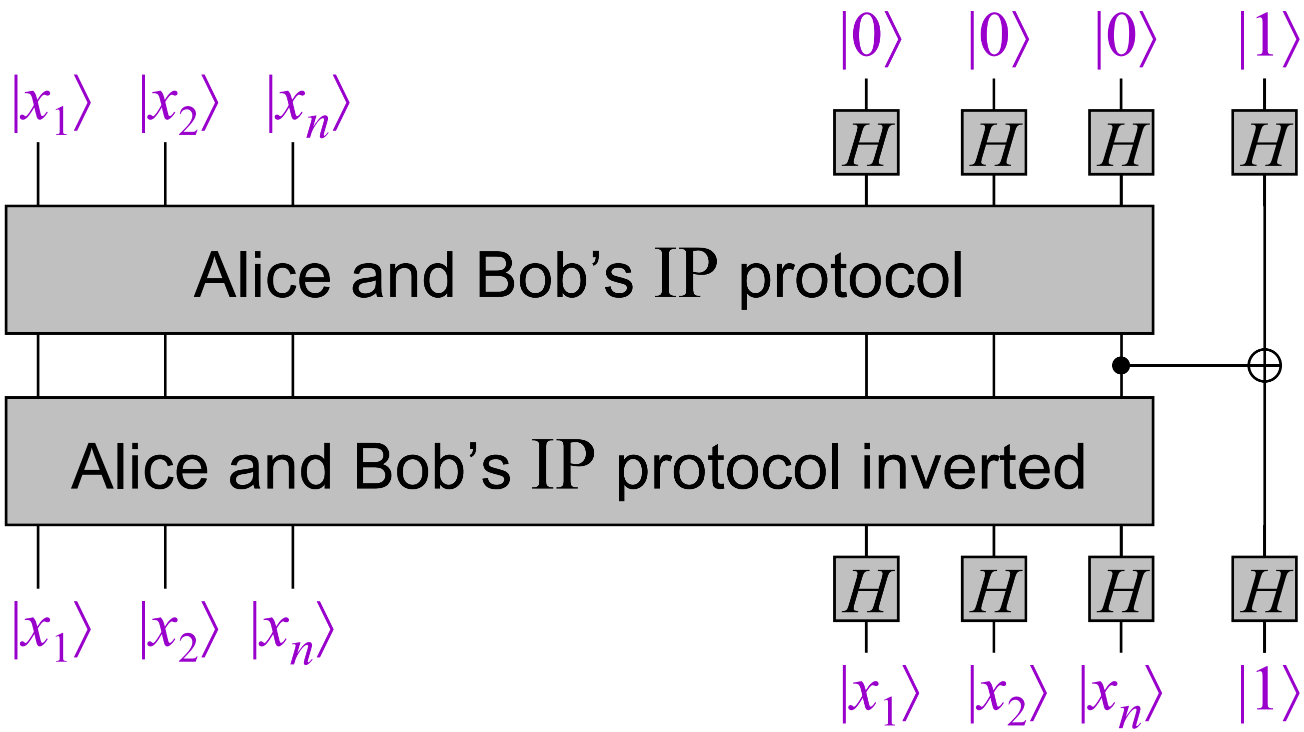
Proof:



Lower bound for inner product

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

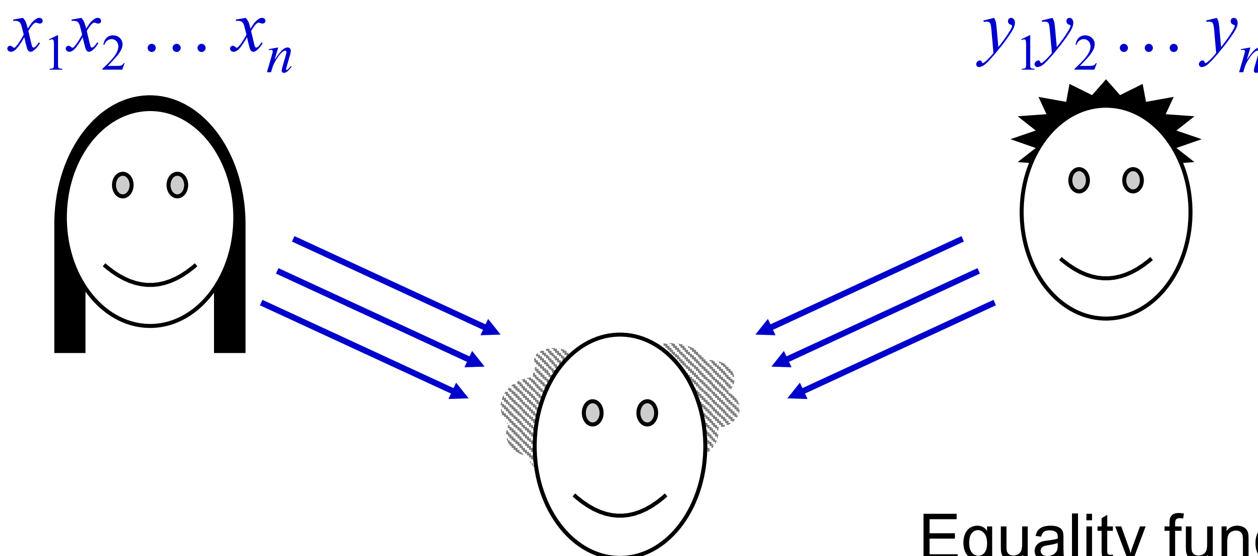
Proof:



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

- The Bell inequality and its violation
  - Physicist's perspective
  - Computer Scientist's perspective
- The magic square game
- Communication complexity
  - Equality checking
  - Appointment scheduling (quadratic savings)
  - Are exponential savings possible?
  - Lower bound for the inner product problem
- Simultaneous message passing and fingerprinting

Equality revisited
in simultaneous message model



$f(x,y)$

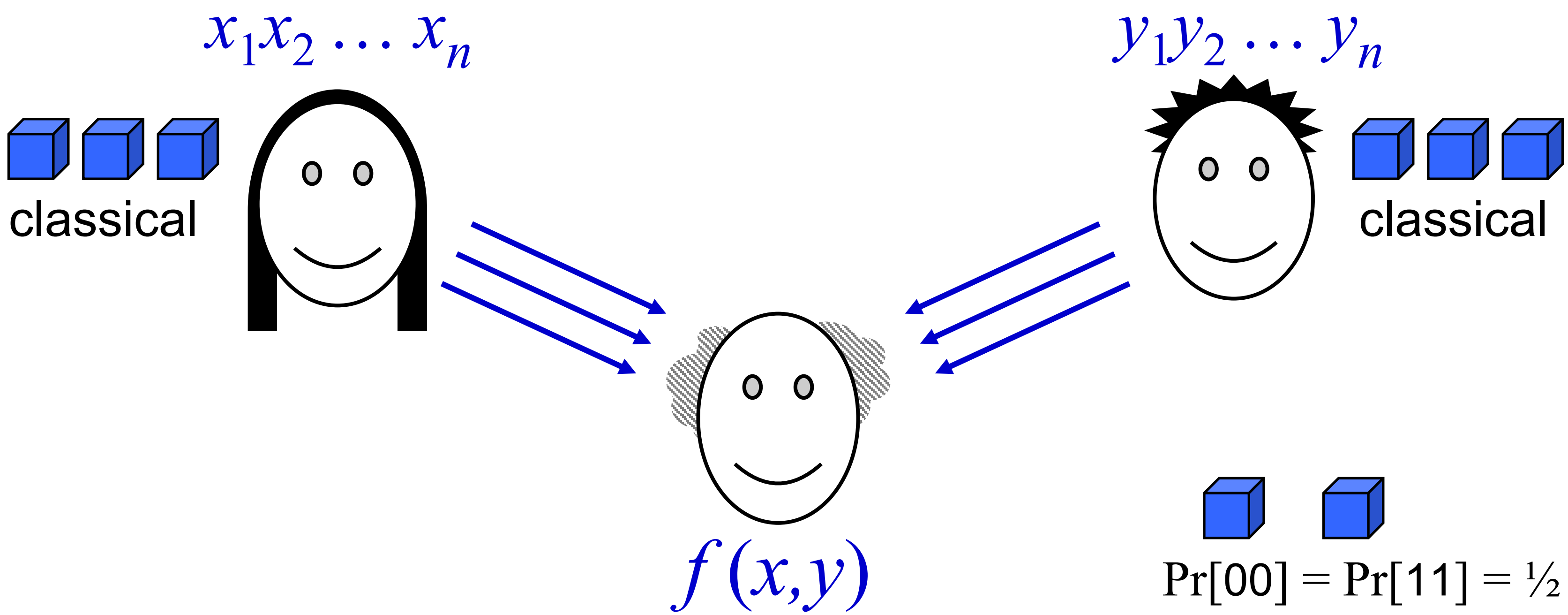
Equality function:

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

Exact protocols: require $2n$ bits communication

Equality revisited

in simultaneous message model



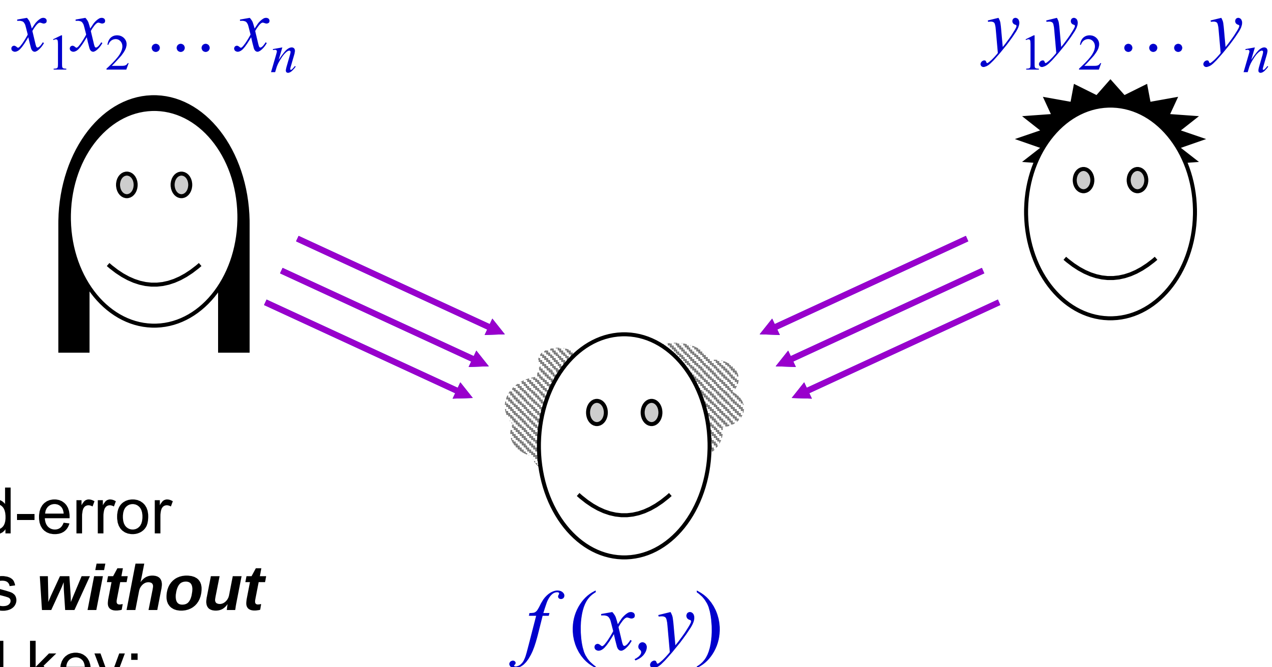
Bounded-error protocols with a shared random key:
require only $O(1)$ bits communication

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



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 $a > 0$

The states can be constructed via 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 $|\langle \psi_x | \psi_y \rangle| \leq 1 - 2d$

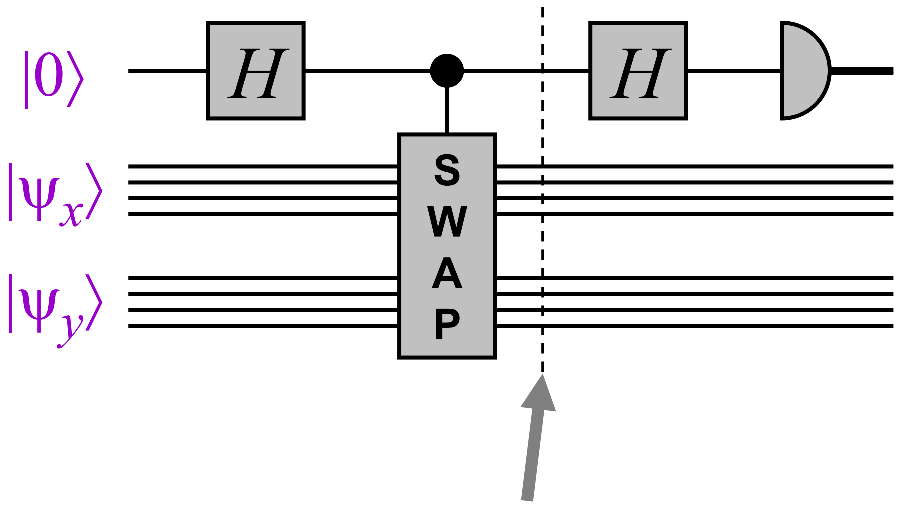
By duplicating each state, $|\psi_x\rangle \otimes |\psi_x\rangle \otimes \ldots \otimes |\psi_x\rangle$, the pairwise inner products can be made arbitrarily small: $(1-2d)^r \leq \varepsilon$

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

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:



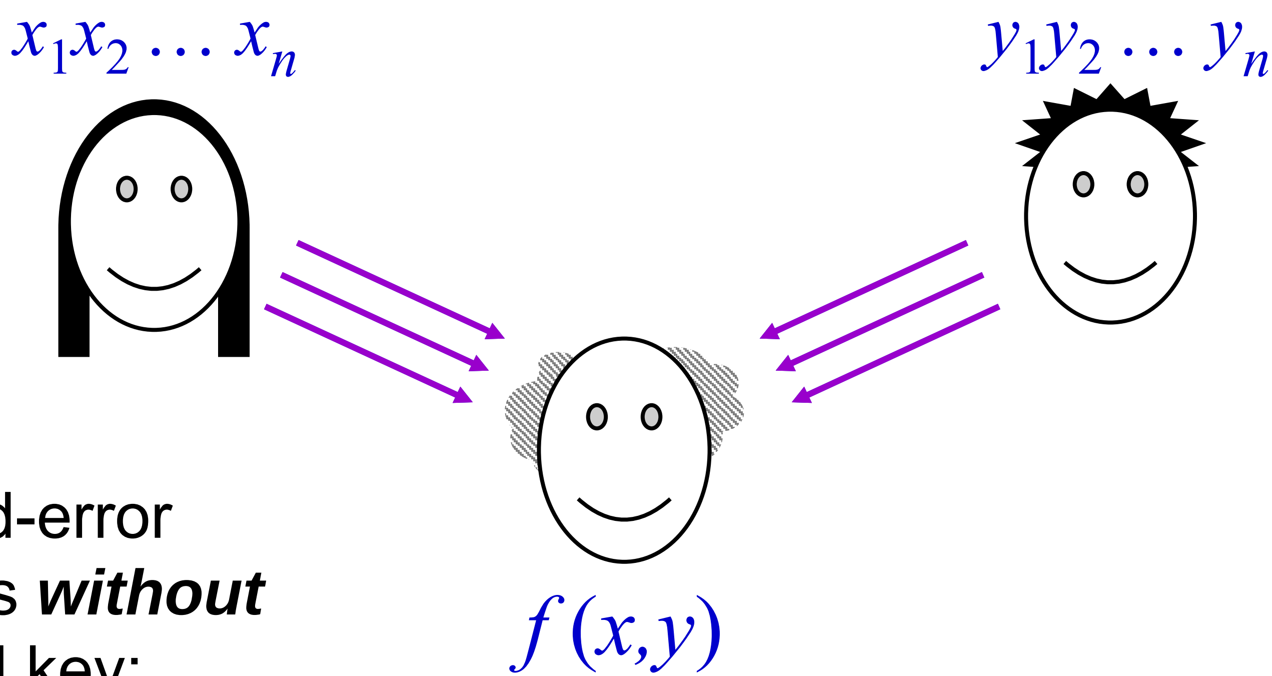
if $x = y$, Pr[output = 0] = 1

if $x \neq y$, Pr[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



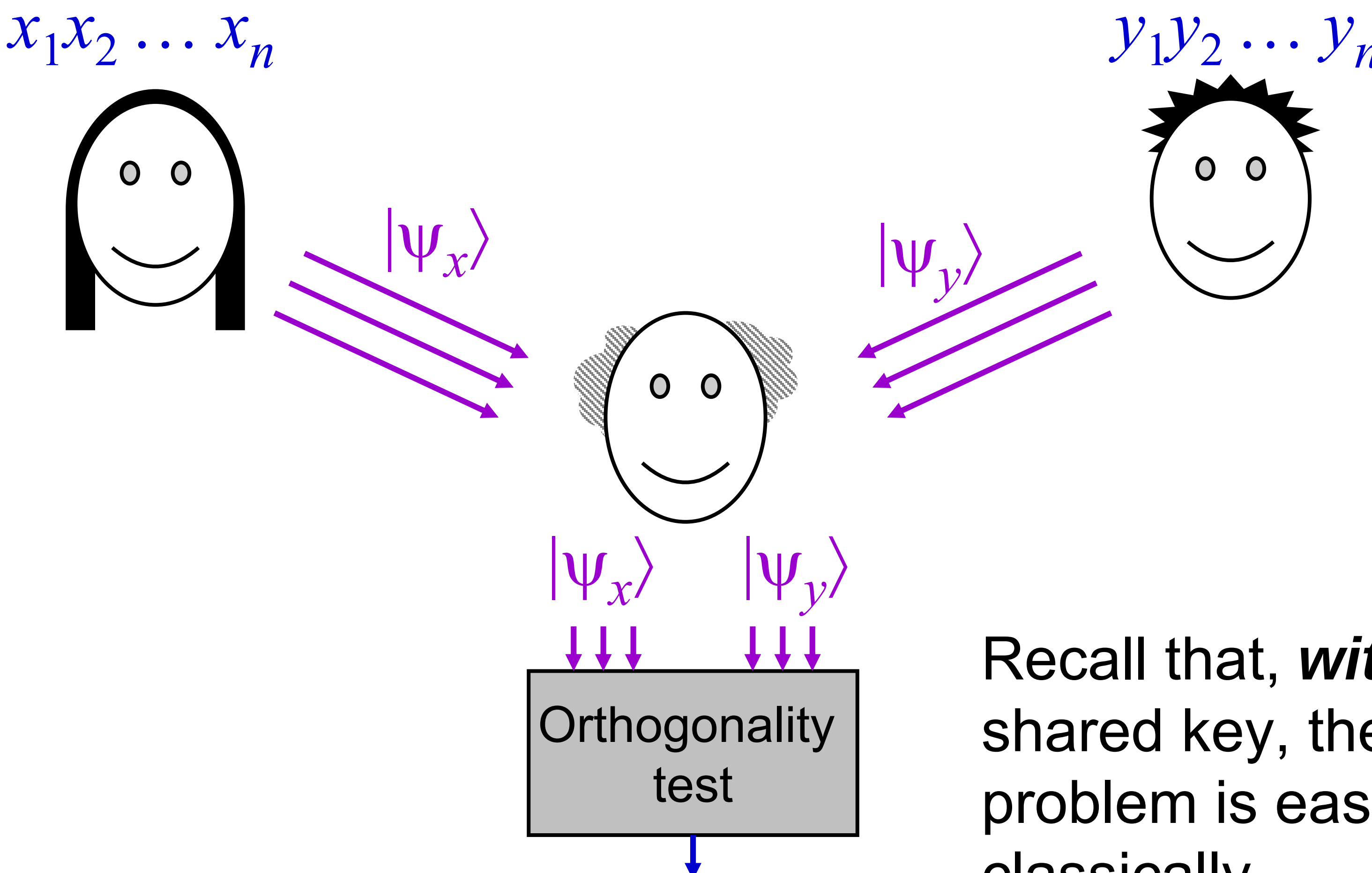
Bounded-error protocols ***without*** a shared key:

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 ...

THE END