Introduction to Quantum Information Processing

Lecture 17

Richard Cleve

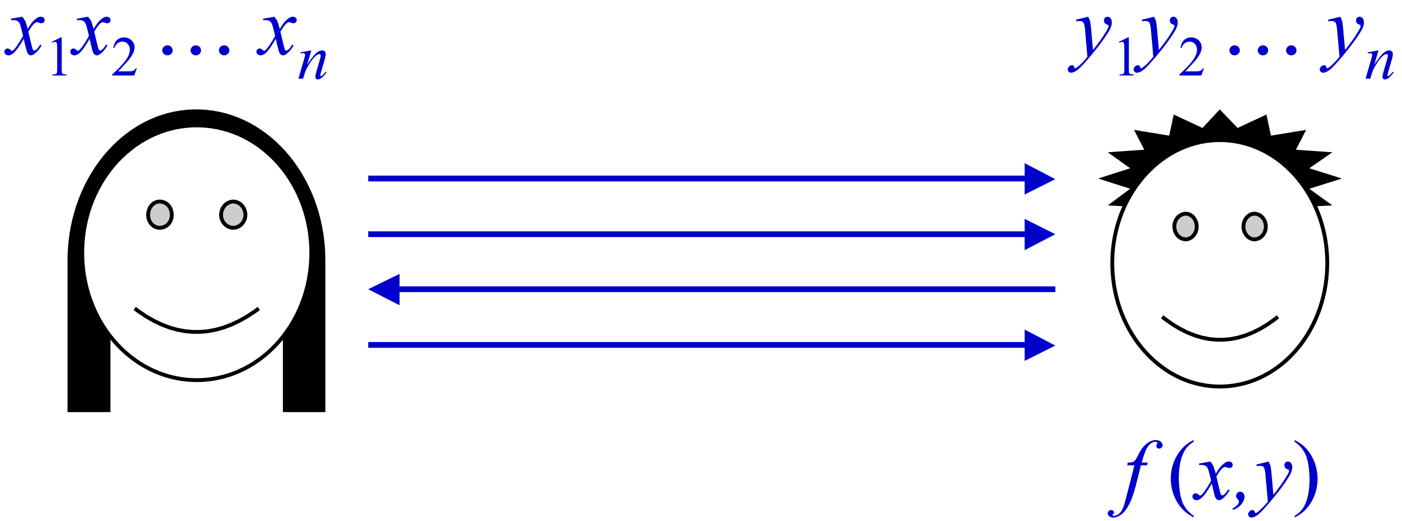
Overview of Lecture 17

- Introduction to **communication complexity**
- Intersection problem (a.k.a. appointment scheduling)
- Restricted equality problem
- Exponential separation in bounded-error setting
- Inner product problem
- Simultaneous message passing model and fingerprinting

communication complexity

Classical communication complexity

[Yao, 1979]



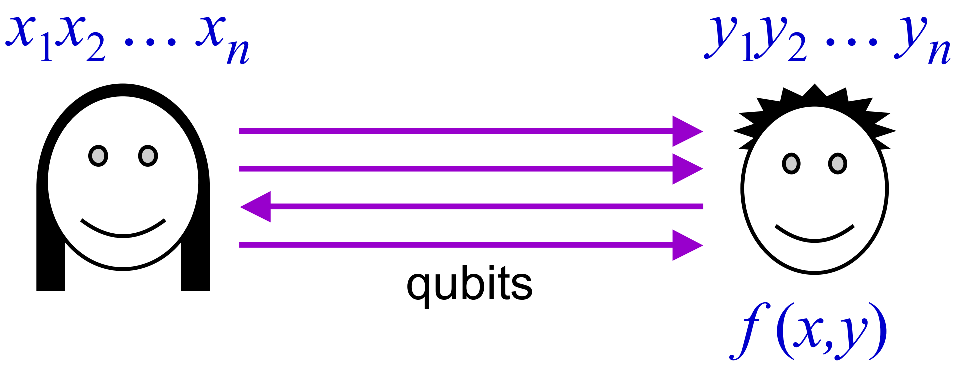
E.g. equality function: $f(x,y) = 1$ if $x = y$, and 0 if $x \neq y$

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

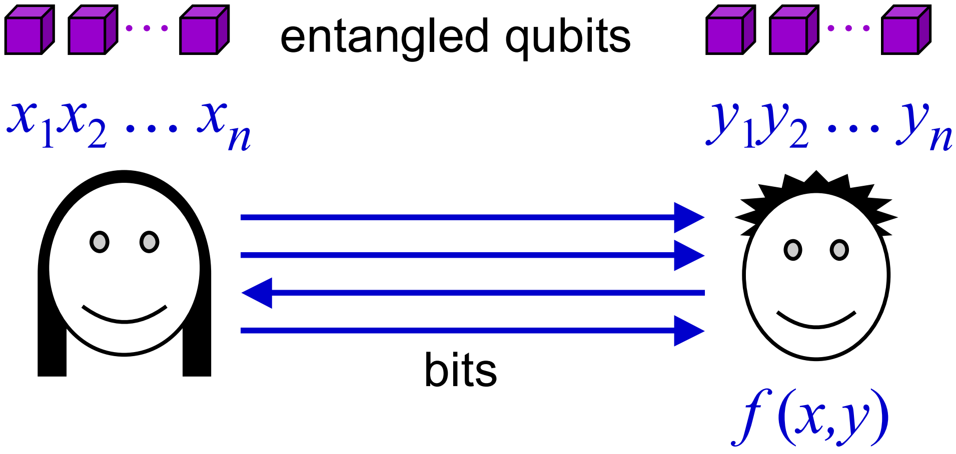
Probabilistic protocols can solve with only $O(\log(n/\varepsilon))$ bits communication (error probability ε), via random hashing

Quantum communication complexity

Qubit communication

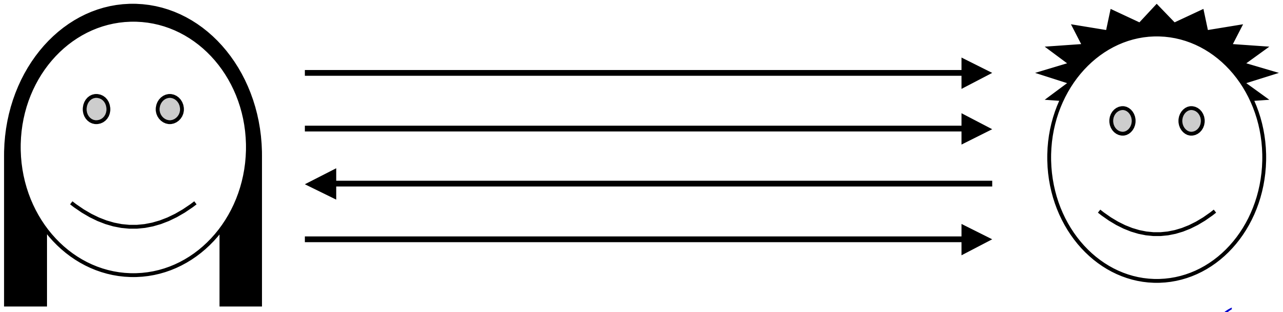


Prior entanglement



Appointment scheduling

$$x = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \end{matrix} \\ \boxed{\begin{matrix} 0 & 1 & 1 & 0 & 1 & \ldots & 0 \end{matrix}} \end{array} \qquad y = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \end{matrix} \\ \boxed{\begin{matrix} 1 & 0 & 0 & 1 & 1 & \ldots & 1 \end{matrix}} \end{array}$$



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

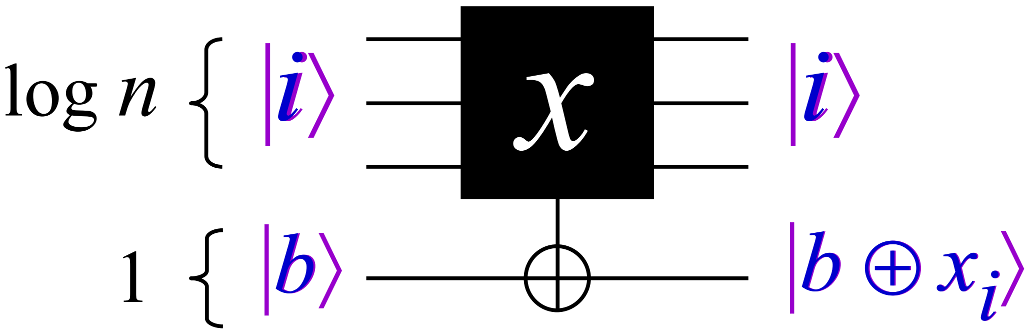
Classically, $\Omega(n)$ **bits** necessary to succeed with prob. ≥ 3/4

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

[KS ‘87] [BCW ‘98]

Search problem

Given: $x = \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \ldots & n \\ \hline \multicolumn{1}{|c}{0} & 0 & 0 & 0 & 1 & 0 & \ldots & \multicolumn{1}{c|}{1} \\ \hline \end{array}$ accessible via ***queries***



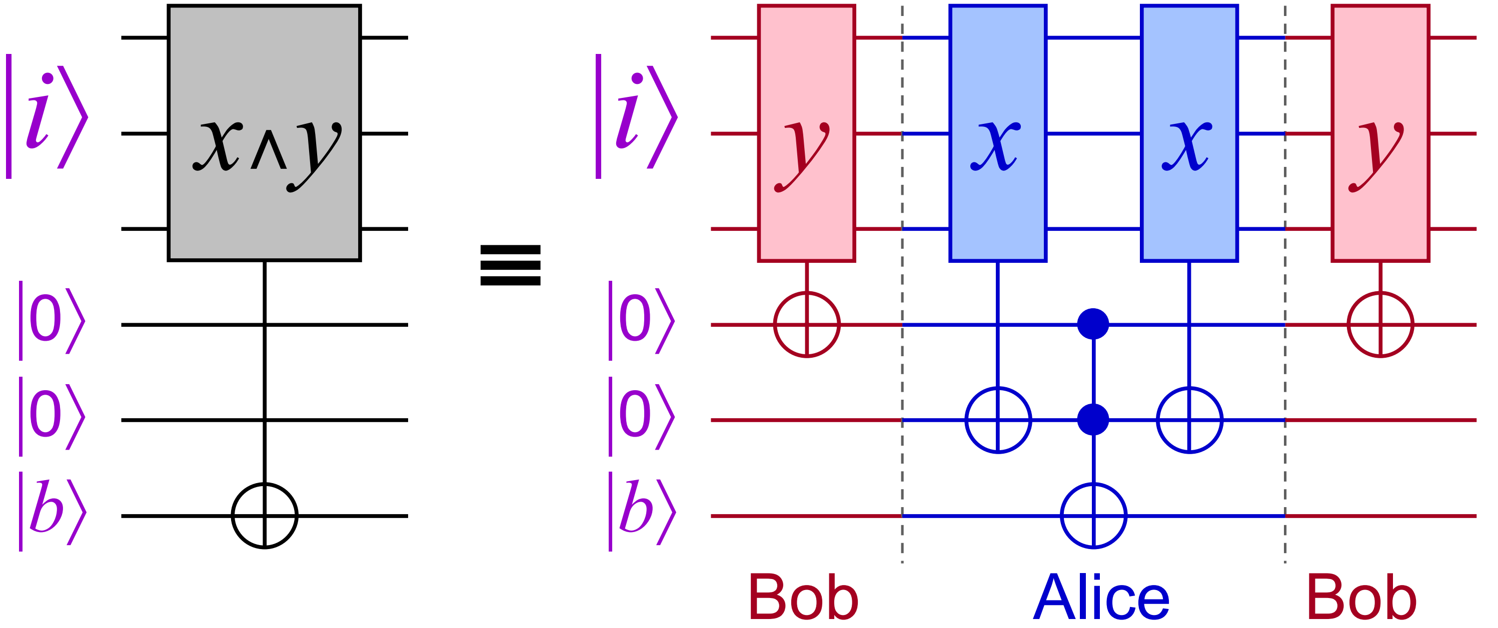
Goal: find $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$

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

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

[Grover, 1996]

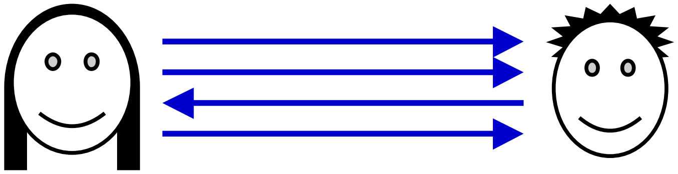
		1	2	3	4	5	6	. . .	n
Alice	$x =$	0	1	1	0	1	0	…	0
Bob	$y =$	1	0	0	1	1	0	…	1
	$x \wedge y =$	0	0	0	0	1	0	…	0



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

Appointment scheduling: epilogue

Bit communication:

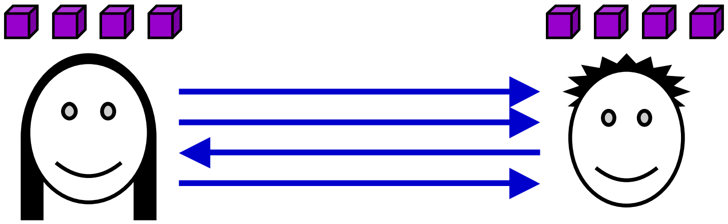


Cost: $\theta(n)$

Qubit communication:

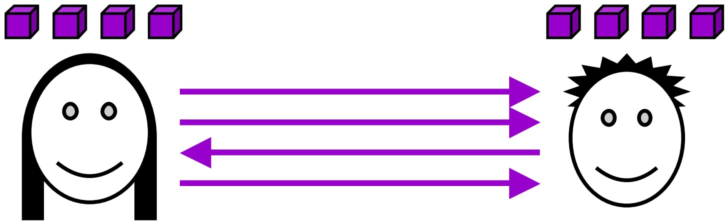
Cost: $\theta(n^{1/2})$ (with refinements)

Bit communication
& prior entanglement:



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

Qubit communication
& prior entanglement:



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

[R ‘02] [AA ‘03]

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 $2^n/\surd n$ input pairs (x, x), where $\Delta(x) = n/2$

Therefore, $2^n/2^k\surd n$ input pairs (x, x) that yield ***same*** conv. $\boldsymbol{C}$

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

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

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

Theorem implies $2^n/2^k\surd n < 1.99^n$, 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?

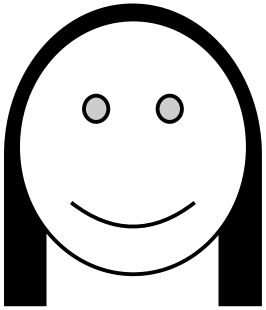
Answer: just $\mathbf{2}$ bits are sufficient!

Exponential quantum vs. classical separation in bounded-error models

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

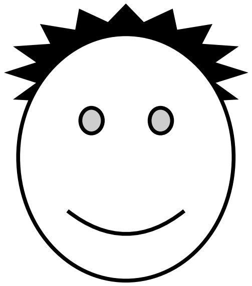
$|\psi\rangle$: a $\log(n)$-qubit state
(described ***classically***)

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



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

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



[Raz, 1999]

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

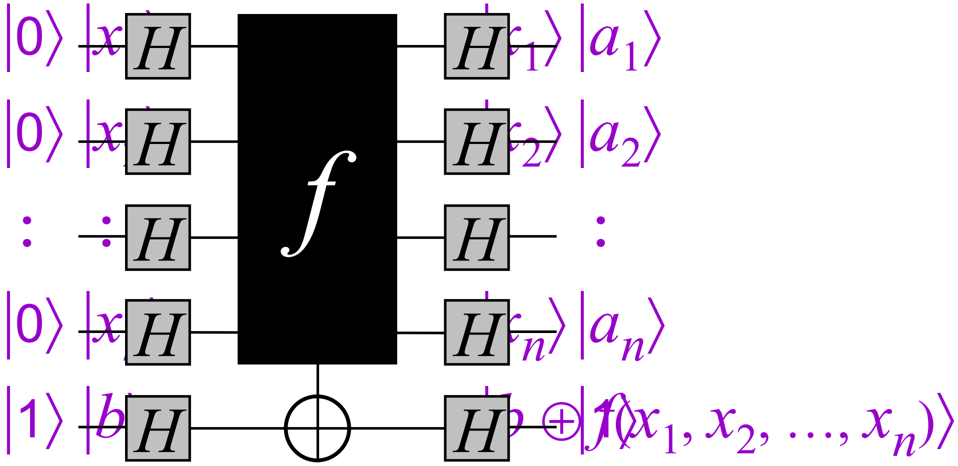
Quantum protocols ***also*** require $\Omega(n)$ communication

[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 $a_1, a_2, \ldots, a_n$

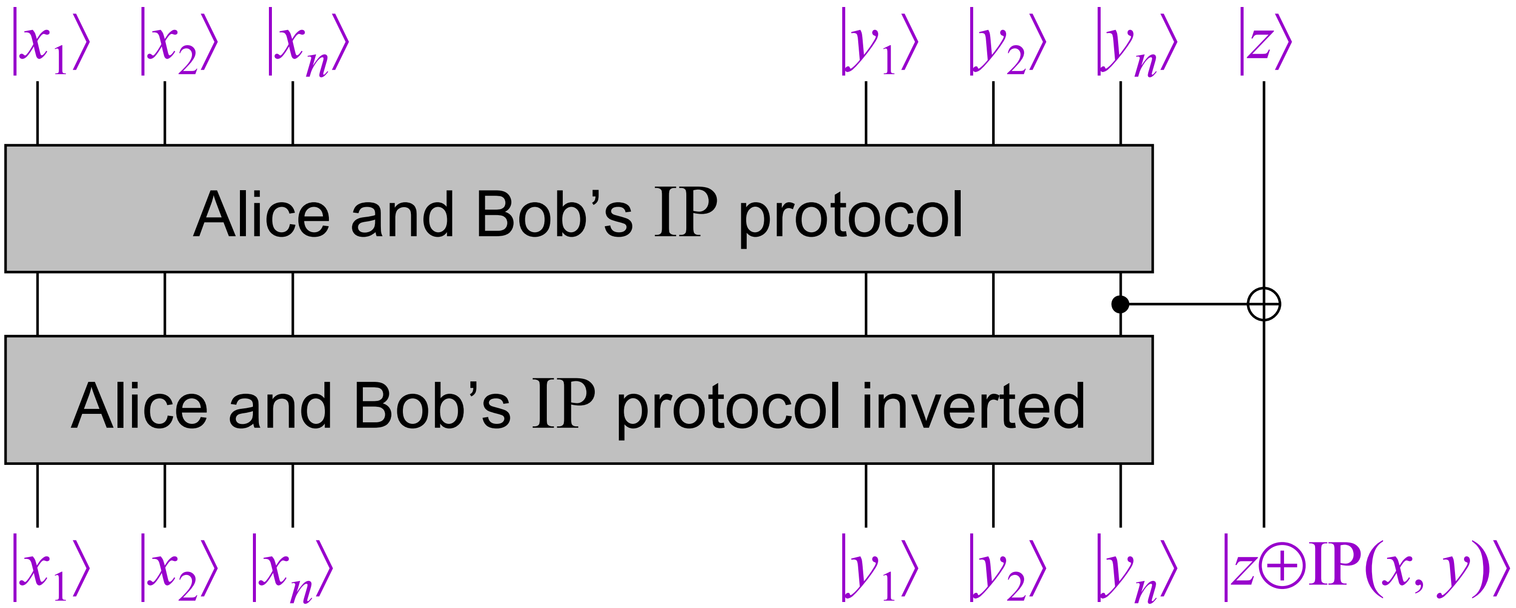
Classically, n queries are necessary

Quantum mechanically, 1 query is sufficient

Lower bound for inner product

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

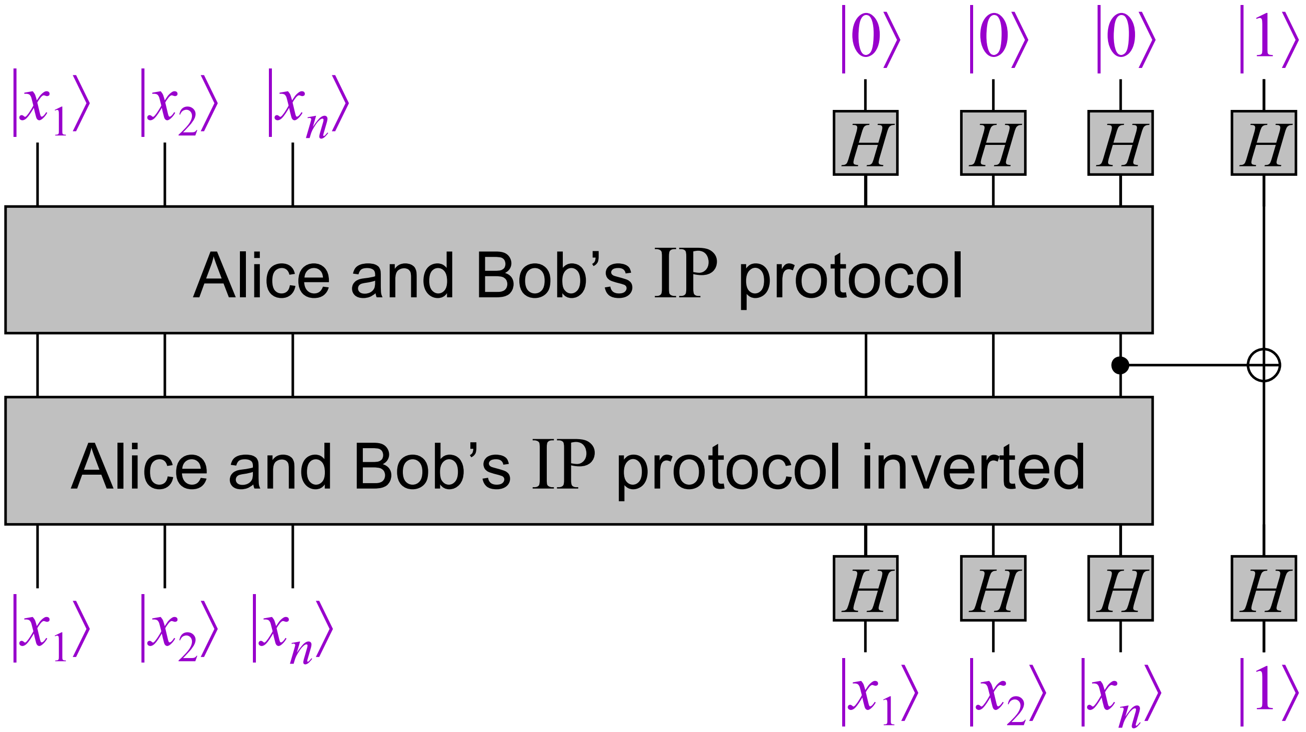
Proof:



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 END