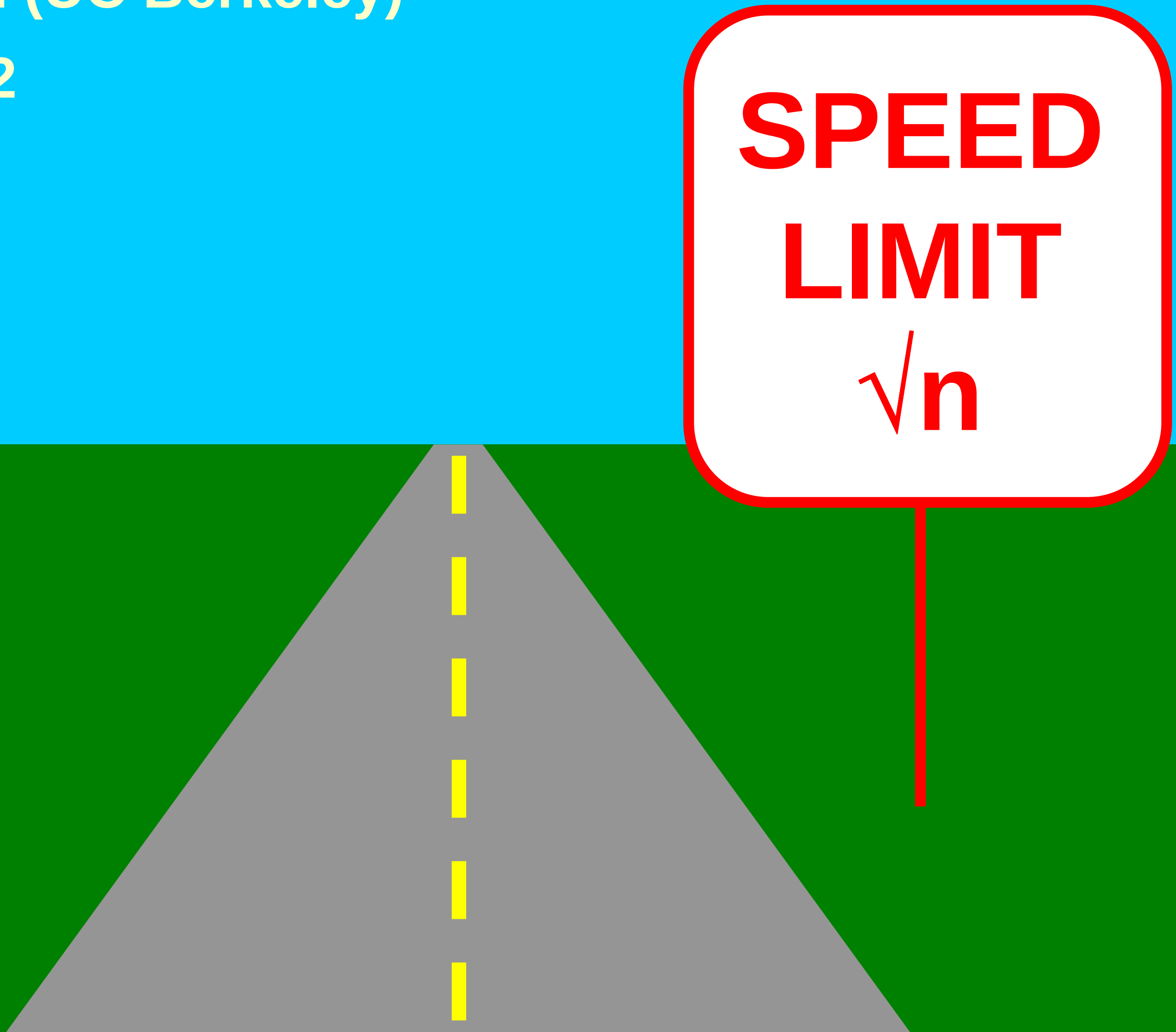
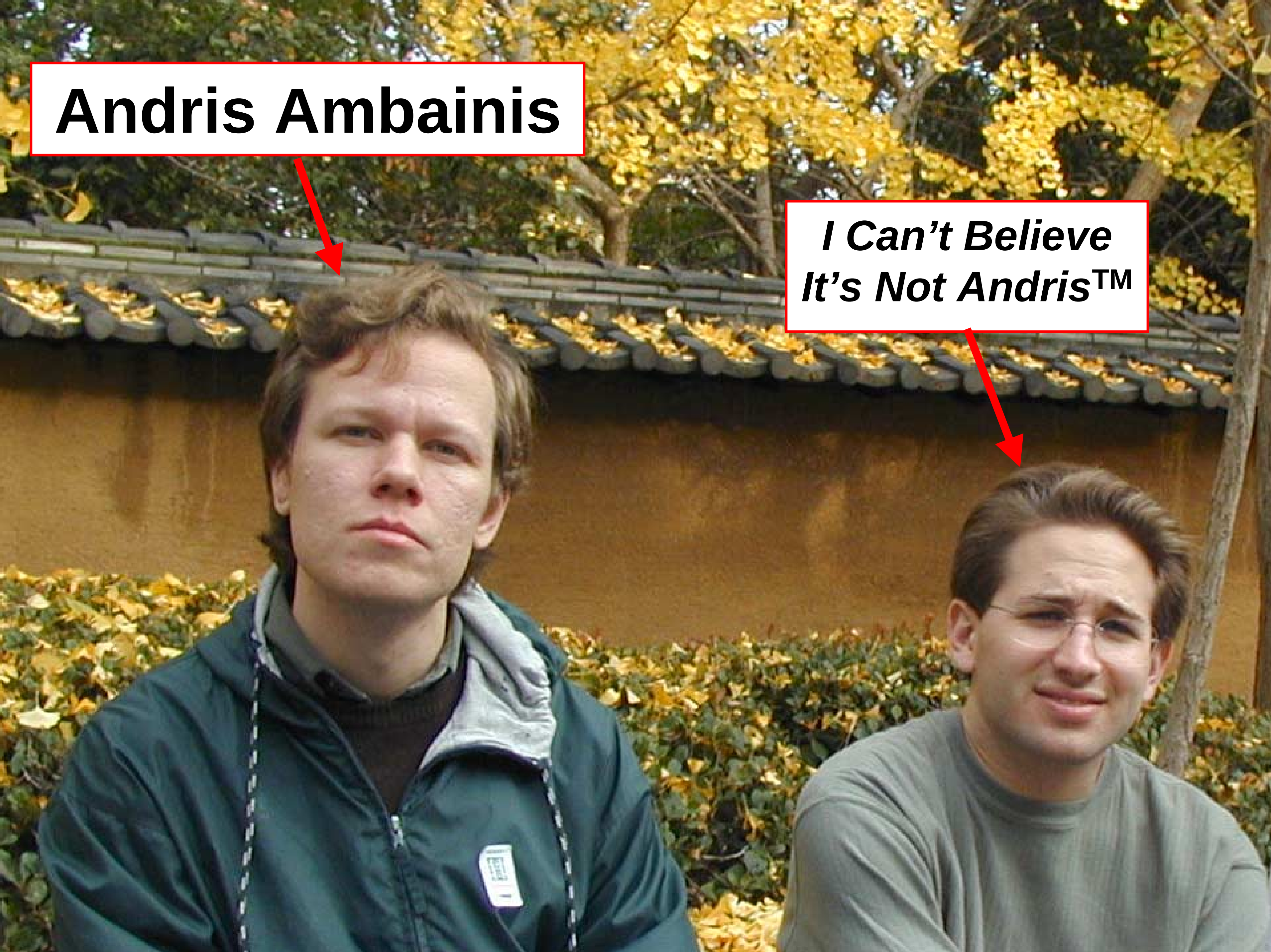
Quantum Lower Bounds

Scott Aaronson (UC Berkeley)

August 29, 2002




Andris Ambainis
I Can't Believe It's Not Andris™

Many of the deepest discoveries of science are **limitations**

- No superluminal signaling
- No perpetual-motion machines
- No complete axiomitization for arithmetic

What limitations on computing are imposed by the laws of physics?

Quantum computing lets us seriously address this question

That's why everyone should care about it

even if factoring machines are never built

Conjecture 1: Quantum computers can't solve NP-complete problems (solve = in polynomial time)

Too hard—we don't even know if classical ones can

Conjecture 2: Quantum computers can't solve NP-complete problems unless classical ones can also

Still too hard

Conjecture 3: Quantum computers can't solve NP-complete problems using only 'brute force'

Looks easier—but can we formalize the notion of 'brute force'?

Black-Box Model

Suppose we want to decide whether Boolean formula φ has a satisfying assignment

Brute force might mean we restrict ourselves to asking, i.e.,

"Does assignment X satisfy φ?"

So we're treating φ as a **black box**

There are 2^n possible questions

How many must we ask to know whether any one has a "yes" answer?

What if we can ask in superposition?

Quantum Query Model

Suppose there are n possible yes/no questions

Let $x_i \in \{0,1\}$ be answer to question i

In quantum algorithm, each basis state has form $|i,z\rangle$, where

i = index to query   z = workspace

Query transformation Q maps each $|i,z\rangle$ to $(1-2x_i)|i,z\rangle$

(i.e. performs phase flip conditioned on $x_i=1$)

Quantum Query Model (con't)

Algorithm consists of **interleaved queries and unitaries**:

$$U_0 \rightarrow Q \rightarrow U_1 \rightarrow \ldots \rightarrow U_{T-1} \rightarrow Q \rightarrow U_T$$

U_t: arbitrary unitary that doesn't depend on x_i's

(we don't care how hard it is to implement)

At the end we measure to obtain a basis state $|i,z\rangle$, then output (say) first bit of z

Quantum Query Complexity

Let $f(X)$ be the function we're trying to compute

Algorithm **computes** f if it outputs $f(X)$ with probability at least 2/3 for every X

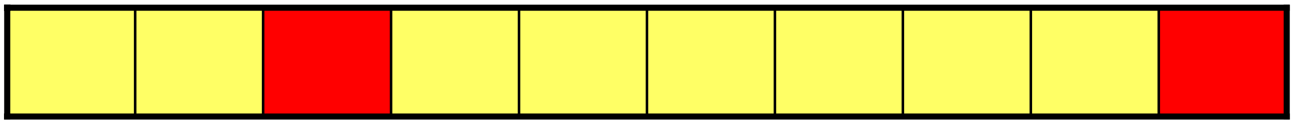
Q(f) = minimum # of queries made by any algorithm that computes f

Immediate: $Q(f) \leq R(f) \leq D(f)$

R(f) = randomized query complexity

D(f) = deterministic query complexity

Example: Search



Are there any marked items in database?

$OR_n(x_1 \ldots x_n) =$ 0 if every x_i is 0

1 otherwise

Classical: $D(OR_n) = R(OR_n) = \Theta(n)$

Quantum: $Q(OR_n) = O(\sqrt{n})$, from Grover's algorithm

Show: $Q(OR_n) = \Omega(\sqrt{n})$—i.e., Grover's algorithm is optimal

Lower Bound Methods

- **Hybrid Method**

  Bennett, Bernstein, Brassard, Vazirani 1994

- **Polynomial Method**

  Beals, Buhrman, Cleve, Mosca, de Wolf 1998

- **Adversary Method**

  Ambainis 2000

We'll skip (1), and prove search lower bound with (2) and again (3)

Polynomial Method

Quantum algorithm that computes f with few queries → Low-degree polynomial approximating f → Low-degree *univariate* polynomial with large derivative

I can prove this can't exist!

Our Mathematician Friend

Multivariate polynomial p **approximates** f if for every $x_1 \ldots x_n$, $|p(x_1 \ldots x_n) - f(x_1 \ldots x_n)| \leq 1/3$

$\widetilde{\deg}(f)$ = minimum degree of polynomial that approximates f

Proposition: $Q(f) \geq \widetilde{\deg}(f)/2$ for all f

Proof: Initially, amplitude $\alpha_{i,z}$ of each $|i,z\rangle$ is a degree-0 multilinear polynomial in $x_1 \ldots x_n$

A query replaces each $\alpha_{i,z}$ by $(1-2x_i)\alpha_{i,z}$, increasing its degree by 1. The U_t's can't increase degree.

At the end, squaring amplitudes doubles degree

Symmetrization

Given a polynomial $p(x_1 \ldots x_n)$ of degree d, let

$$q(k) = \underset{x_1+\cdots+x_n=k}{EX}\left[p(x_1 \ldots x_n)\right]$$

Proposition (Minsky-Papert 1968): q(k) is a univariate polynomial in k, with degree at most d

Proof: Let $X=x_1 \ldots x_n$ and $|X|=x_1+\ldots+x_n$. Then

$$q(|X|) = p_{sym}(X) = \frac{1}{n!}\sum_{permutations\ \sigma} p(\sigma(X)).$$

Furthermore, for some $a_1 \ldots a_d$

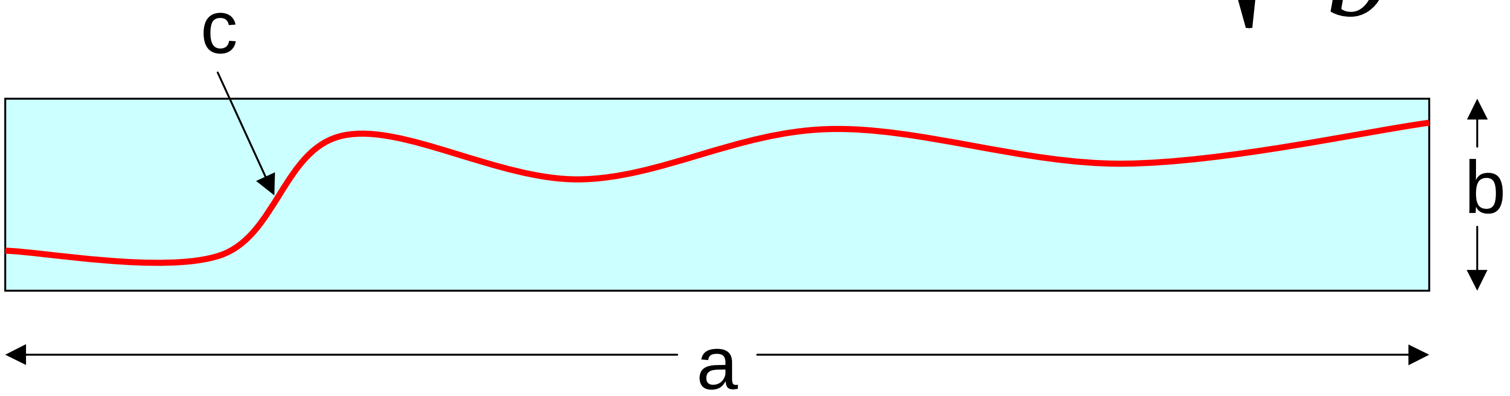
$$p_{sym}(X) = a_0 + a_1\binom{|X|}{1} + \cdots + a_d\binom{|X|}{d}$$

which is a polynomial in |X| of degree d.

Markov's Inequality

Let p be a polynomial bounded in [0,b] in the interval [0,a], that has derivative at least c somewhere in that interval. Then

$$\deg(p) \geq \sqrt{\frac{ac}{b}}.$$



Approximate Degree of OR

Ehlich-Zeller 1964 / Rivlin-Cheney 1966 / Nisan-Szegedy 1994

The polynomial q(k) has q(0)≤1/3 and q(1)≥2/3, so |q'(k)|≥1/3 for some k∈[0,1]

Since q represents acceptance probability, q(k)∈[0,1] for integers k∈{0…n}

What about non-integer k? If q strays h away from [0,1], then |q'(k)|≥2h somewhere

So by Markov,

$$\boxed{\deg(q) \geq \sqrt{\frac{n \max(1/3, 2h)}{1+2h}} = \Omega\left(\sqrt{n}\right)}$$

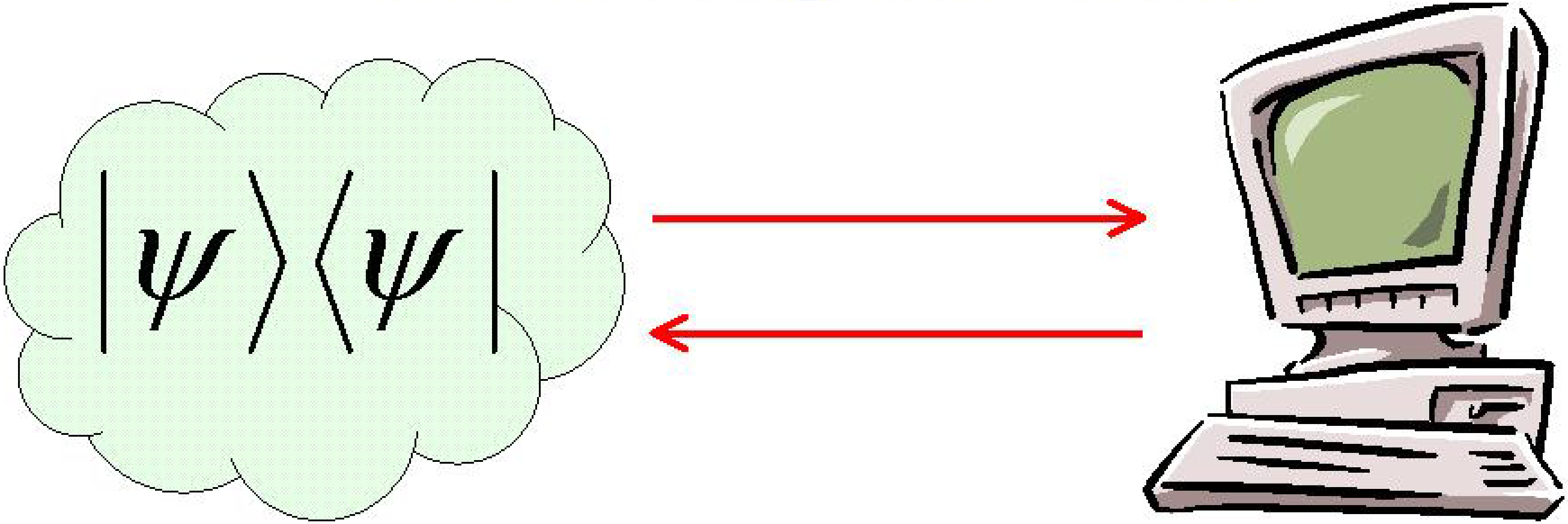
What Else The Polynomial Method Gives Us

$Q(\text{Parity}_n)$ and $Q(\text{Majority}_n)$ are $\Omega(n)$

For any *total* Boolean f, $Q(f) = \Omega(D(f)^{1/6})$

($Q(f) = \Omega(D(f)^{1/4})$ if f is monotone)

Adversary Method



Give algorithm a **superposition of inputs**

Consider bipartite state: (1) input and (2) algorithm workspace

Initially, these systems are **unentangled**

By end, must be **highly entangled**

Argue entanglement can't increase much by one query

Applying This To Search

Let Y_i = input with i^{th} bit 1, all others 0

Feed algorithm $\frac{1}{\sqrt{n}}\sum_i |Y_i\rangle$ as input

Keep track of density matrix ρ of **input** part

Initial ρ**:**

$$\begin{bmatrix} \frac{1}{n} & \mathrm{L} & \frac{1}{n} \\ \mathrm{M} & & \mathrm{M} \\ \frac{1}{n} & \mathrm{L} & \frac{1}{n} \end{bmatrix}$$

Final ρ**:**

$$\begin{bmatrix} \frac{1}{n} & & \frac{\pm\varepsilon}{n} \\ & \mathrm{O} & \\ \frac{\pm\varepsilon}{n} & & \frac{1}{n} \end{bmatrix}$$

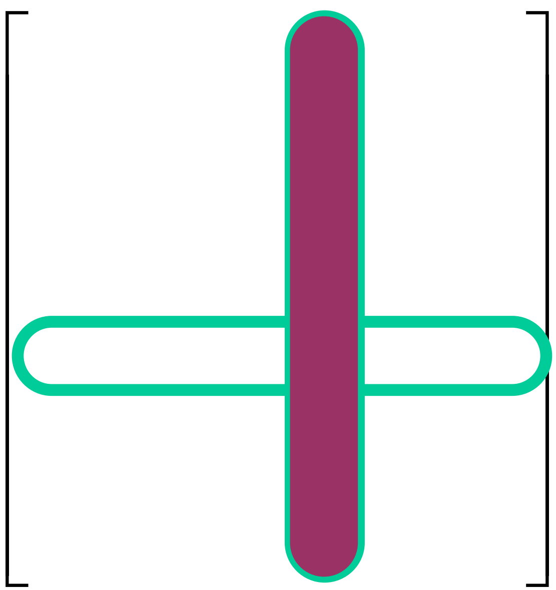
Off-diagonal entries must be small

Let $S = \sum_{i \neq j} \rho_{ij}$ be sum of off-diagonal entries

S = N-1 initially. By end, need (say) S ≤ N/3

Claim: A query can decrease S by at most O(√N)

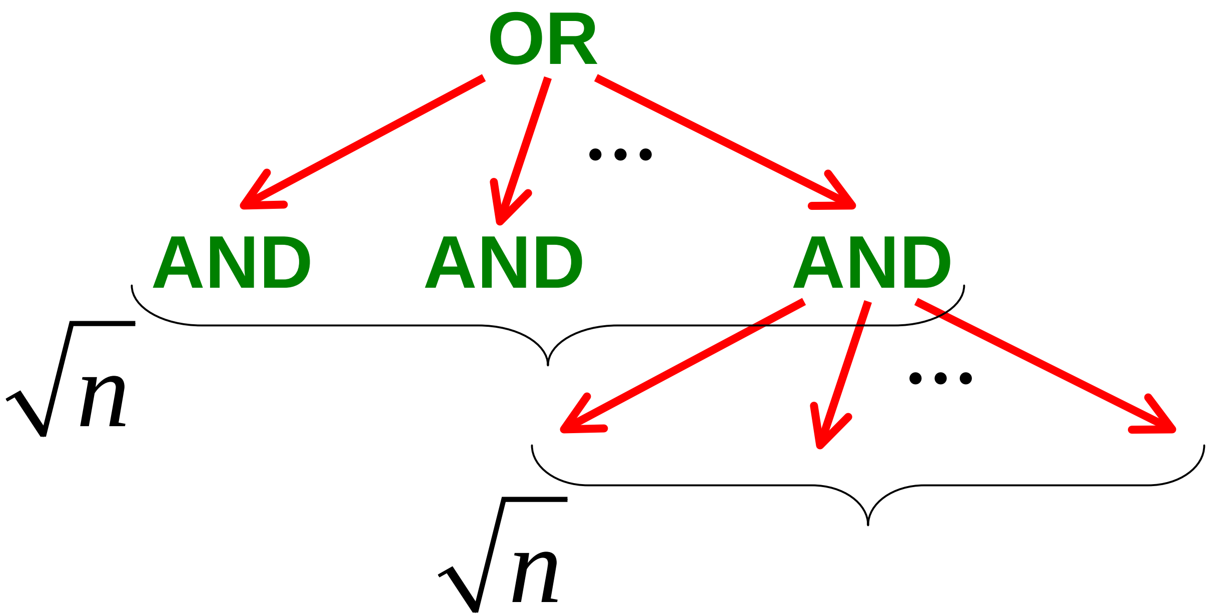
Proof: Decompose ρ into pure states, one for each basis state |i,z⟩ of algorithm part

$|\psi_{i,z}\rangle\langle\psi_{i,z}| =$ 

Querying x_i only affects i^{th} row and i^{th} column

By Cauchy-Schwarz, each row or column sums to at most √n

Depth-2 Game-Tree Search



"Recursive Grover" gives $Q(GameTree_n) = O\left(\sqrt{n \log n}\right)$

With polynomial method, only know how to get

$Q(\text{GameTree}_n) = \Omega(n^{1/4})$

Adversary method gives $Q(\text{GameTree}_n) = \Omega(\sqrt{n})$

Inverting A Permutation

5 2 1 7 4 6 3

Problem: Find the 1

Could this be easier than ordinary search?

Hybrid method gives $Q(\mathrm{Invert}_n) = \Omega(n^{1/3})$

Adversary method gives $Q(\mathrm{Invert}_n) = \Omega(\sqrt{n})$

Collision Problem

- Given $X = x_1 \ldots x_n : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\}$
- **Promised:**

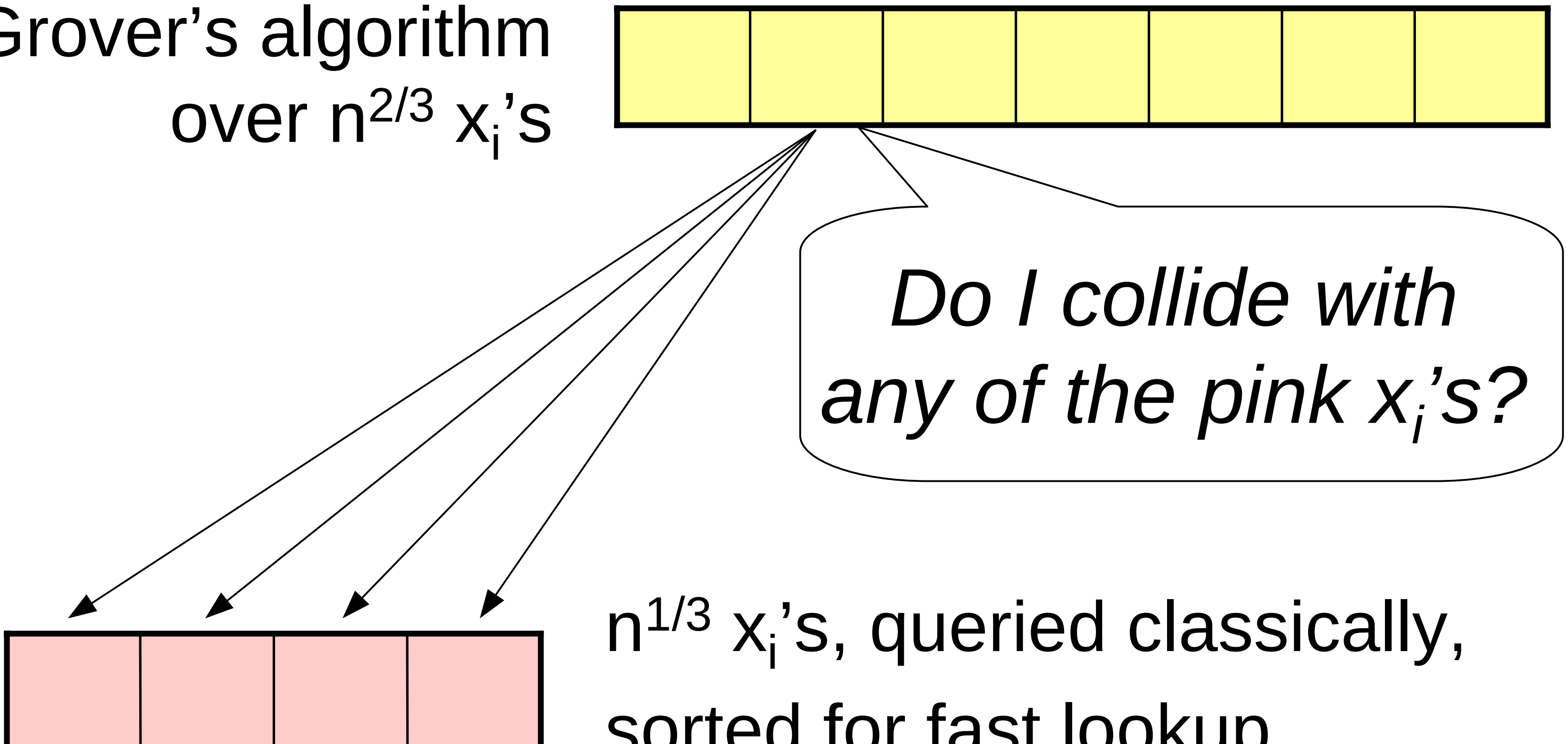
  (1) X is one-to-one (permutation) or

  (2) X is two-to-one
- **Problem:** Decide which using few queries to the x_i
- $R(\text{Collision}_n) = \Theta(\sqrt{n})$

Brassard-Høyer-Tapp (1997)

$O(n^{1/3})$ quantum alg for collision problem

Grover's algorithm over $n^{2/3}$ x_i's



$n^{1/3}$ x_i's, queried classically, sorted for fast lookup

Result

- $Q(\text{Collision}_n) = \Omega(n^{1/5})$ (A 2002)
- Shi 2002 improved to $\Omega(n^{1/4})$

  $\Omega(n^{1/3})$ when $|\text{range}| \geq 3n/2$
- Previously no lower bound better than $\Omega(1)$
- Why so much harder than search?

Cartoon Version of Proof

Imagine feeding algorithm g-to-1 functions, where g could be greater than 2

Let P(g) = expected probability that algorithm outputs "2-to-1" when given random g-to-1 function

Crucial Lemma: P(g) is a polynomial in g, with deg(P)$\leq$2T (where T = number of queries)

P(g)$\in$[0,1] for integers g, and P'(g)$\geq$1/3 for some g$\in$[1,2]. So we can use Markov's inequality

Caveat: What does "g-to-1 function" mean if g doesn't divide n? (Related to why argument breaks down for g>$\sqrt{}$n)

~~There are no good open problems left in quantum lower bounds~~

BULL

In the collision problem, suppose the function $X:\{0,1\}^n \rightarrow \{0,1\}^n$ is 1-to-1 rather than 2-to-1.

Can you give me a polynomial-size quantum certificate, by which I can verify that fact in polynomial time?

We know $Q(f) = \Omega(R(f)^{1/6})$ for Boolean f defined on all 2^n inputs. Can we show a similar bound for f defined on $1-\varepsilon$ fraction of inputs?

Would be large step toward

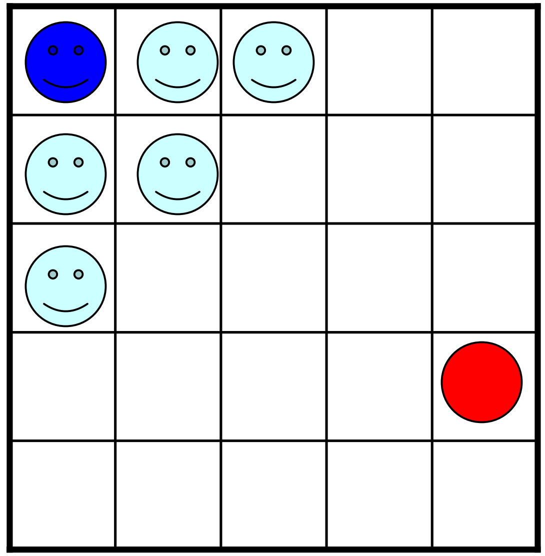
Conjecture: If $BPP^A \neq BQP^A$ for a random oracle A with probability 1, then $BPP \neq BQP$

Suppose that wh… our quantum computer mak… placing $|i\rangle$ by $|i\rangle|x_i\rangle$—the $|x_i\rangle$ …ed immediately. Can still … finding in this model, but not … search

PHYSICALLY MOTIVATED

Is there any total function for which we get a speedup over classical?

Quantum computer



Marked item

Suppose inputs to Grover's algorithm are arranged in a $\sqrt{n}$-by-$\sqrt{n}$ grid. Our quantum computer has unbounded memory, but to move the 'read' head one square takes unit time.

Can we search in less than $\Theta(n)$ time?