Introduction to Quantum Information Processing

CS 667 / Phys 767 / C&O 681

Lecture 15 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

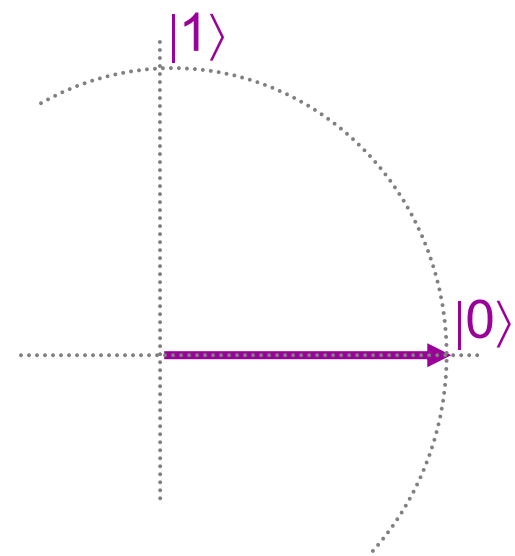
Continuous-time evolution

Continuous-time evolution

Although we've expressed quantum operations in discrete terms, in real physical systems, the evolution is continuous

Let H be any ***Hermitian*** matrix and $t \in \mathbf{R}$

Then e^{iHt} is ***unitary*** – why?



$H = U^{\dagger} D U$, where $D = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{bmatrix}$

Therefore $e^{iHt} = U^{\dagger} e^{iDt} U = U^{\dagger} \begin{bmatrix} e^{i\lambda_1 t} & & \\ & \ddots & \\ & & e^{i\lambda_d t} \end{bmatrix} U$ (unitary)

Grover’s quantum search algorithm

Quantum search problem

Given: a black box computing $f: \{0,1\}^n \rightarrow \{0,1\}$

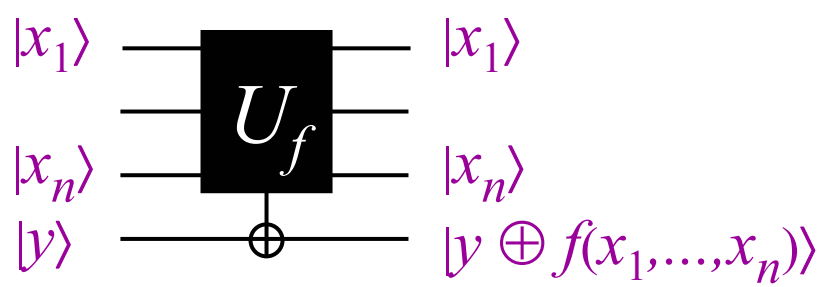
Goal: determine if f is ***satisfiable*** (if $\exists x \in \{0,1\}^n$ s.t. $f(x) = 1$)

In positive instances, it makes sense to also ***find*** such a satisfying assignment x

Classically, using probabilistic procedures, order 2^n queries are necessary to succeed—even with probability ¾ (say)

Grover's ***quantum*** algorithm that makes only $O(\sqrt{2^n})$ queries

Query:



[Grover '96]

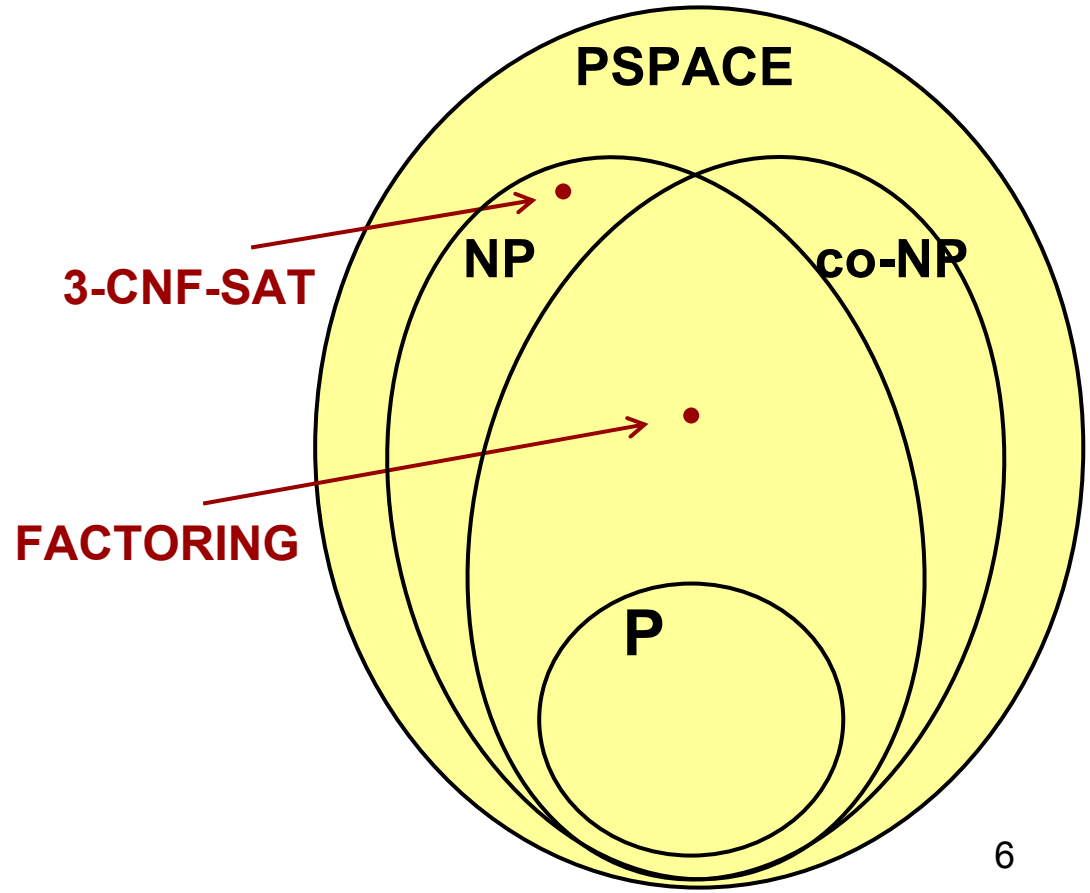
Applications of quantum search

The function f could be realized as a **3-CNF formula**:

$$f(x_1,\ldots,x_n)=(x_1 \vee \bar{x}_3 \vee x_4)\wedge(\bar{x}_2 \vee x_3 \vee \bar{x}_5)\wedge\cdots\wedge(\bar{x}_1 \vee x_5 \vee \bar{x}_n)$$

Alternatively, the search could be for a certificate for any problem in **NP**

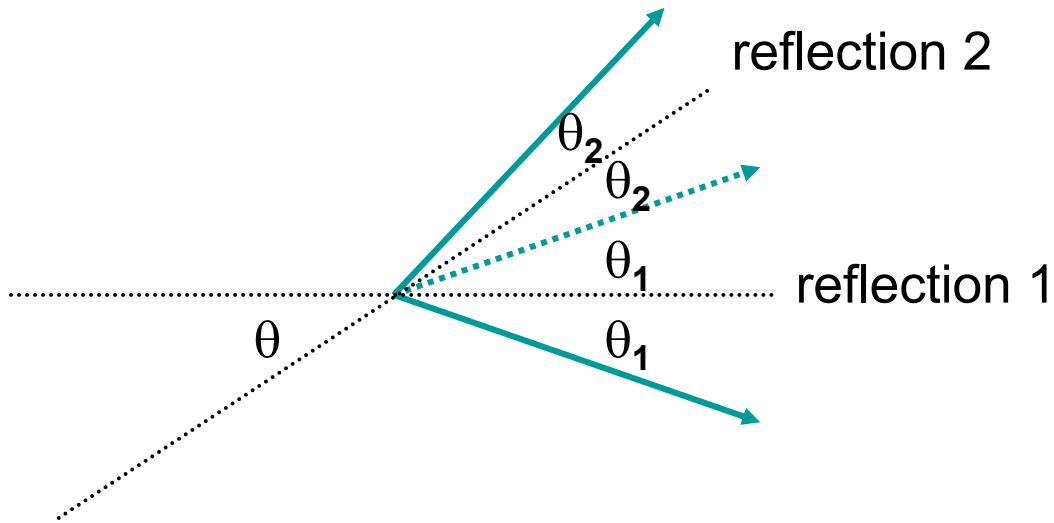
The resulting quantum algorithms appear to be ***quadratically*** more efficient than the best classical algorithms known



Prelude to Grover's algorithm:

two reflections = a rotation

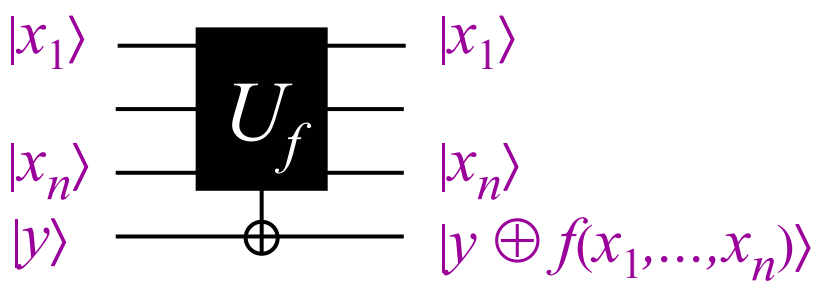
Consider two lines with intersection angle θ:



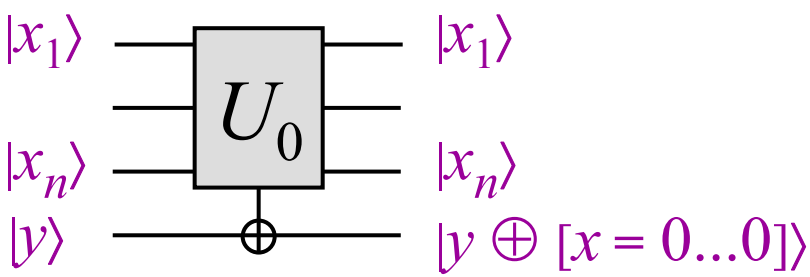
Net effect: rotation by angle 2θ, ***regardless of starting vector***

Grover's algorithm: description I

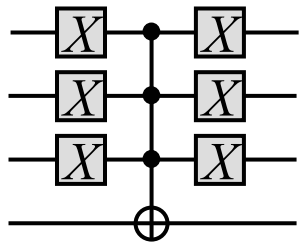
Basic operations used:



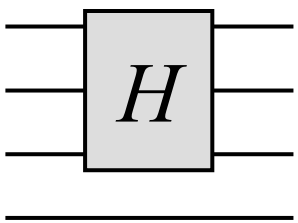
$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$



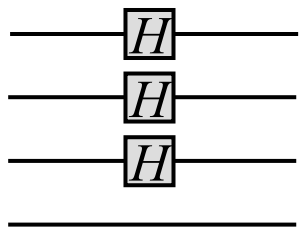
Implementation?



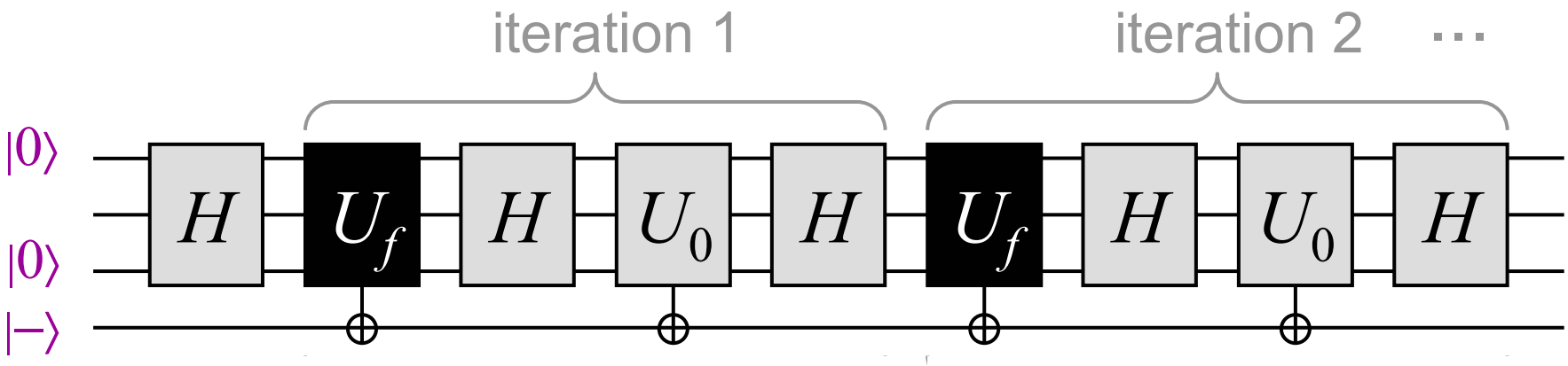
$$U_0\,|x\rangle|-\rangle = (-1)^{[x\,=\,0\ldots0]}|x\rangle|-\rangle$$



Hadamard



Grover's algorithm: description II



1. construct state $H|0...0\rangle|-\rangle$
2. <u>repeat</u> k <u>times</u>:

   apply $-HU_0HU_f$ to state
3. measure state, to get $x \in \{0,1\}^n$, and check if $f(x)=1$

(The setting of k will be determined later)

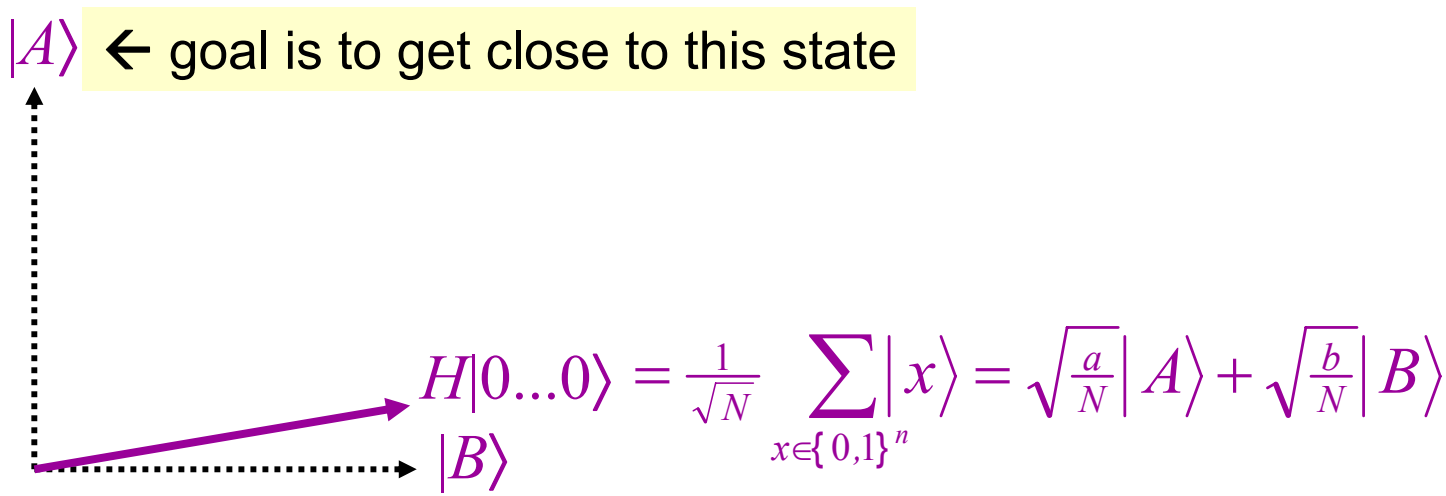
Grover's algorithm: analysis I

Let $A = \{x \in \{0,1\}^n : f(x) = 1\}$ and $B = \{x \in \{0,1\}^n : f(x) = 0\}$

and $N = 2^n$ and $a = |A|$ and $b = |B|$

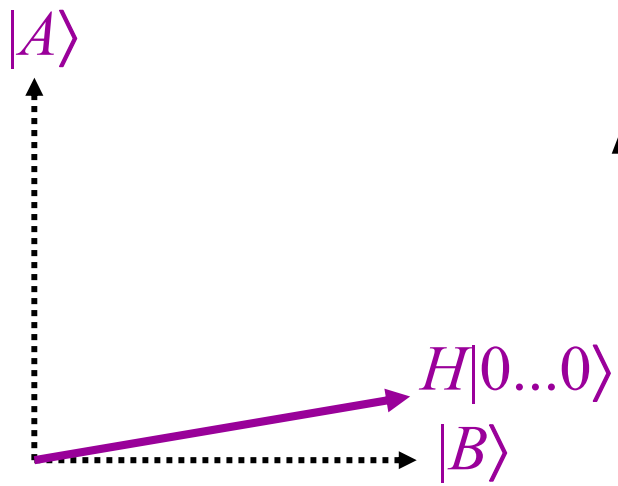
Let $|A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$ and $|B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$

Consider the space spanned by $|A\rangle$ and $|B\rangle$



Interesting case: $a << N$

Grover's algorithm: analysis II



Algorithm: $(-HU_0HU_f)^k H|0...0\rangle$

Observation:

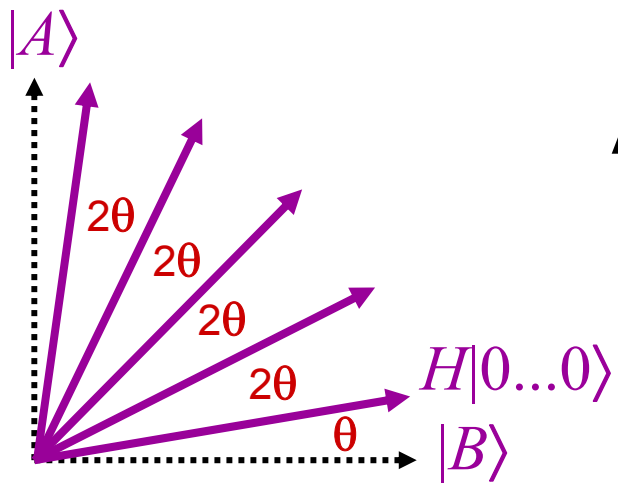
U_f is a reflection about $|B\rangle$: $U_f|A\rangle = -|A\rangle$ and $U_f|B\rangle = |B\rangle$

Question: what is $-HU_0H$? U_0 is a reflection about $H|0...0\rangle$

Partial proof:

$$-HU_0HH|0...0\rangle = -HU_0|0...0\rangle = -H(-|0...0\rangle) = H|0...0\rangle$$

Grover's algorithm: analysis III



Algorithm: $(-HU_0HU_f)^k H|0...0\rangle$

Since $-HU_0HU_f$ is a composition of two reflections, it is a rotation by 2θ, where $\sin(\theta)=\sqrt{a/N} \approx \sqrt{a/N}$

When $a = 1$, we want $(2k+1)(1/\sqrt{N}) \approx \pi/2$, so $k \approx (\pi/4)\sqrt{N}$

More generally, it suffices to set $k \approx (\pi/4)\sqrt{N/a}$

Question: what if a is not known in advance?

Introduction to Quantum Information Processing

CS 667 / Phys 767 / C&O 681

Lecture 17 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Optimality of Grover's algorithm

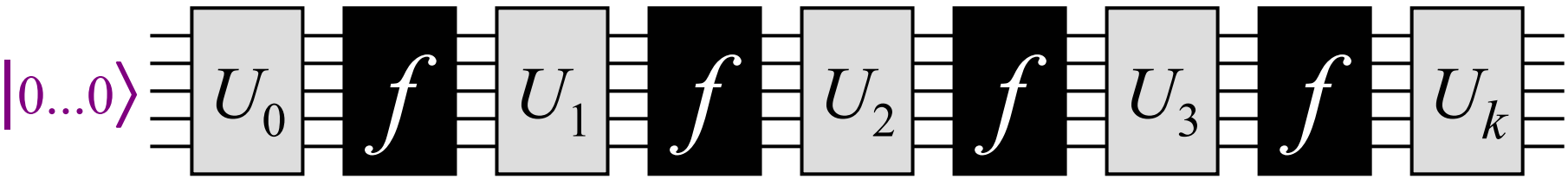
Optimality of Grover's algorithm

Theorem: any quantum search algorithm for $f: \{0,1\}^n \rightarrow \{0,1\}$ must make $\Omega(\sqrt{2^n})$ queries to f (if f is used as a black-box)

Proof (of a slightly simplified version)**:**

Assume queries are of the form

and that a k-query algorithm is of the form

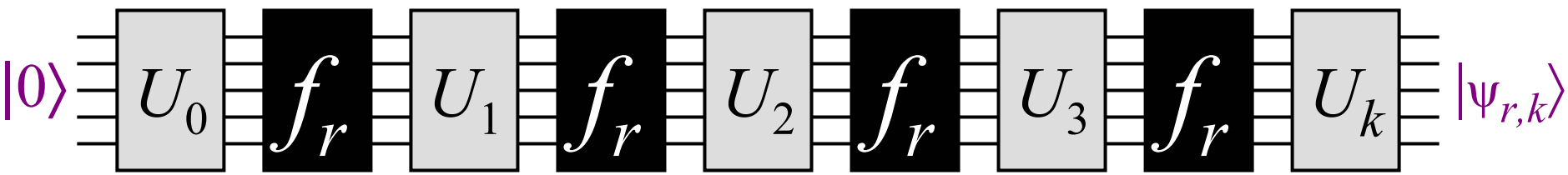


where U_0, U_1, U_2, ..., U_k, are arbitrary unitary operations

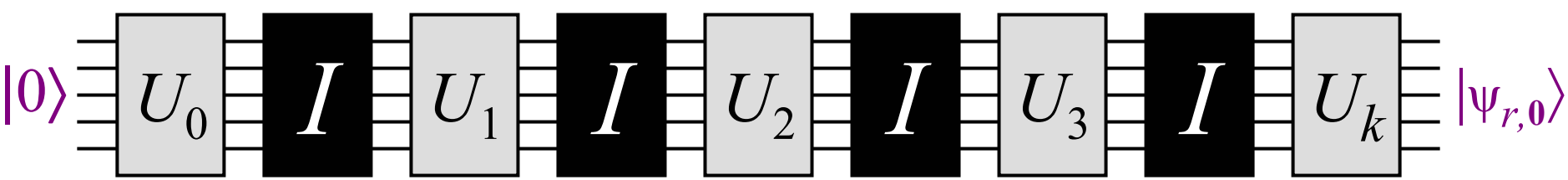
Optimality of Grover's algorithm

Define $f_r : \{0,1\}^n \rightarrow \{0,1\}$ as $f_r(x) = 1$ iff $x = r$

Consider



versus

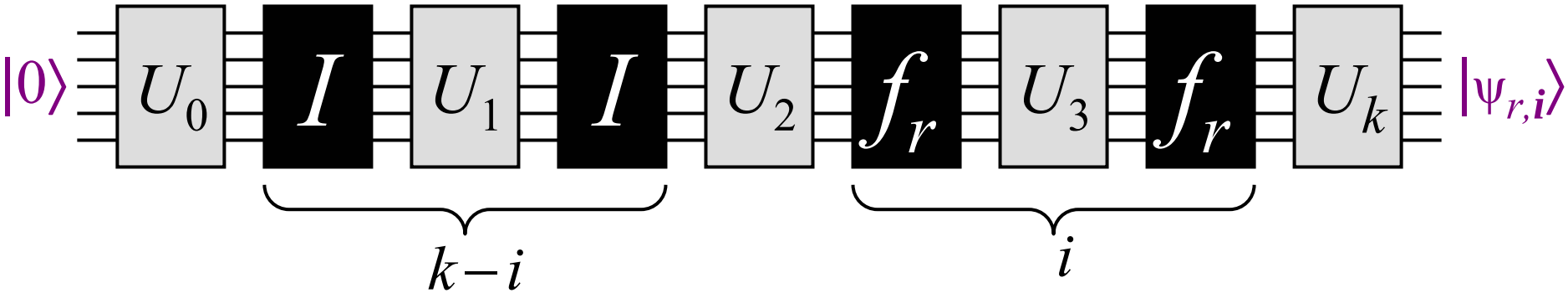


We'll show that, averaging over all $r \in \{0,1\}^n$,

$$\| \, |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \, \| \leq 2k/\sqrt{2^n}$$

Optimality of Grover's algorithm

Consider



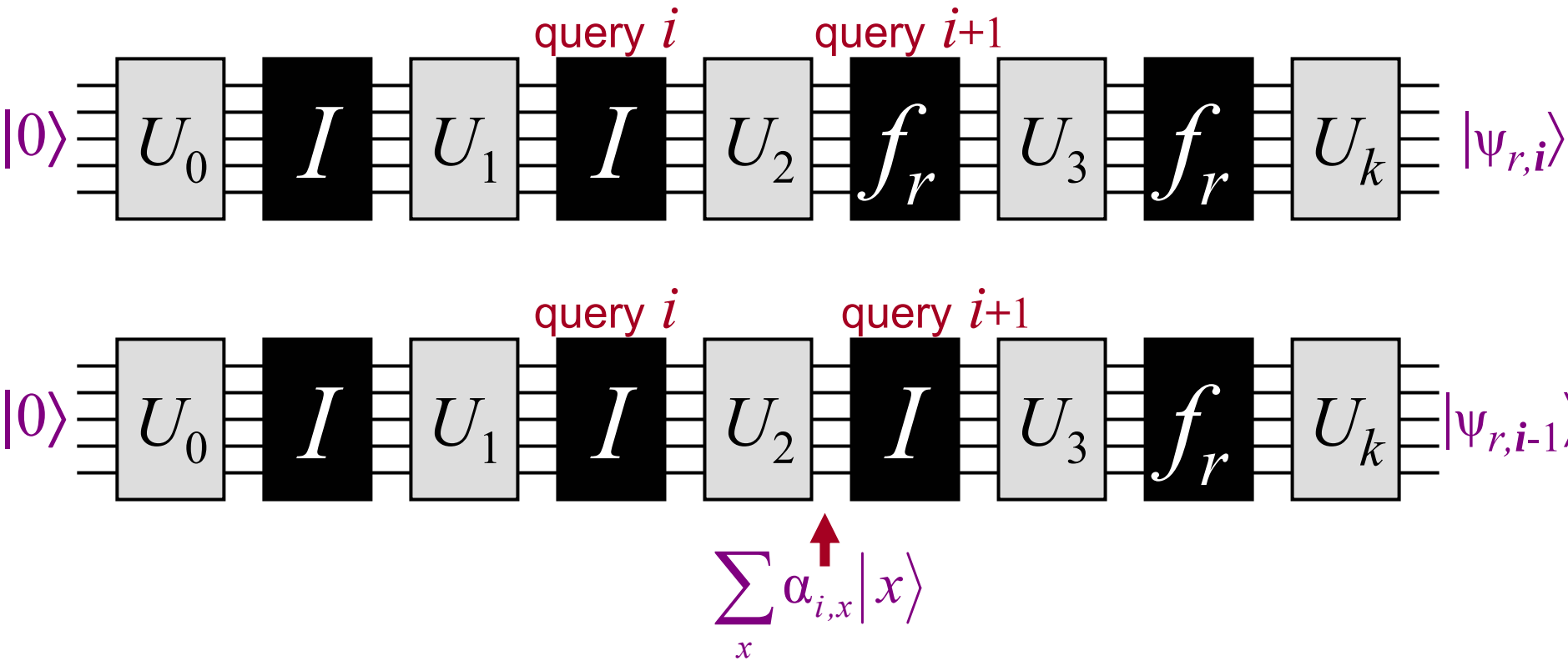
Note that

$$|\psi_{r,k}\rangle - |\psi_{r,0}\rangle = \left(|\psi_{r,k}\rangle - |\psi_{r,k-1}\rangle\right) + \left(|\psi_{r,k-1}\rangle - |\psi_{r,k-2}\rangle\right) + \ldots + \left(|\psi_{r,1}\rangle - |\psi_{r,0}\rangle\right)$$

which implies

$$\| \, |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \, \| \leq \| \, |\psi_{r,k}\rangle - |\psi_{r,k-1}\rangle \, \| + \ldots + \| \, |\psi_{r,1}\rangle - |\psi_{r,0}\rangle \, \|$$

Optimality of Grover's algorithm



$\| \, |\psi_{r,i}\rangle - |\psi_{r,i\text{-}1}\rangle \, \| = |2\alpha_{i,r}|$, since query only negates $|r\rangle$

Therefore, $\| \, |\psi_{r,k}\rangle - |\psi_{r,0}\rangle \, \| \leq \sum_{i=0}^{k-1} 2|\alpha_{i,r}|$

Optimality of Grover's algorithm

Now, averaging over all $r \in \{0,1\}^n$,

$$\frac{1}{2^n}\sum_r \left\| \left|\psi_{r,k}\right\rangle - \left|\psi_{r,0}\right\rangle \right\| \le \frac{1}{2^n}\sum_r \left(\sum_{i=0}^{k-1} 2\left|\alpha_{i,r}\right| \right)$$

$$= \frac{1}{2^n}\sum_{i=0}^{k-1} 2\left(\sum_r \left|\alpha_{i,r}\right| \right)$$

$$\le \frac{1}{2^n}\sum_{i=0}^{k-1} 2\left(\sqrt{2^n}\right) \qquad \text{(By Cauchy-Schwarz)}$$

$$= \frac{2k}{\sqrt{2^n}}$$

Therefore, for ***some*** $r \in \{0,1\}^n$, the number of queries k must be $\Omega\left(\sqrt{2^n}\right)$, in order to distinguish f_r from the all-zero function

This completes the proof

Introduction to Quantum Information Processing

CS 667 / Phys 767 / C&O 681

Lecture 18 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Lab tour

(instead of a regular lecture)

Introduction to Quantum Information Processing

CS 667 / Phys 767 / C&O 681

Lecture 19 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Preliminary remarks about quantum communication

Quantum information can apparently be used to substantially reduce ***computation*** costs for a number of interesting problems

How does quantum information affect the ***communication costs*** of information processing tasks?

We explore this issue ...

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 ***teleportation*** and ***superdense coding***

—but they ***cannot*** be used to “signal instantaneously”

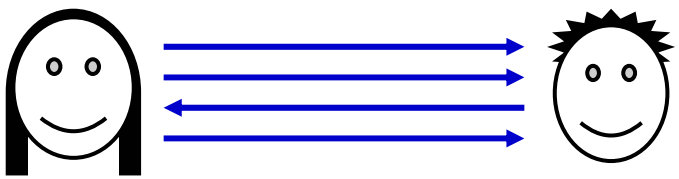
Any operation performed on one system has no affect on the state of the other system (its reduced density matrix)

Basic communication scenario

Goal: convey n bits from Alice to Bob

Basic communication scenario

Bit communication:

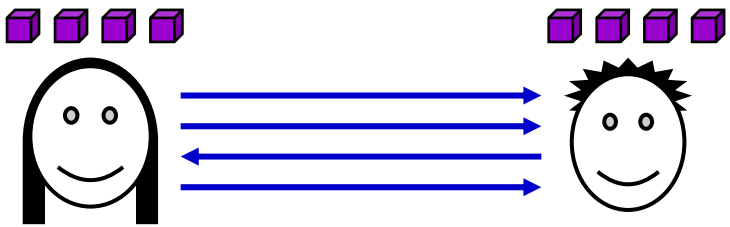


Cost: n

Qubit communication:

Cost: n [Holevo's Theorem, 1973]

Bit communication
& prior entanglement:



Cost: n (can be deduced)

Qubit communication
& prior entanglement:

Cost: $n/2$ superdense coding

[Bennett & Wiesner, 1992]

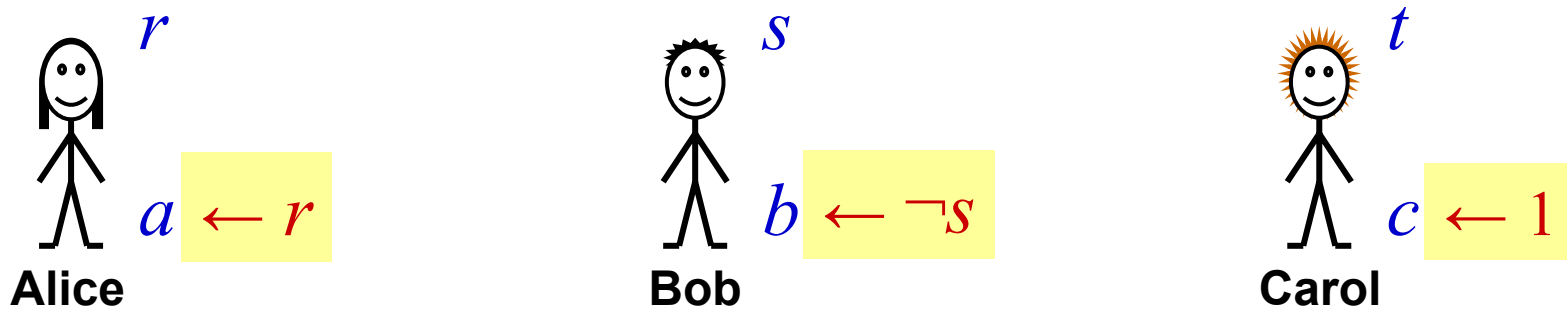
The GHZ “paradox”

GHZ scenario

[Greenberger, Horne, Zeilinger, 1980]

Input: r s t

Output: $a \leftarrow r$ $b \leftarrow \neg s$ $c \leftarrow 1$



Rules of the game:

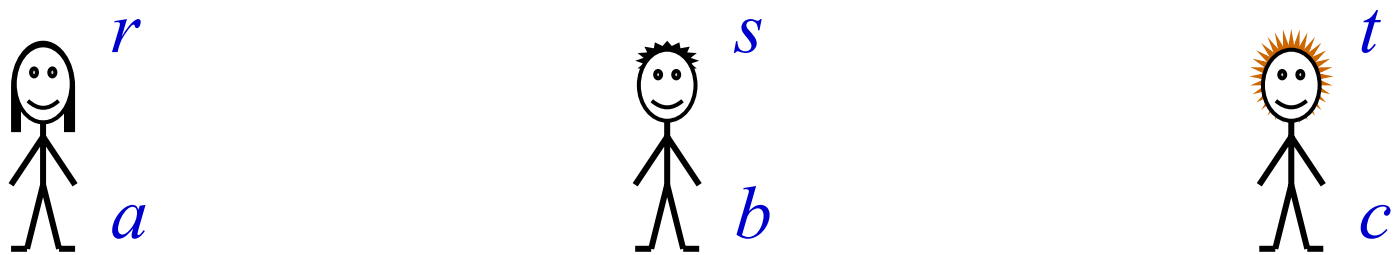
1. It is promised that $r \oplus s \oplus t = 0$
2. No communication after inputs received
3. They ***win*** if $a \oplus b \oplus c = r \vee s \vee t$

rst	$a \oplus b \oplus c$	abc
000	0	011
011	1	001
101	1	111
110	1	101

No perfect strategy for GHZ

Input:

Output:



rst	$a \oplus b \oplus c$
000	0
011	1
101	1
110	1

General deterministic strategy:

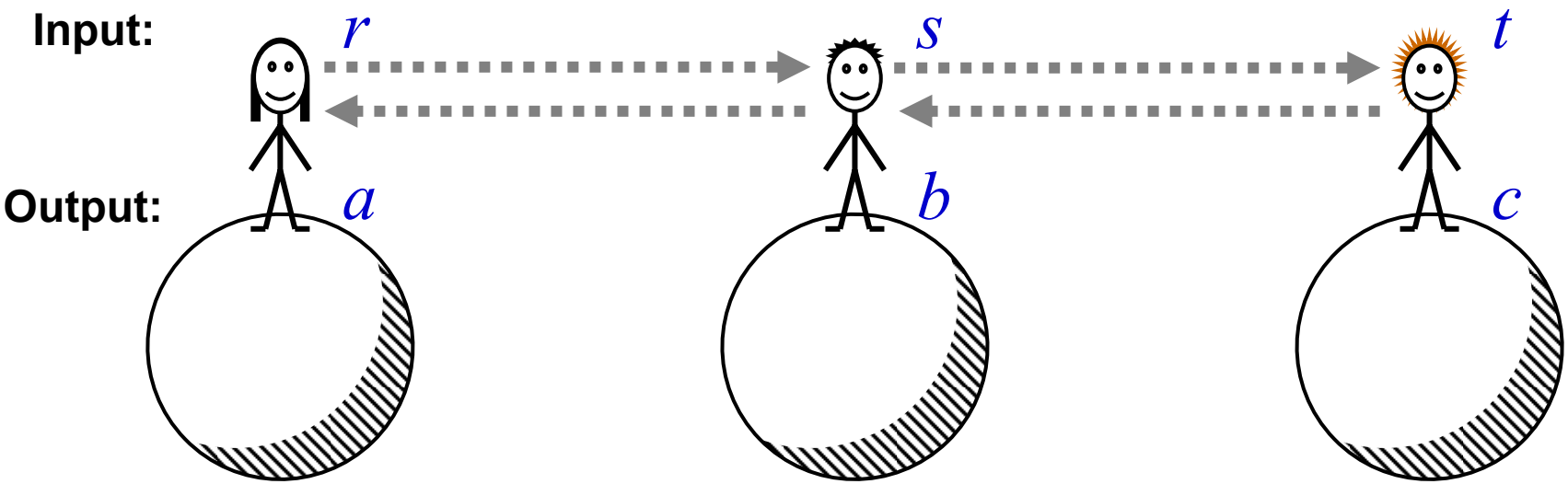
$a_0, a_1, b_0, b_1, c_0, c_1$

Winning conditions:

$$\begin{cases} a_0 \oplus b_0 \oplus c_0 = 0 \\ a_0 \oplus b_1 \oplus c_1 = 1 \\ a_1 \oplus b_0 \oplus c_1 = 1 \\ a_1 \oplus b_1 \oplus c_0 = 1 \end{cases}$$

Has no solution, thus no perfect strategy exists

GHZ: preventing communication

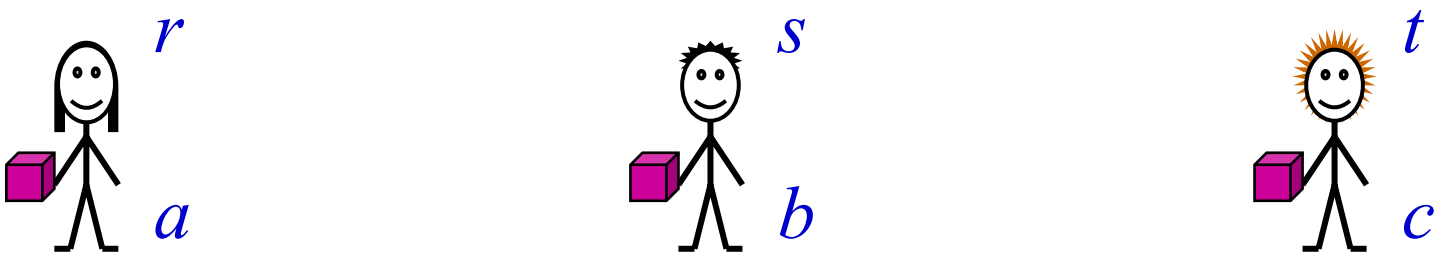


Input and output events can be ***space-like*** separated:
so signals at the speed of light are not fast enough for cheating

What if Alice, Bob, and Carol ***still*** keep on winning?

"GHZ Paradox" explained

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



<u>Alice's strategy:</u>

1. if $r = 1$ then apply H to qubit
2. measure qubit and set a to result

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

<u>Bob's & Carol's strategies:</u> similar

Case 1 ($rst = 000$): state is $|001\rangle + |010\rangle - |100\rangle - |111\rangle$

Case 2 ($rst = 001$): state measured directly ...

Cases 3 & 4 ($rst = 101$ & 110): similar by symmetry

GHZ: conclusions

- For the GHZ game, any ***classical*** team succeeds with probability at most ¾
- 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***

The Bell inequality and its violation

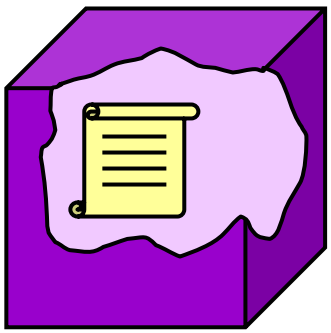
– Physicist's perspective

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:

if $\{|0\rangle,|1\rangle\}$ measurement then output **0**

if $\{|+\rangle,|-\rangle\}$ measurement then output **1**

if **...** (etc)

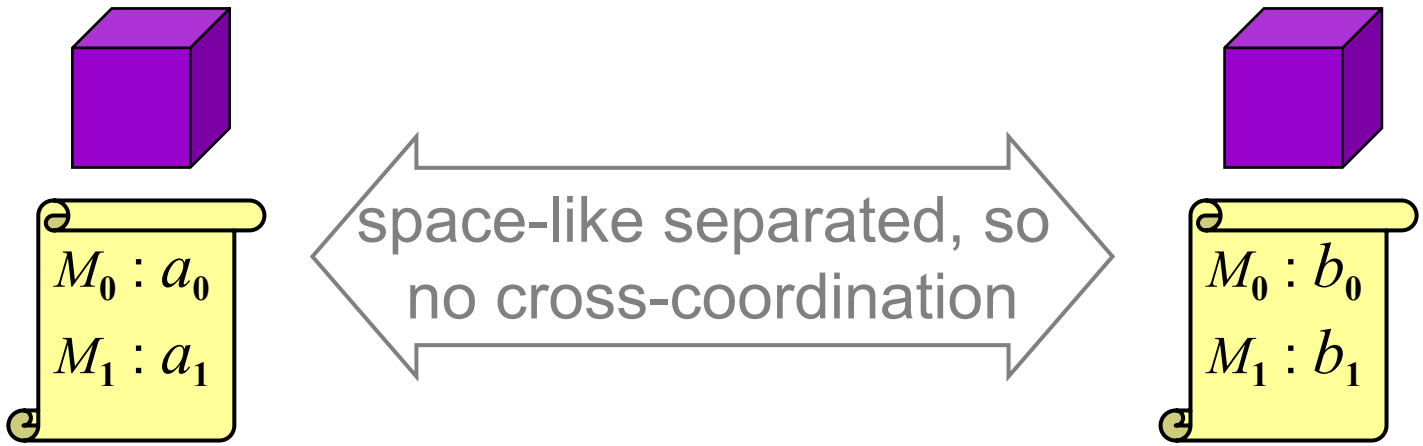
called ***hidden variables***

table could be implicitly given by some formula

[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: $A_0 \underbrace{(B_0 + B_1)} + A_1 \underbrace{(B_0 - B_1)} \leq 2$

one is ± 2 and the other is 0

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****

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 ≤ ½

* also called CHSH Inequality

Introduction to Quantum Information Processing

CS 667 / Phys 767 / C&O 681

Lecture 20 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Violating the Bell Inequality

Two-qubit system in state

$|\phi\rangle = |00\rangle - |11\rangle$

Applying rotations θ_A and θ_B yields:

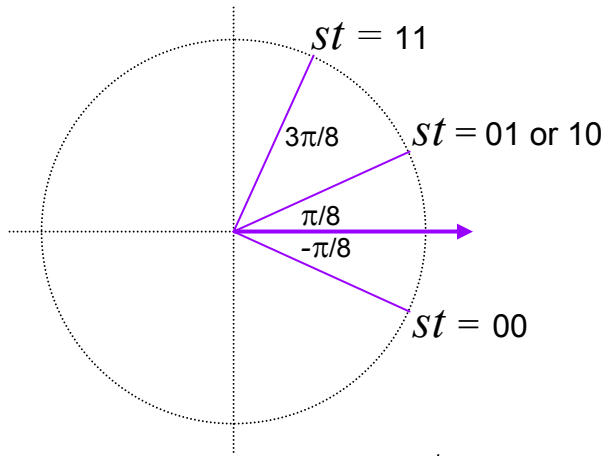
$$\cos(\theta_A + \theta_B)\,\underbrace{(|00\rangle - |11\rangle)}_{AB\,=\,+1} + \sin(\theta_A + \theta_B)\,\underbrace{(|01\rangle + |10\rangle)}_{AB\,=\,-1}$$

Define

M_0: rotate by $-\pi/16$ then measure

M_1: rotate by $+3\pi/16$ then measure

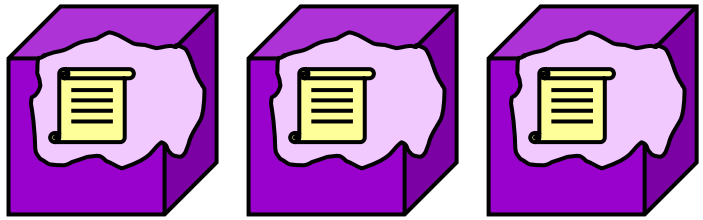
Then $A_0 B_0,\ A_0 B_1,\ A_1 B_0,\ -A_1 B_1$ all have expected value $\frac{1}{2}\sqrt{2}$, which ***contradicts*** the upper bound of $\frac{1}{2}$



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

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

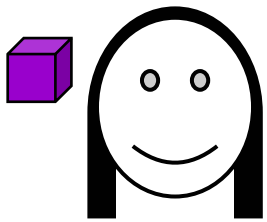
This is, in principle, experimentally verifiable, and experiments along these lines have actually been conducted

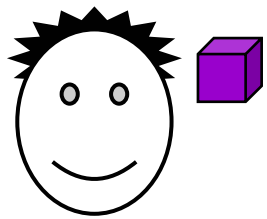
The Bell inequality and its violation – Computer Scientist's perspective

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

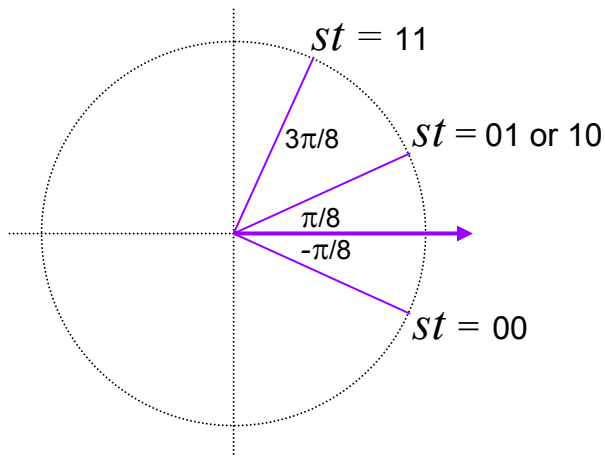
$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = ½ + ¼\sqrt{2} = 0.853\ldots$

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

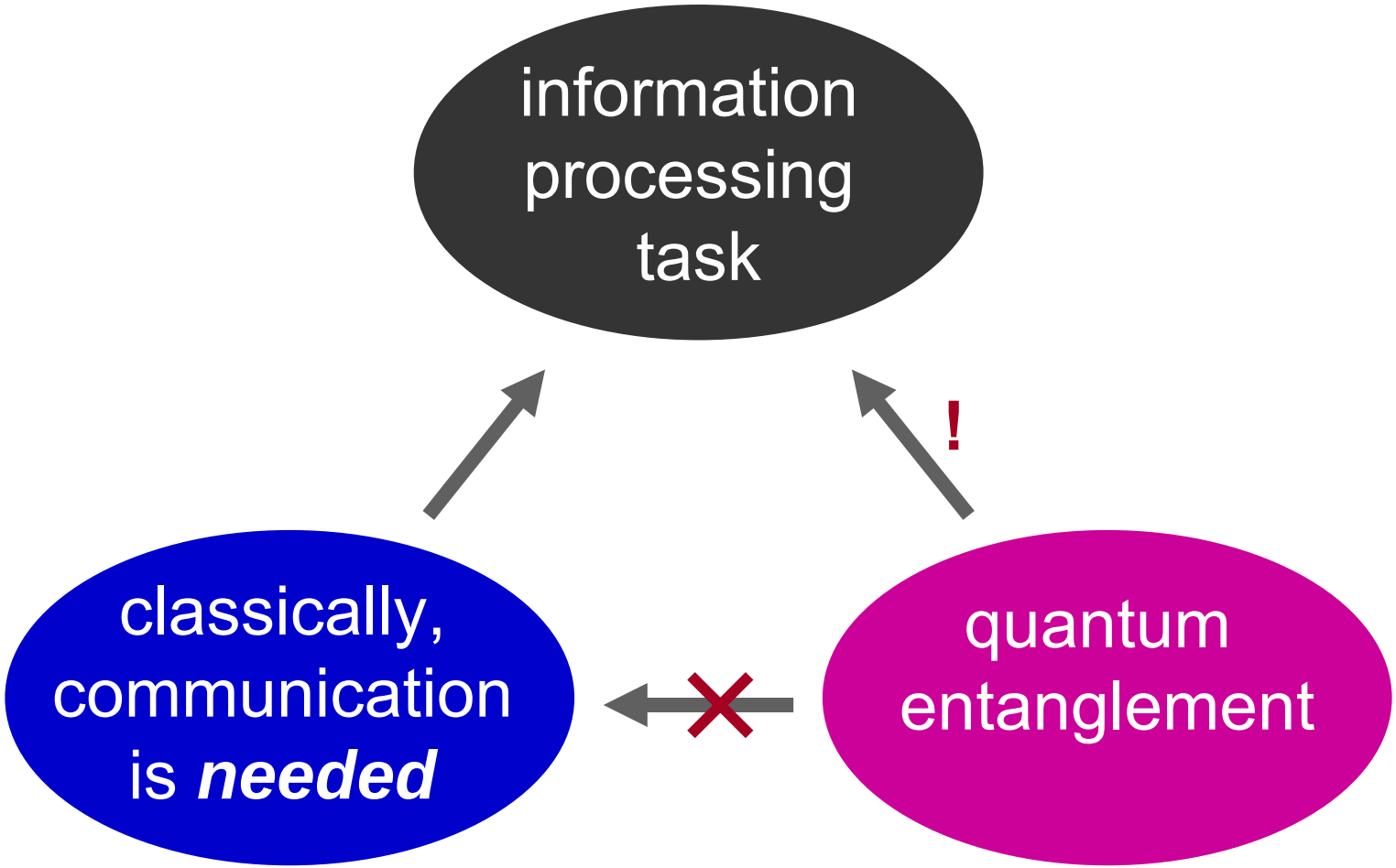


$$\cos(\theta_A - \theta_B)\,(|00\rangle - |11\rangle) + \sin(\theta_A - \theta_B)\,(|01\rangle + |10\rangle)$$

Success probability:

$$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = \tfrac{1}{2} + \tfrac{1}{4}\sqrt{2} = 0.853\ldots$$

Nonlocality in operational terms



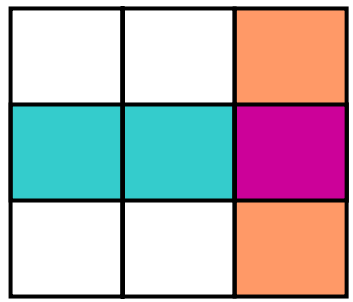
The magic square game

Magic square game

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

a_{11}	a_{12}	a_{13}	even
a_{21}	a_{22}	a_{23}	even
a_{31}	a_{32}	a_{33}	even
odd	odd	odd	

IMPOSSIBLE



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

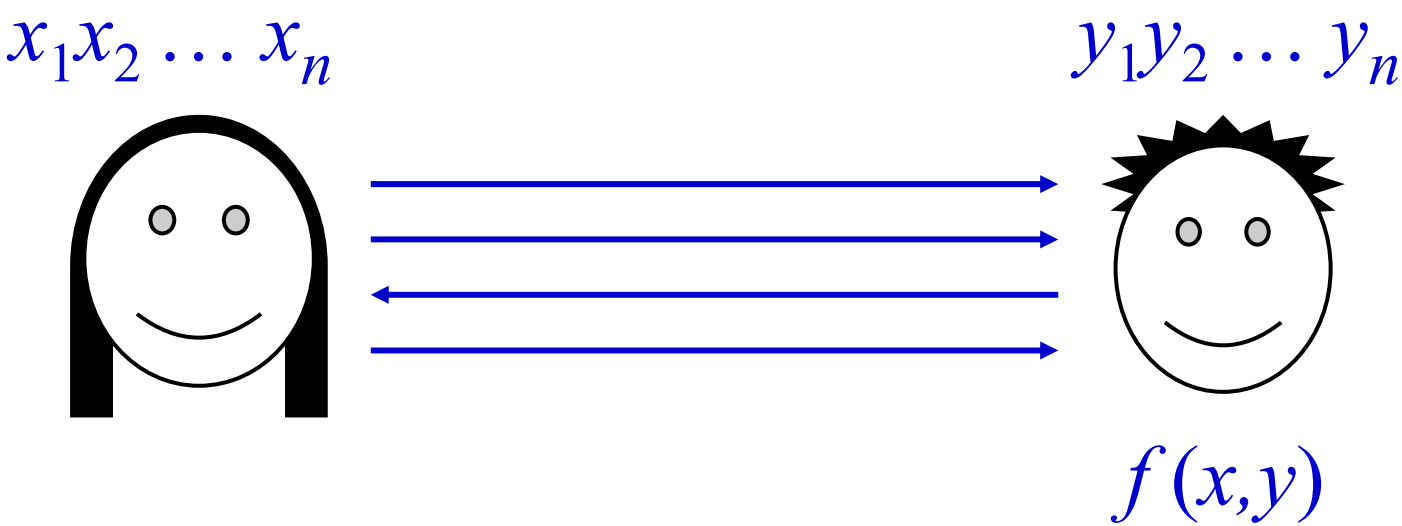
Success probabilities: $8/9$ classical and 1 quantum

[Aravind, 2002] (details omitted here)

Preview of communication complexity

Classical Communication Complexity

[Yao, 1979]



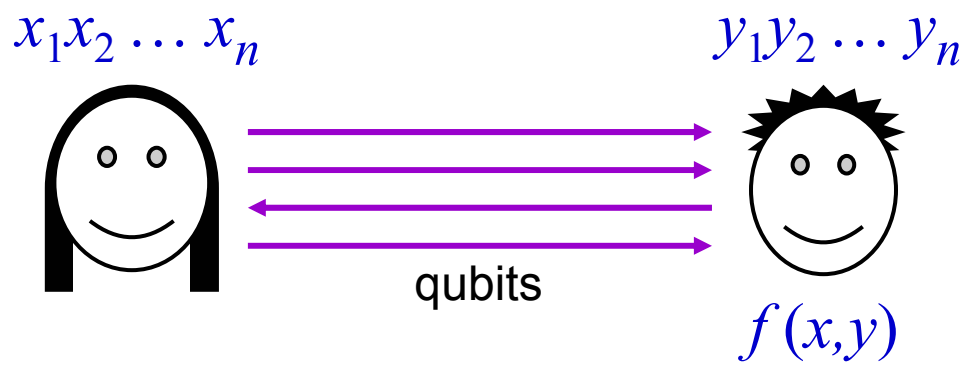
E.g. equality function: $f(x,y) = 1$ if $x = y$, and 0 if $x \neq y$

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

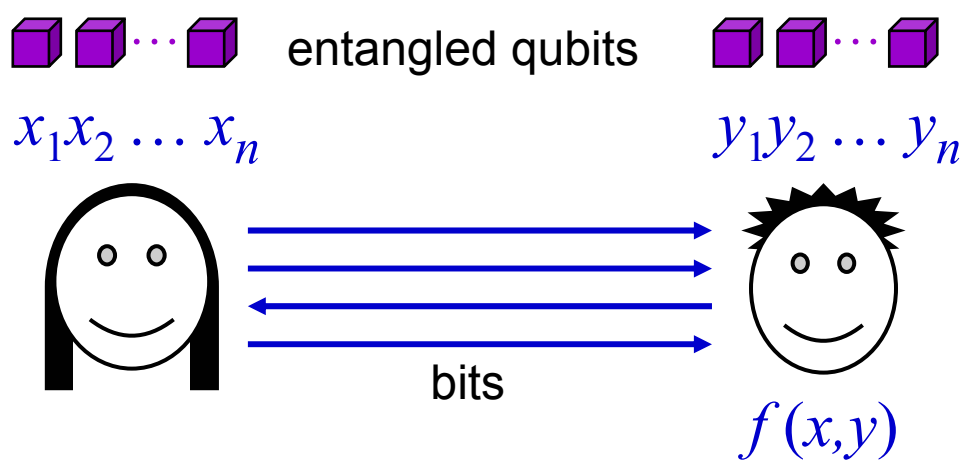
Probabilistic protocols can solve with only $O(\log(n/\varepsilon))$ bits communication (error probability ε)

Quantum Communication Complexity

Qubit communication



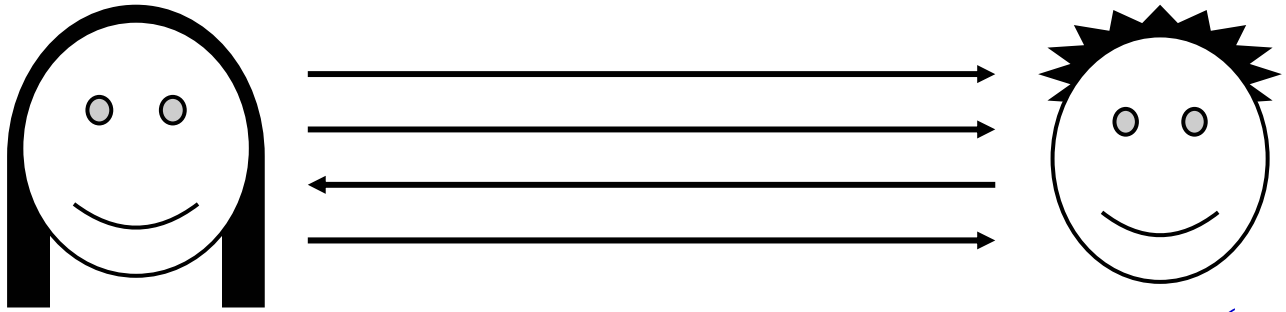
Prior entanglement



Question: can quantum beast classical in this context?

Appointment scheduling

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



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

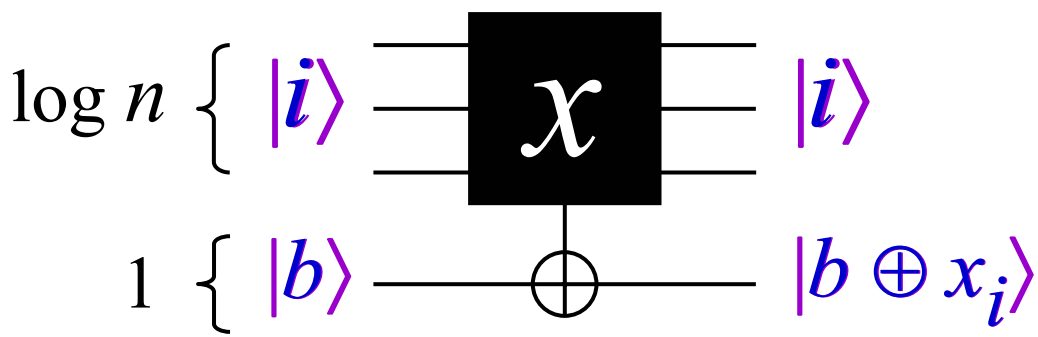
Classically, $\Omega(n)$ **bits** necessary to succeed with prob. $\geq 3/4$

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

[KS '87] [BCW '98]

Search problem

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



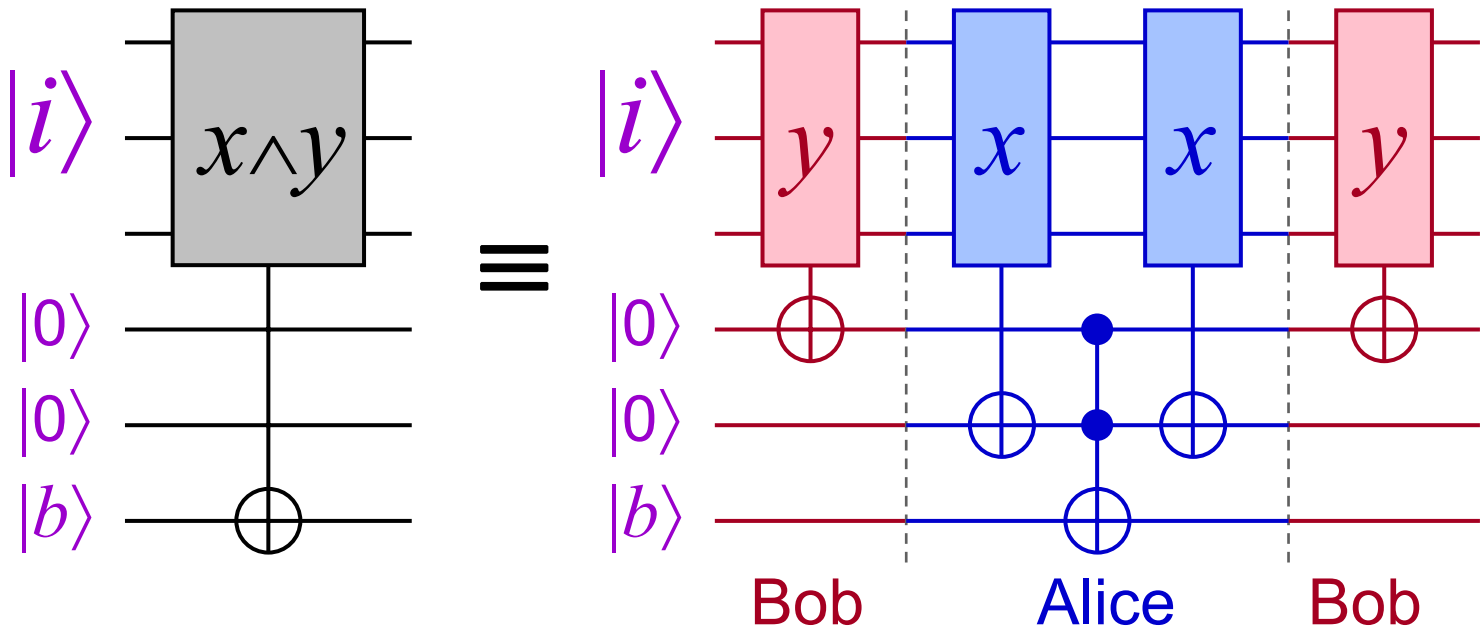
Goal: find $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$

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

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

[Grover, 1996]

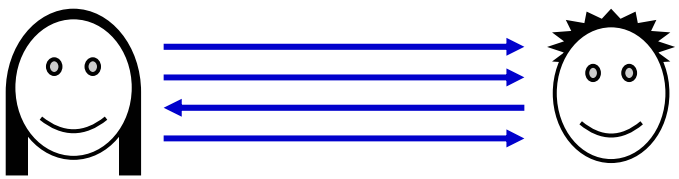
		1	2	3	4	5	6	...	n
Alice	$x =$	0	1	1	0	1	0	...	0
Bob	$y =$	1	0	0	1	1	0	...	1
	$x \wedge y =$	0	0	0	0	1	0	...	0



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

Appointment scheduling: epilogue

Bit communication:

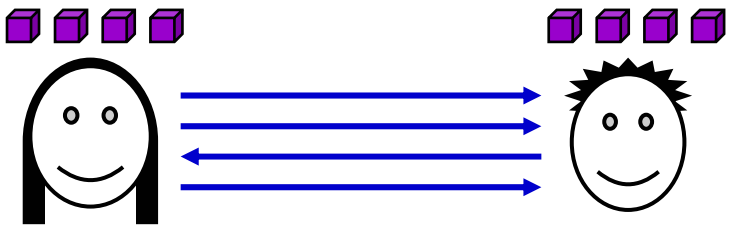


Cost: $\theta(n)$

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]

Are exponential savings possible?

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. $\boldsymbol{C}$

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 $2^n/2^k\sqrt{n} < 1.99^n$, 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?

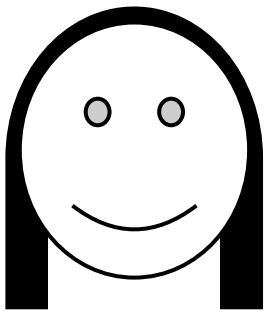
Answer: just 2 bits are sufficient!

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

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

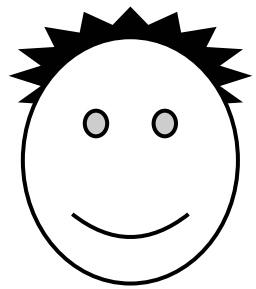
$|\psi\rangle$: a $\log(n)$-qubit state (described ***classically***)

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



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

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



[Raz, 1999]

Lower bound for the inner product problem

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

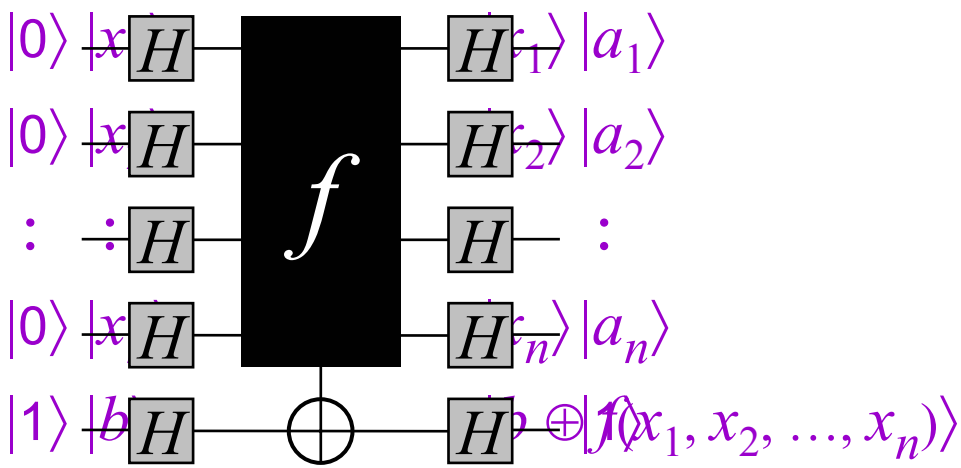
[KY '95] [CNDT '98] [NS '02]

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 $a_1, a_2, \ldots, a_n$

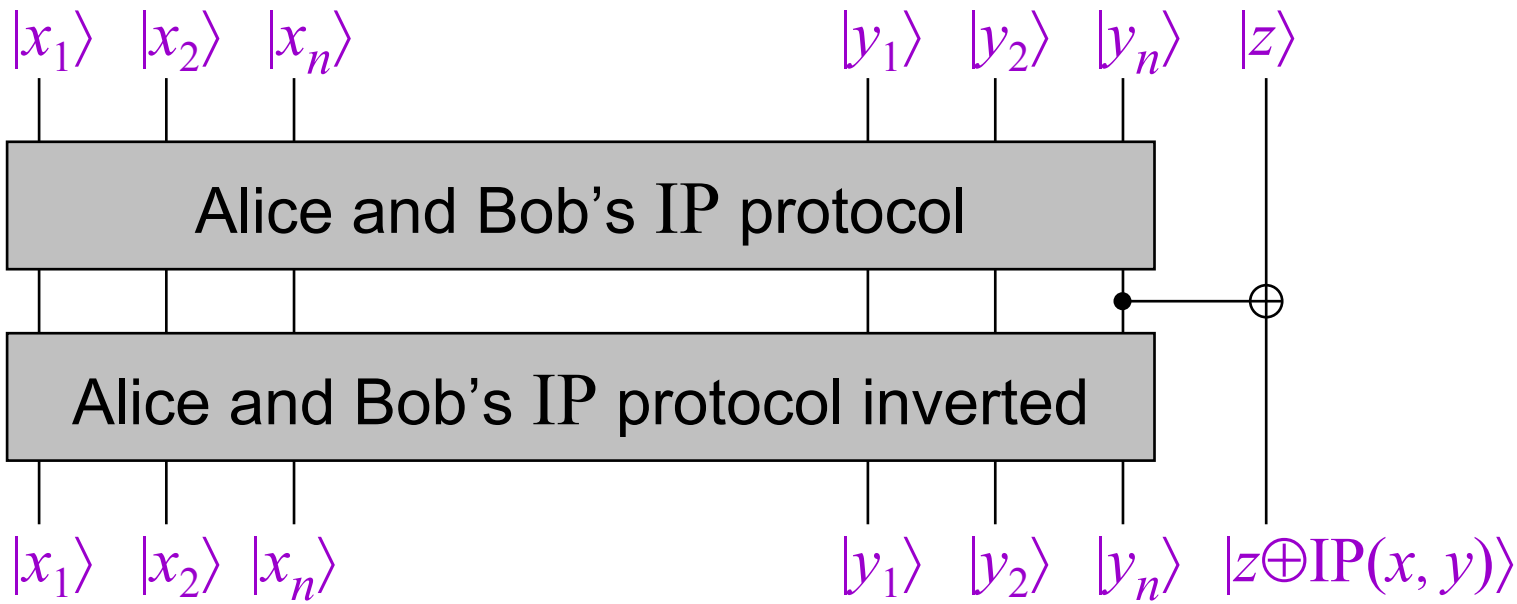
Classically, n queries are necessary

Quantum mechanically, 1 query is sufficient

Lower bound for inner product

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

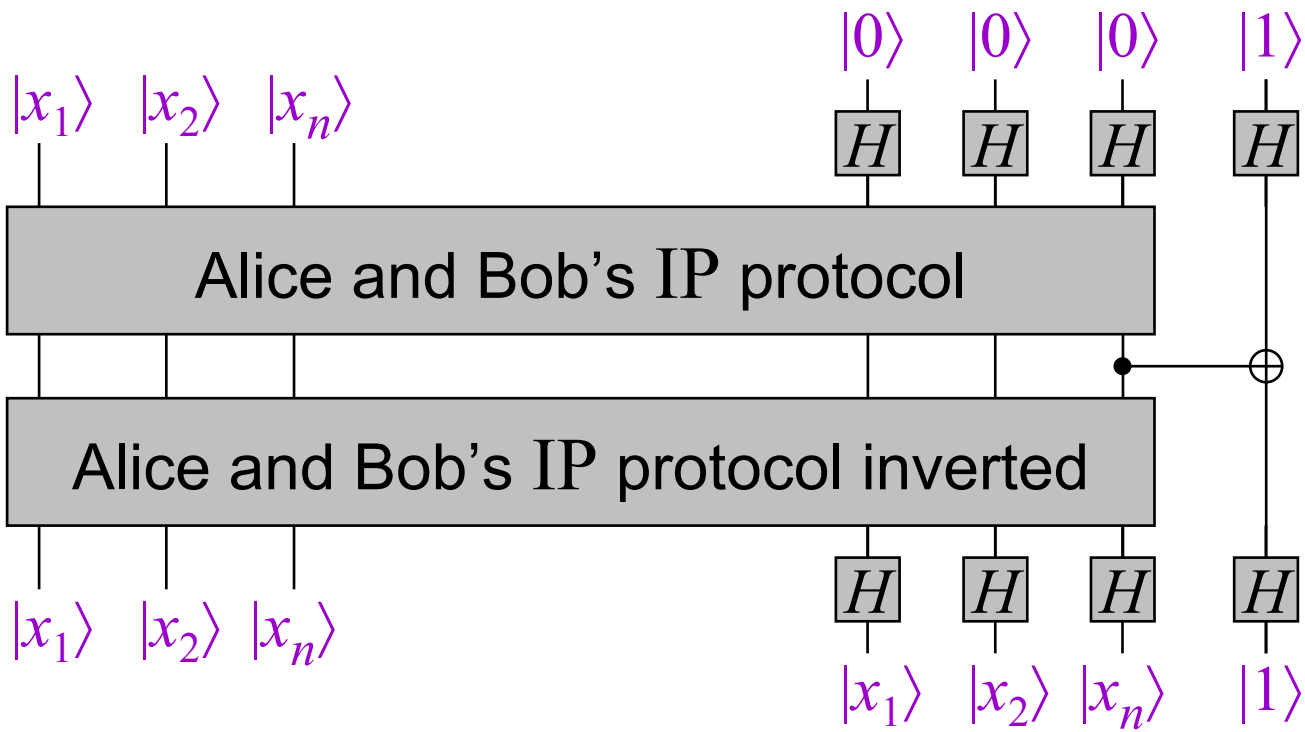
Proof:



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:

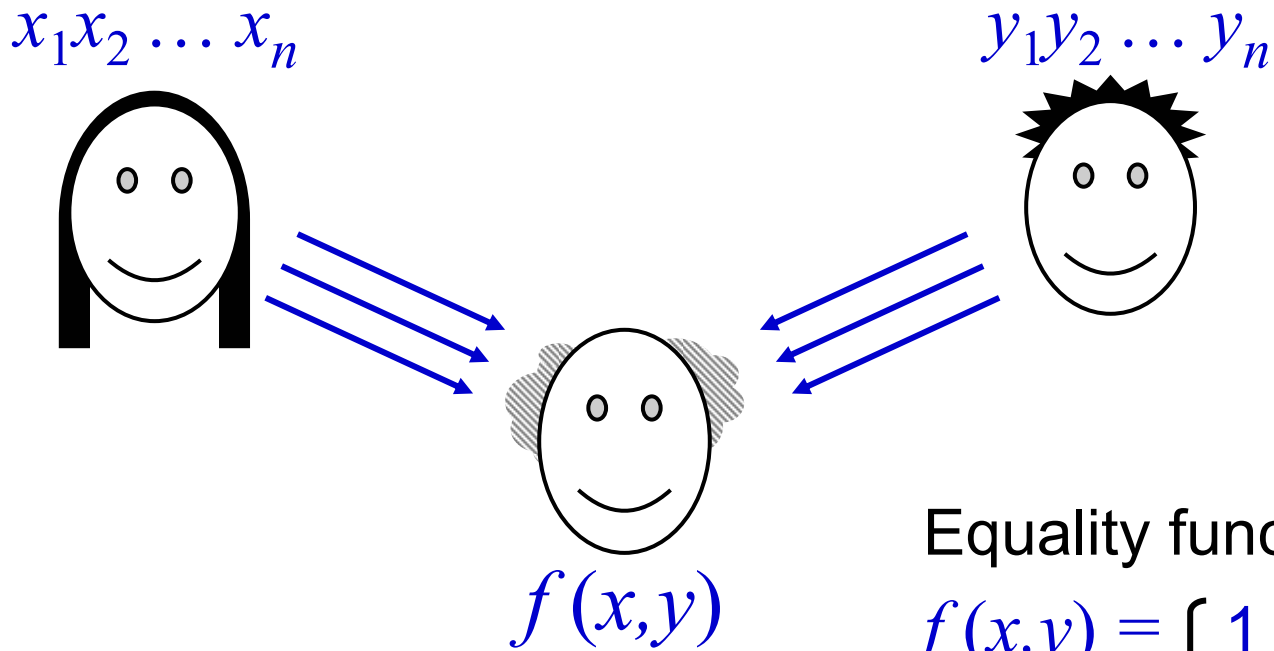


Since n bits are conveyed from Alice to Bob, n qubits communication necessary (by Holevo's Theorem)

Simultaneous message passing and fingerprinting

Equality revisited

in simultaneous message model

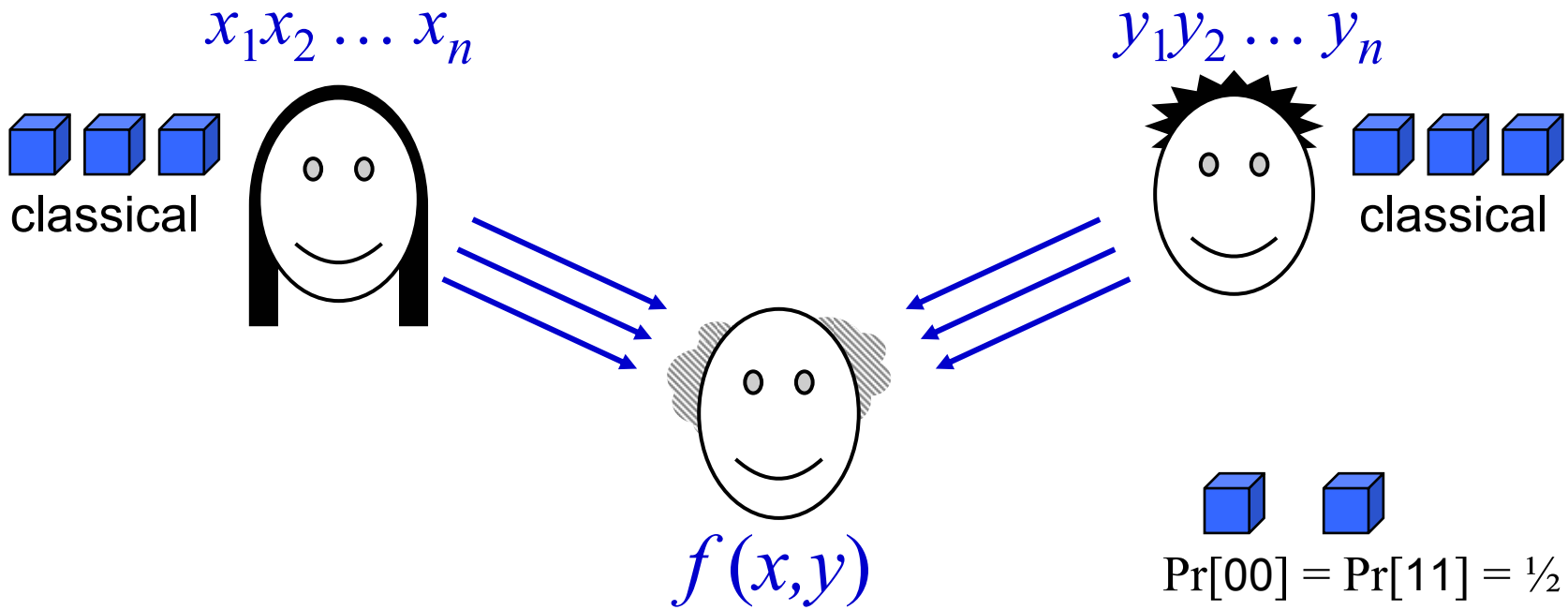


Equality function:

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

Exact protocols: require $2n$ bits communication

Equality revisited
in simultaneous message model



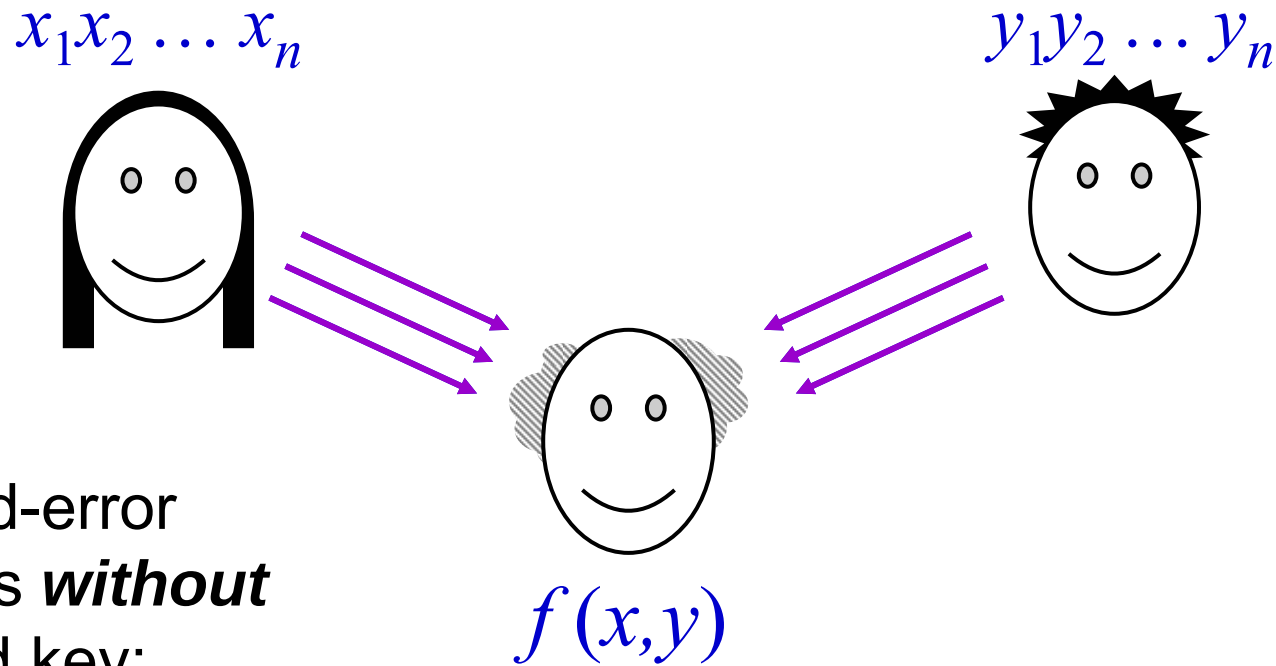
Bounded-error protocols with a shared random key:
require only $O(1)$ bits communication

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

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

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 $a > 0$

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

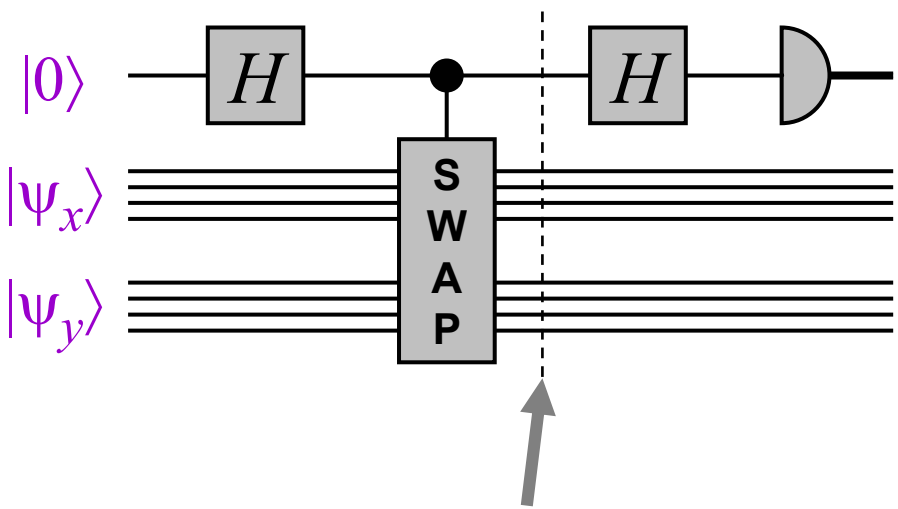
By duplicating each state, $|\psi_x\rangle \otimes |\psi_x\rangle \otimes \ldots \otimes |\psi_x\rangle$, the pairwise inner products can be made arbitrarily small: $(1-2d)^r \le \varepsilon$

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:



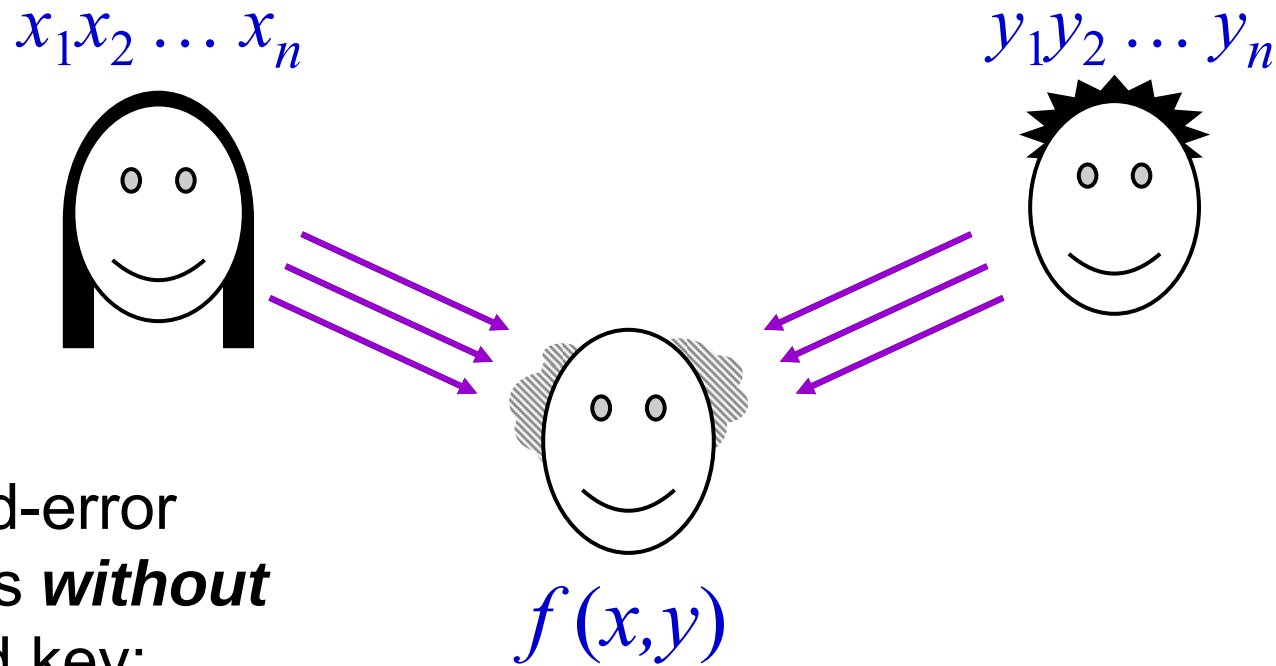
if $x = y$, $\Pr[\text{output} = 0] = 1$

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



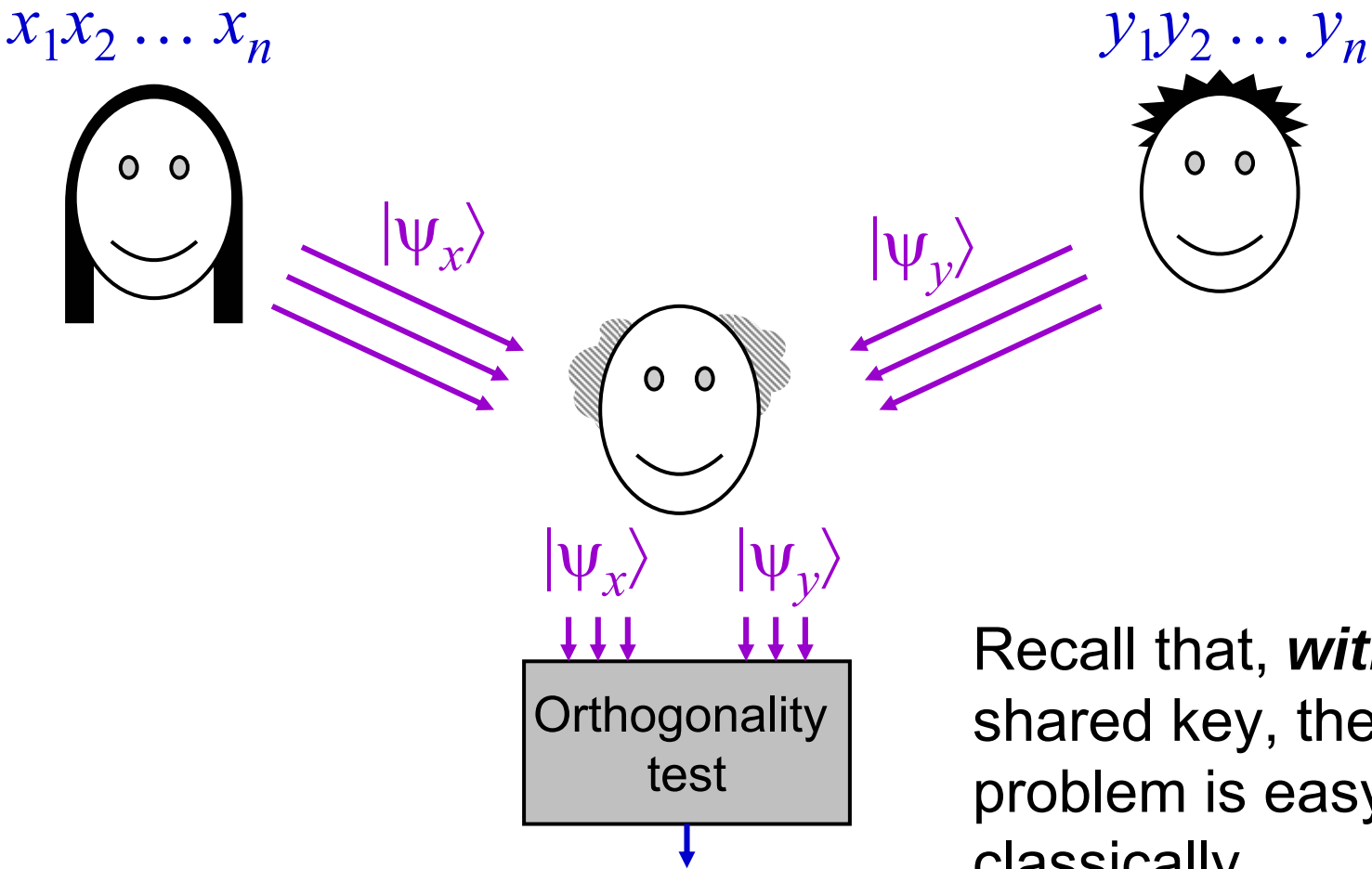
Bounded-error protocols ***without*** a shared key:

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

Quantum: $\theta(\log n)$

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

Quantum protocol for equality
in simultaneous message model



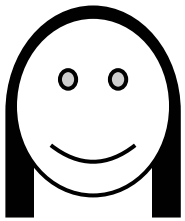
Recall that, ***with*** a shared key, the problem is easy classically ...

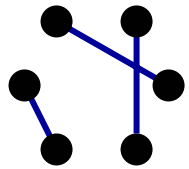
Hidden matching problem

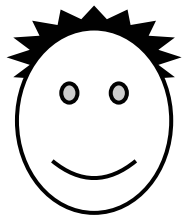
Hidden matching problem

For this problem, a quantum protocol is exponentially more efficient than any classical protocol—even with a shared key

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



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



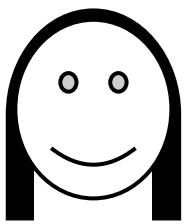
Output: $(i, j, x_i \oplus x_j)$, such that $(i, j) \in M$

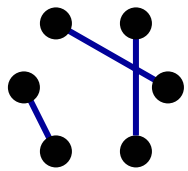
Only ***one-way*** communication (Alice to Bob) is permitted

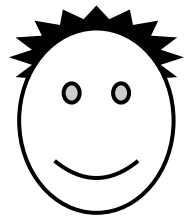
[Bar-Yossef, Jayram, Kerenidis, 2004]

The hidden matching problem

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



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



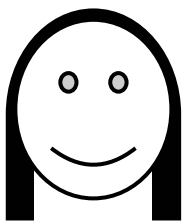
Output: $(i, j, x_i \oplus x_j)$, $(i, j) \in M$

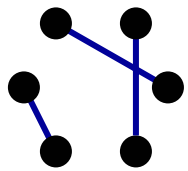
Classically, one-way communication is $\Omega(\sqrt{n})$, even with a shared classical key (the proof is omitted here)

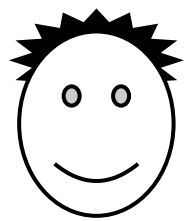
Rough intuition: Alice doesn't know which edges are in M, so she apparently has to send $\Omega(\sqrt{n})$ bits of the form $x_i \oplus x_j$ …

The hidden matching problem

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



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



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

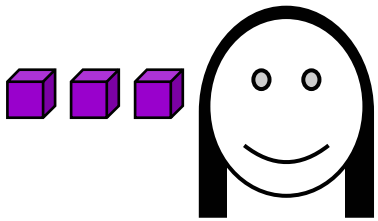
Quantum protocol: Alice sends $\frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_k} |k\rangle$ ($\log n$ qubits)

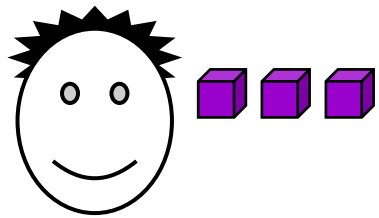
Bob measures in $|i\rangle \pm |j\rangle$ basis, $(i, j) \in M$, and uses the outcome's relative phase to determine $x_i \oplus x_j$

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****

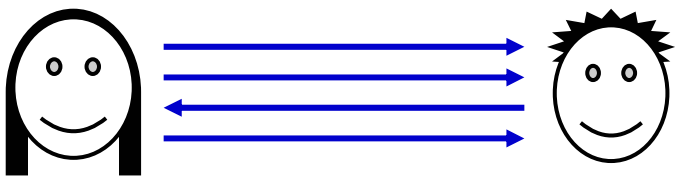
With $(|00\rangle + |11\rangle)^{\otimes \log n}$ prior entanglement, no communication is needed at all*

∗ Technical details similar to restricted equality of Lecture 17

[BCT '99]

Restricted-equality nonlocality

Bit communication:

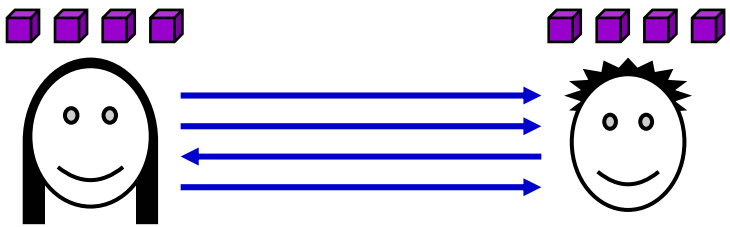


Cost: $\theta(n)$

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