Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 22-23 (2019)

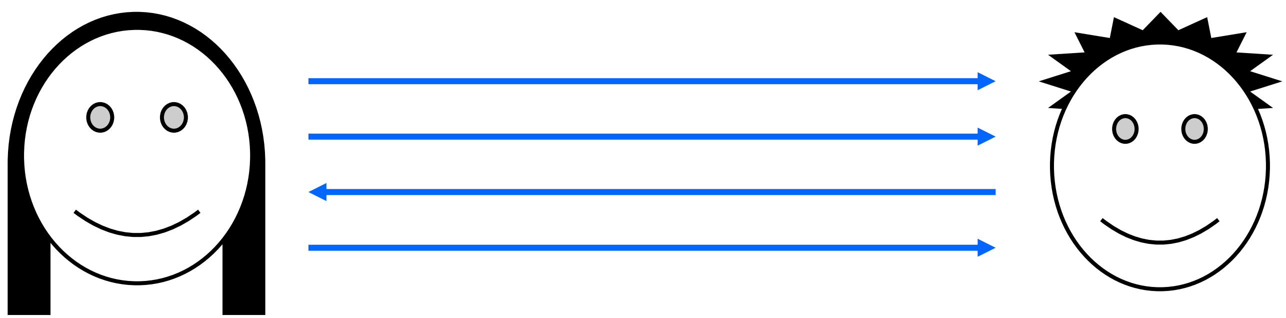
Richard Cleve
QNC 3129
cleve@uwaterloo.ca

Communication complexity

Classical communication complexity

[Yao, 1979]

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



$f(x,y)$

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?

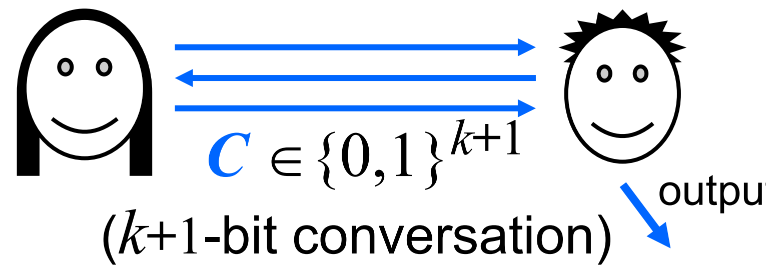
Deterministic cost is n bits (I)

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

	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*** (including output)



Several inputs may lead to the same conversation ...

Definition: A (combinatorial) ***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

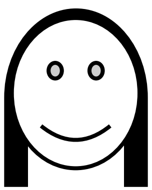
Start with a "good" classical error-correcting code, which is a function $e: \{0,1\}^n \to \{0,1\}^{cn}$ such that, for all $x \neq y$,

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

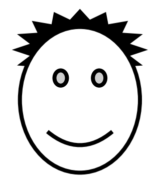
(Δ means Hamming distance),

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

$e(x) =$ 1 0 1 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1

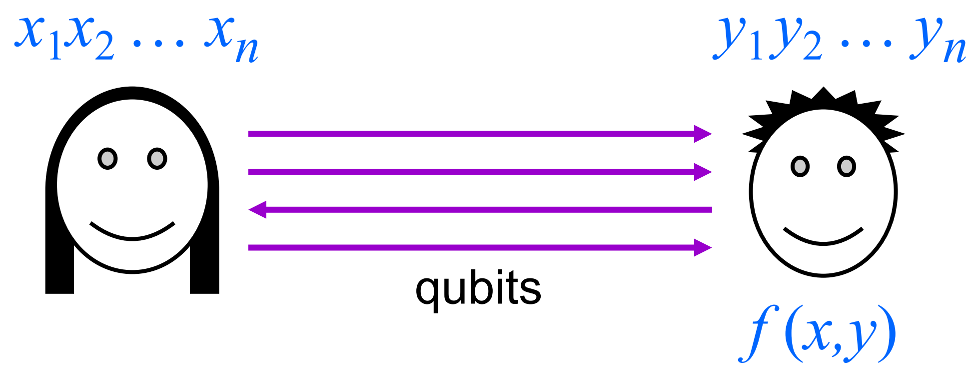
$e(y) =$ 0 1 1 0 1 0 1 1 0 0 1 1 0 0 1 0 1 0

random $\boldsymbol{k}$

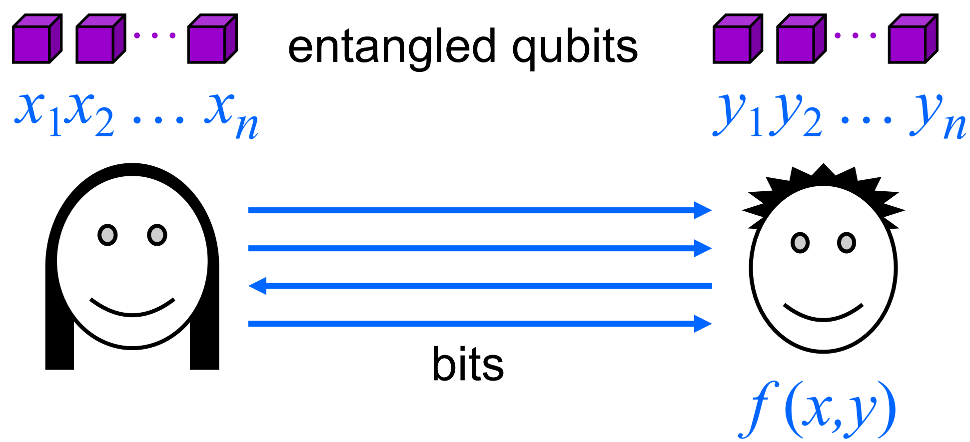
Can repeat to reduce error

Quantum communication complexity

Qubit communication



Prior entanglement



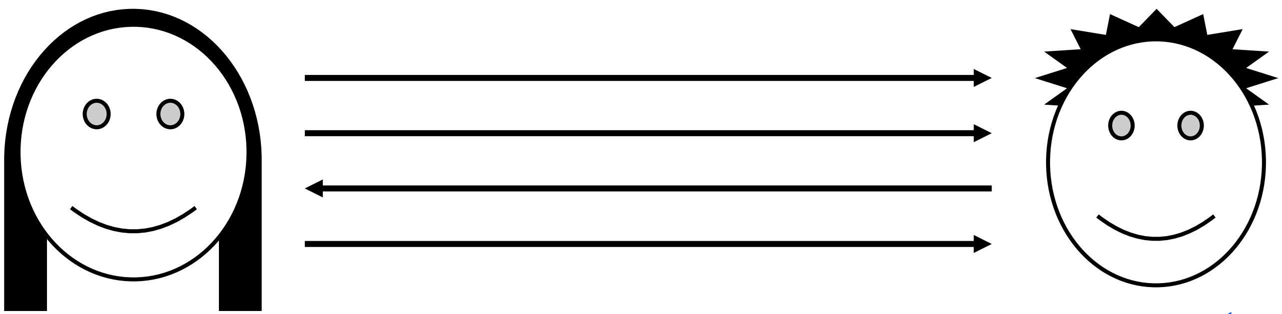
Question: can quantum beat classical in either of these this contexts?

Appointment scheduling

(also known as the ***Disjointness Problem***)

1 2 3 4 5 . . . n 1 2 3 4 5 . . . n

$x =$ 0 1 1 0 1 … 0 $y =$ 1 0 0 1 1 … 1



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

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

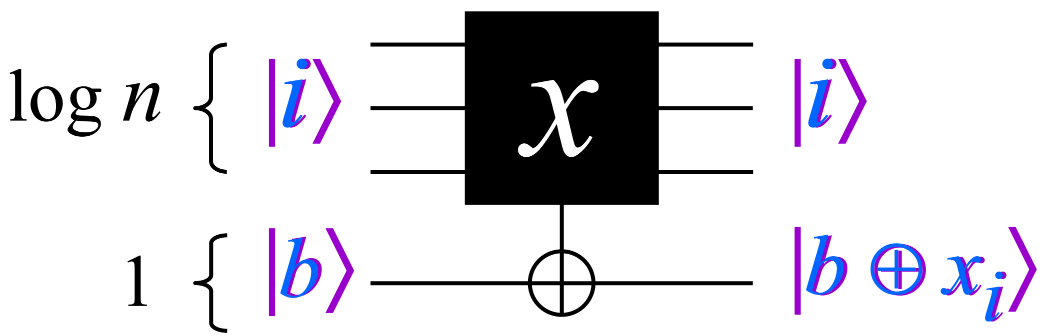
For all $\varepsilon > 0$, $O(n^{1/2} \log n)$ **qubits** sufficient for error prob. < ε

[KS '87] [BCW '98]

Search problem

1 2 3 4 5 6 . . . n

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



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

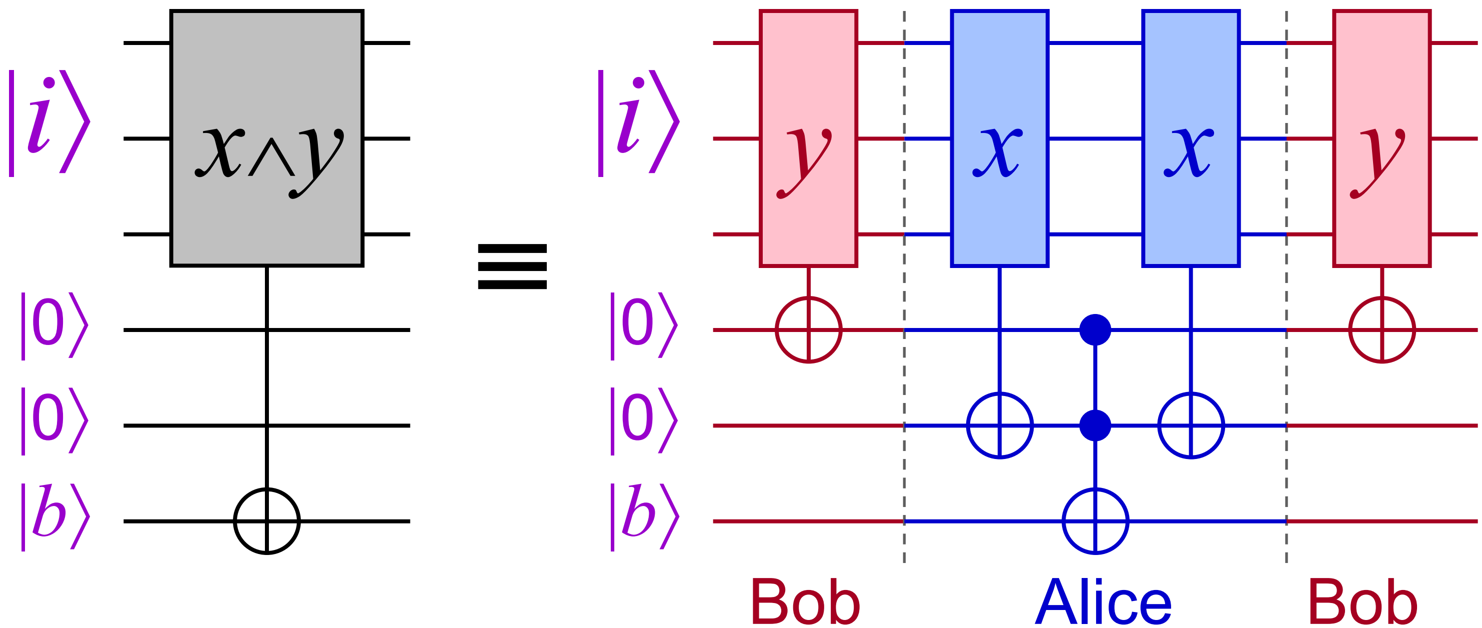
Classically: $\Omega(n)$ queries are necessary

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

(bitwise AND of x and y)



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

Appointment scheduling: epilogue

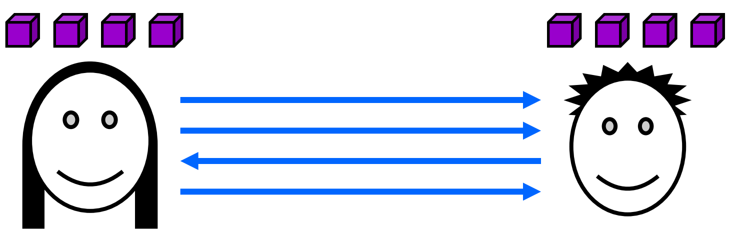
Bit communication:

Cost: $\theta(n)$

Qubit communication:

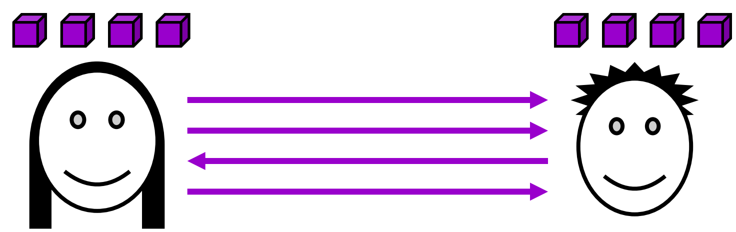
Cost: $\theta(n^{1/2})$ (with refinements)

Bit communication & prior entanglement:



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

Qubit communication & prior entanglement:

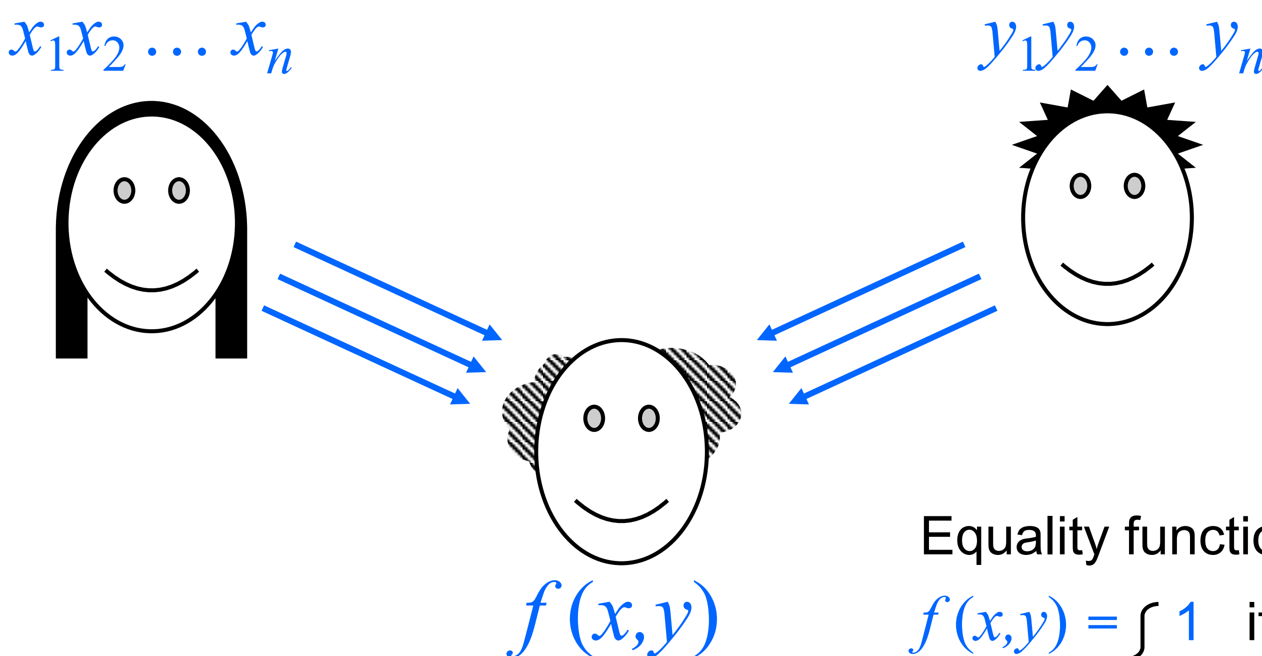


Cost: $\theta(n^{1/2})$

[R ‘02] [AA ‘03]

Quantum fingerprinting

Equality revisited
in simultaneous message model

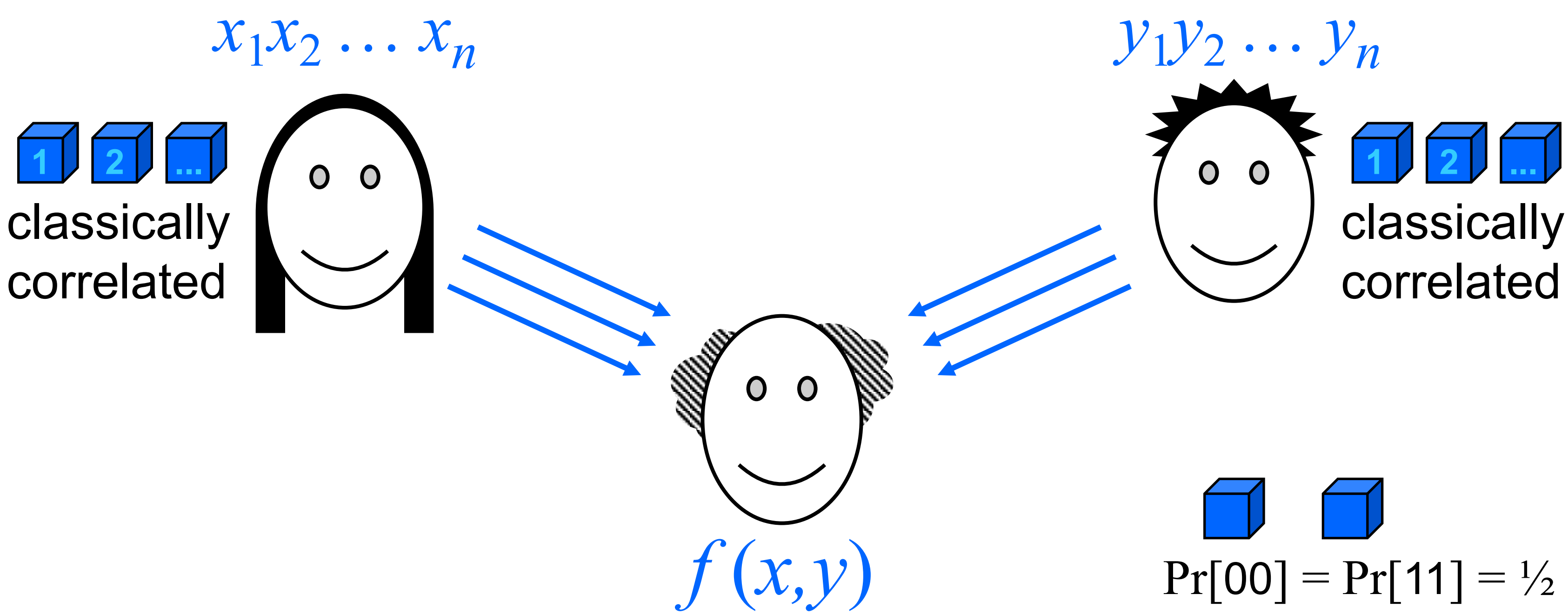


Equality function:

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

Exact protocols: require $2n$ bits communication

Equality revisited
in simultaneous message model

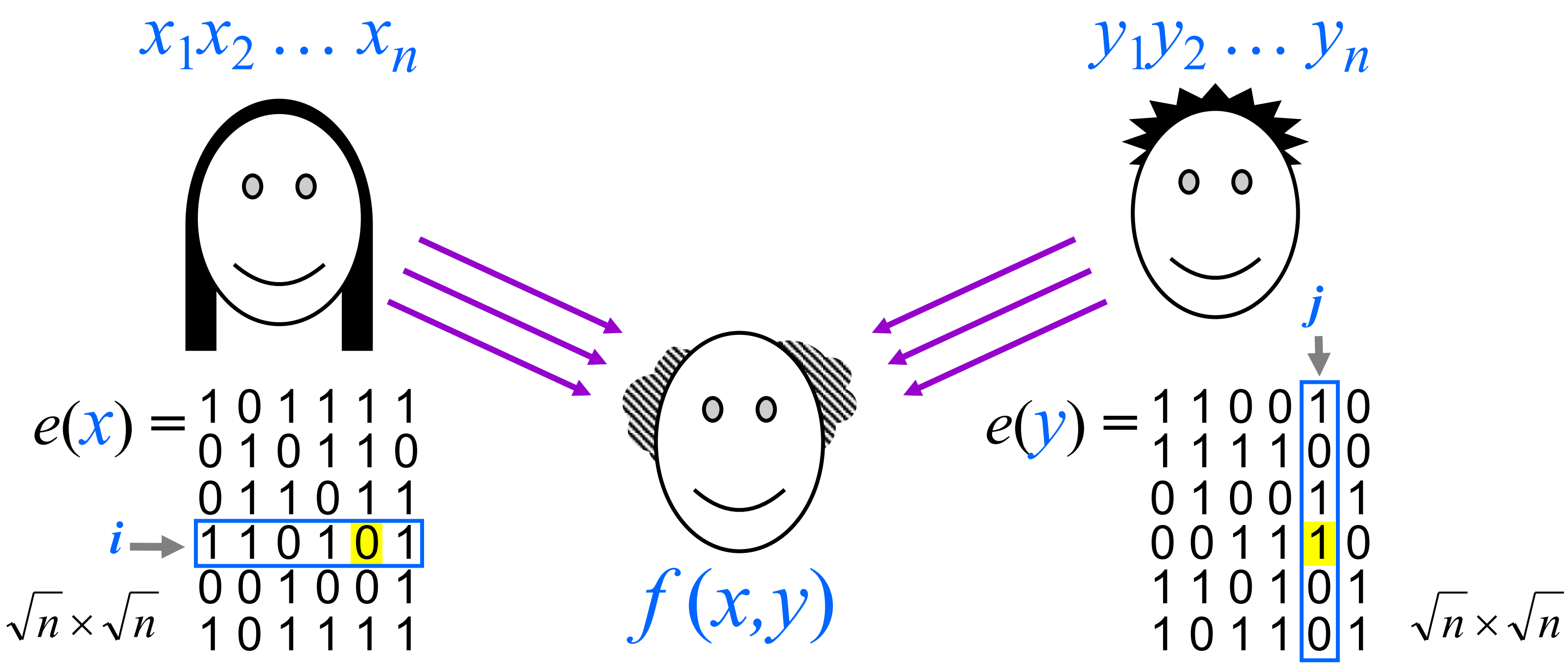


Bounded-error protocols with a shared random key: require only $O(1)$ bits communication

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 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 $|\langle\psi_x|\psi_y\rangle| \le \varepsilon$)

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 $x \neq y$,

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

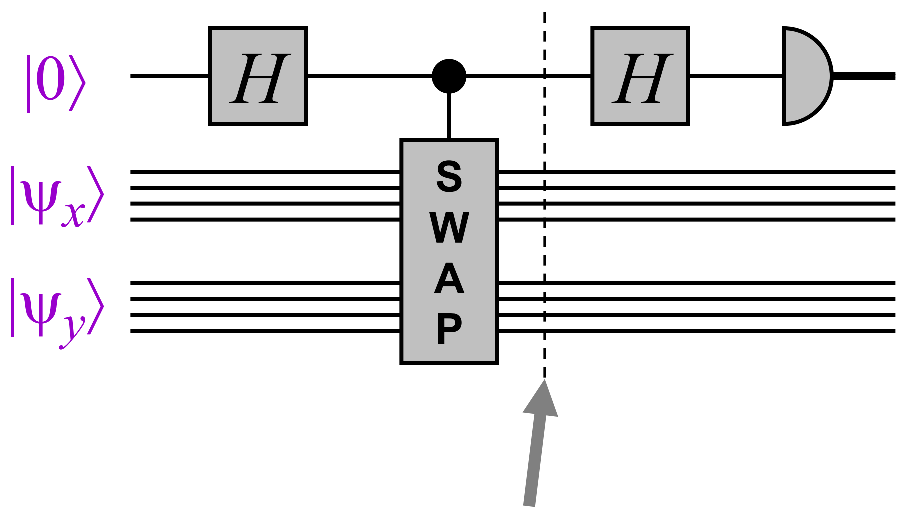
- they're both the same state
- they're almost orthogonal

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 $|\langle\psi_x|\psi_y\rangle| \le \varepsilon$ for all $x \neq y$

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



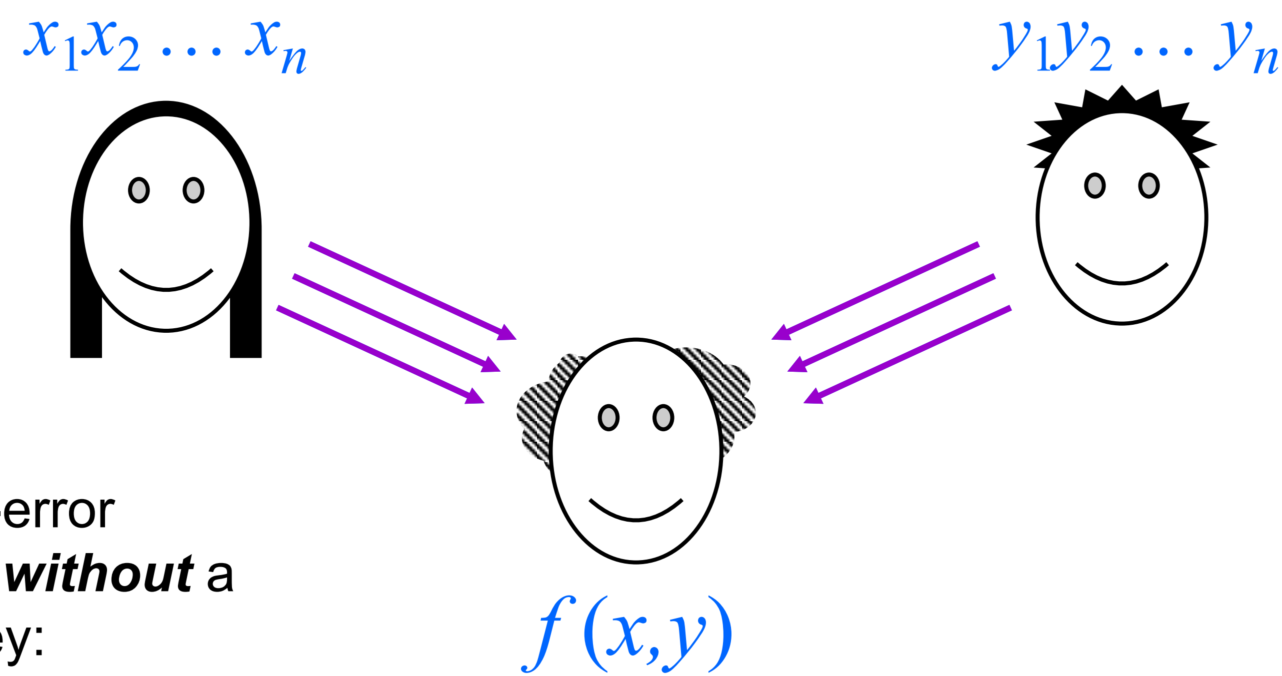
if $x = y$, $\Pr[\text{output} = 0] = 1$

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



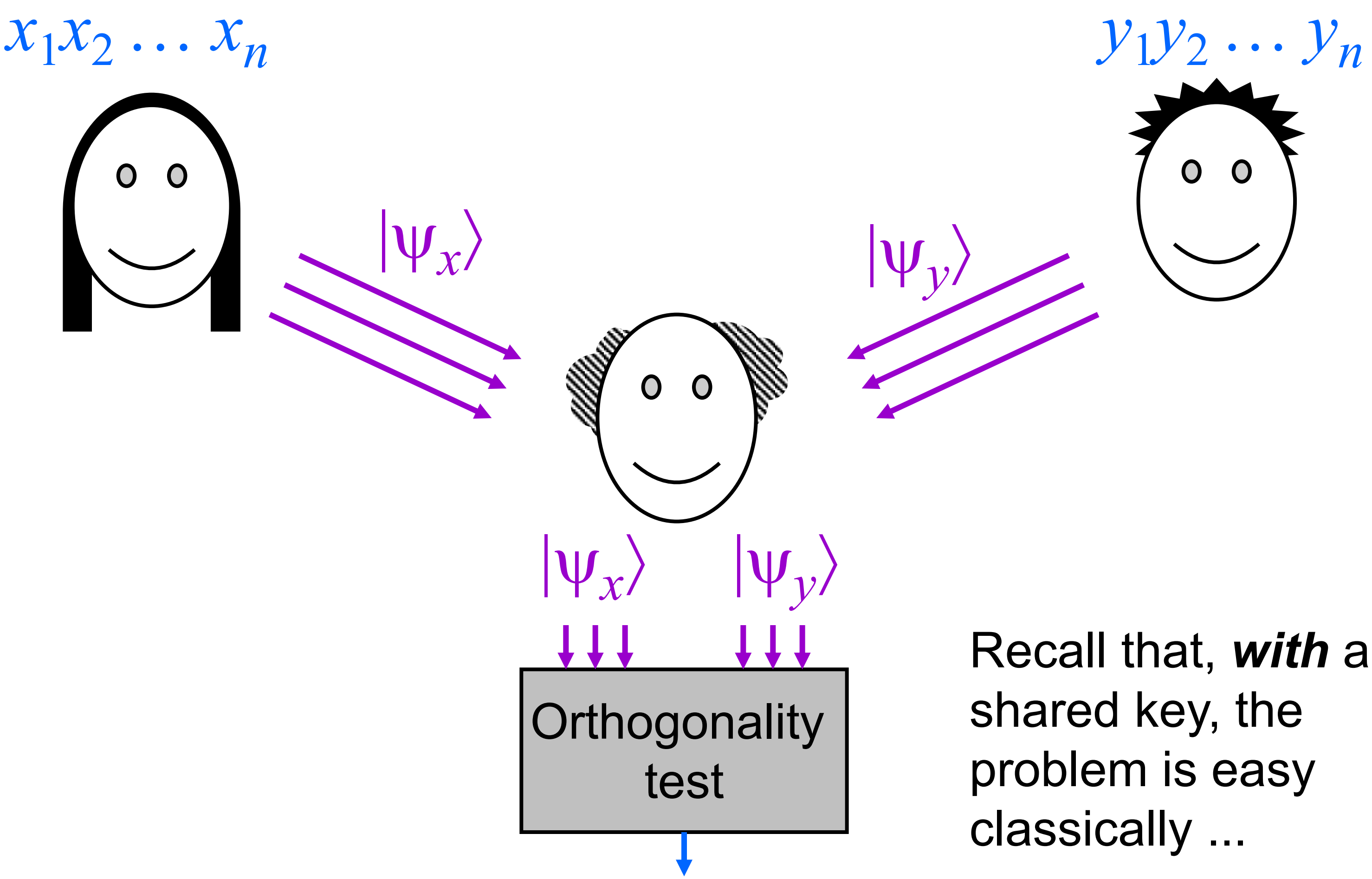
Bounded-error protocols ***without*** a shared key:

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

Quantum: $\theta(\log n)$

[A ‘96] [NS ‘96] [BCWW ‘01]

Quantum protocol for equality
in simultaneous message model

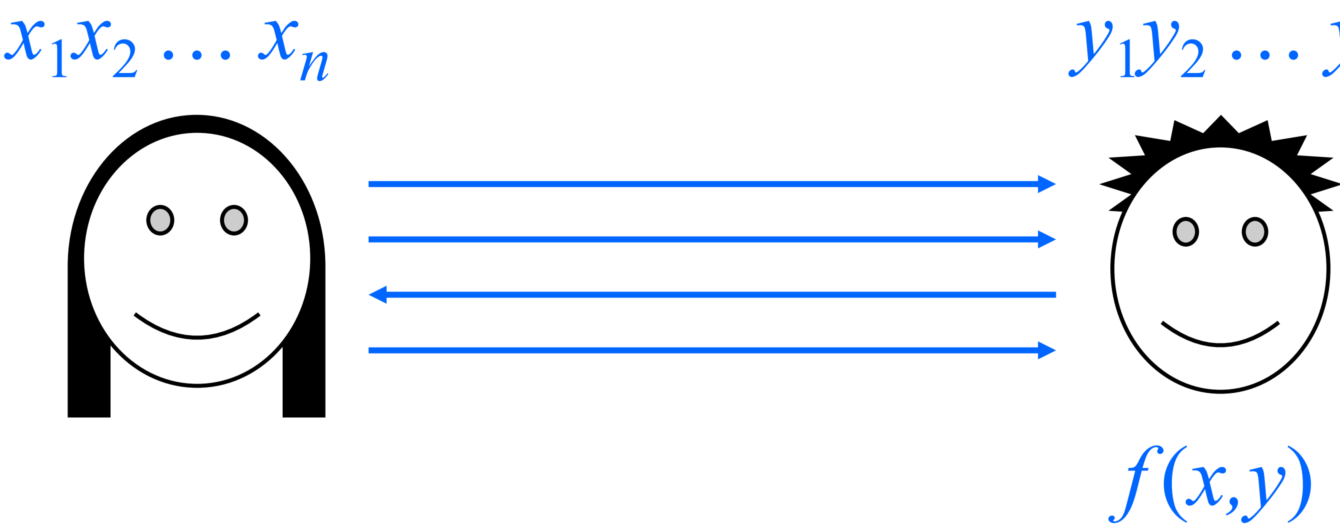


Recall that, ***with*** a shared key, the problem is easy classically ...

This quantum protocol only requires $\theta(\log n)$ qubits

Inner product

Inner product function

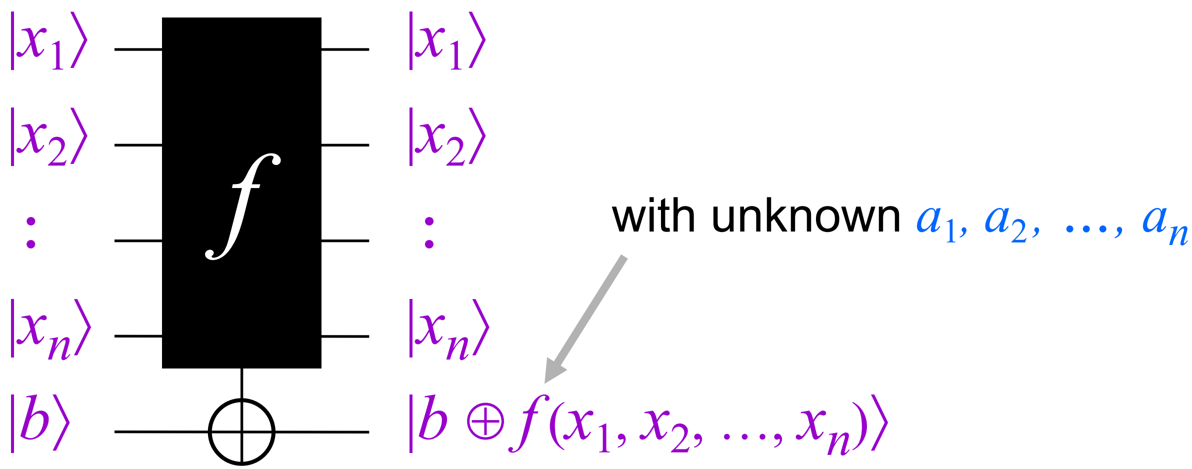


$$f(x,y) = x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \bmod 2$$

Aside: Bernstein-Vazirani problem I

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:



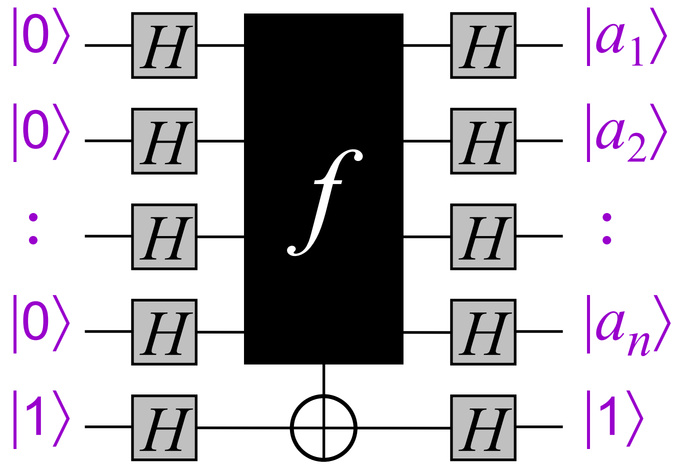
Goal: determine $a_1, a_2, \ldots, a_n$

Classically, n queries are necessary

Aside: Bernstein-Vazirani problem II

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 $a_1, a_2, \ldots, a_n$

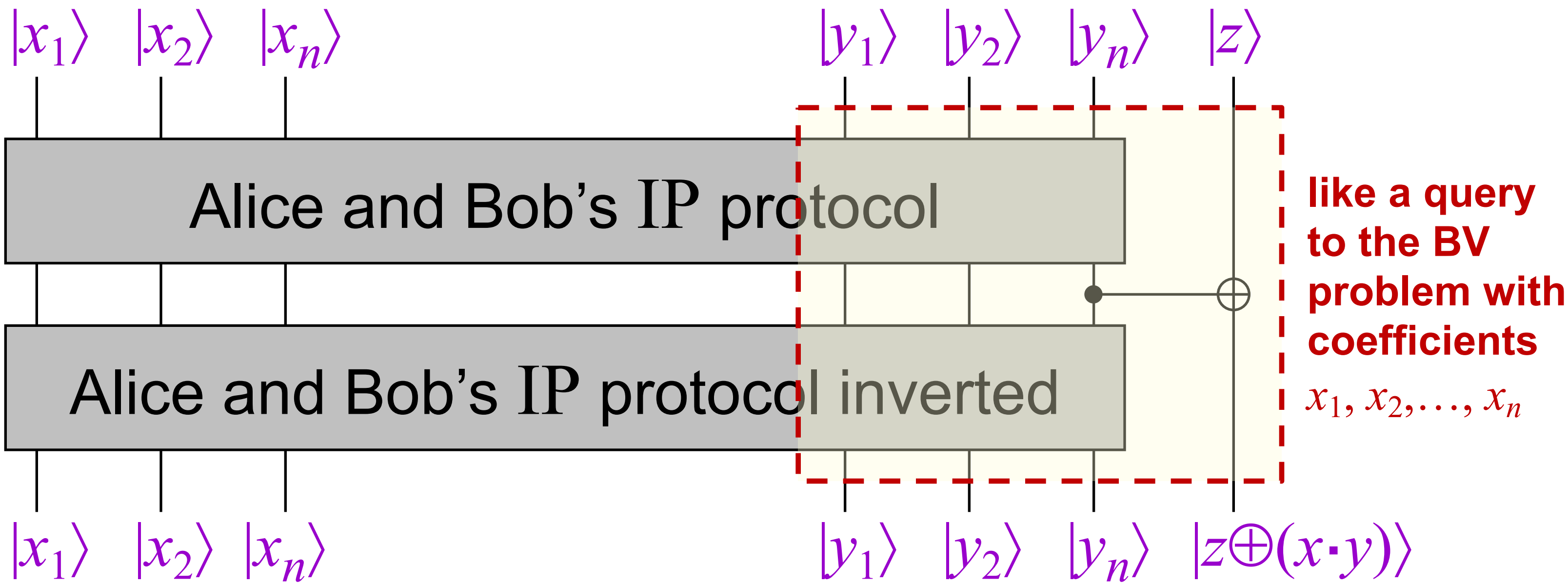
Classically, n queries are necessary

Quantum mechanically, 1 query is sufficient

Lower bound for inner product I

$$x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \bmod 2$$

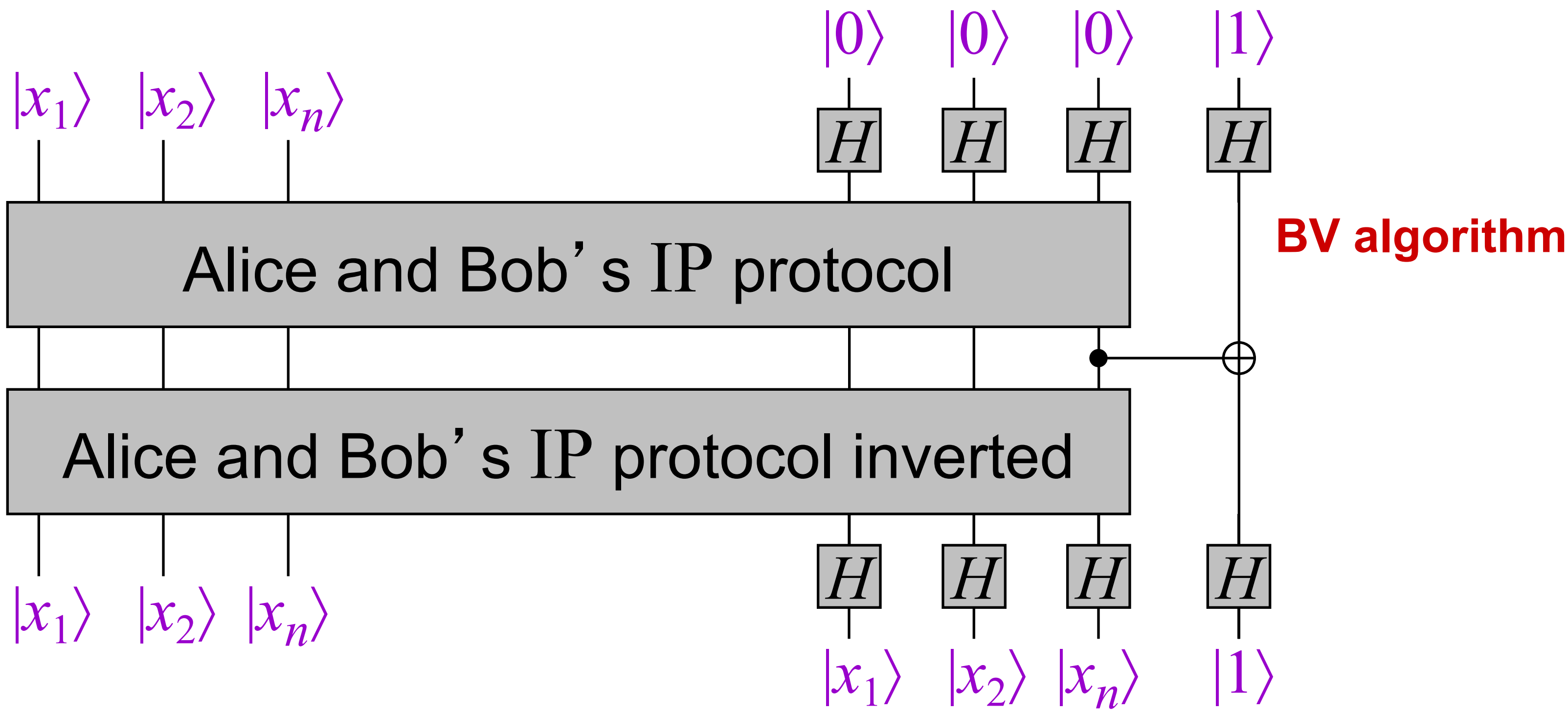
Proof:



Lower bound for inner product II

$$x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \bmod 2$$

Proof:



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