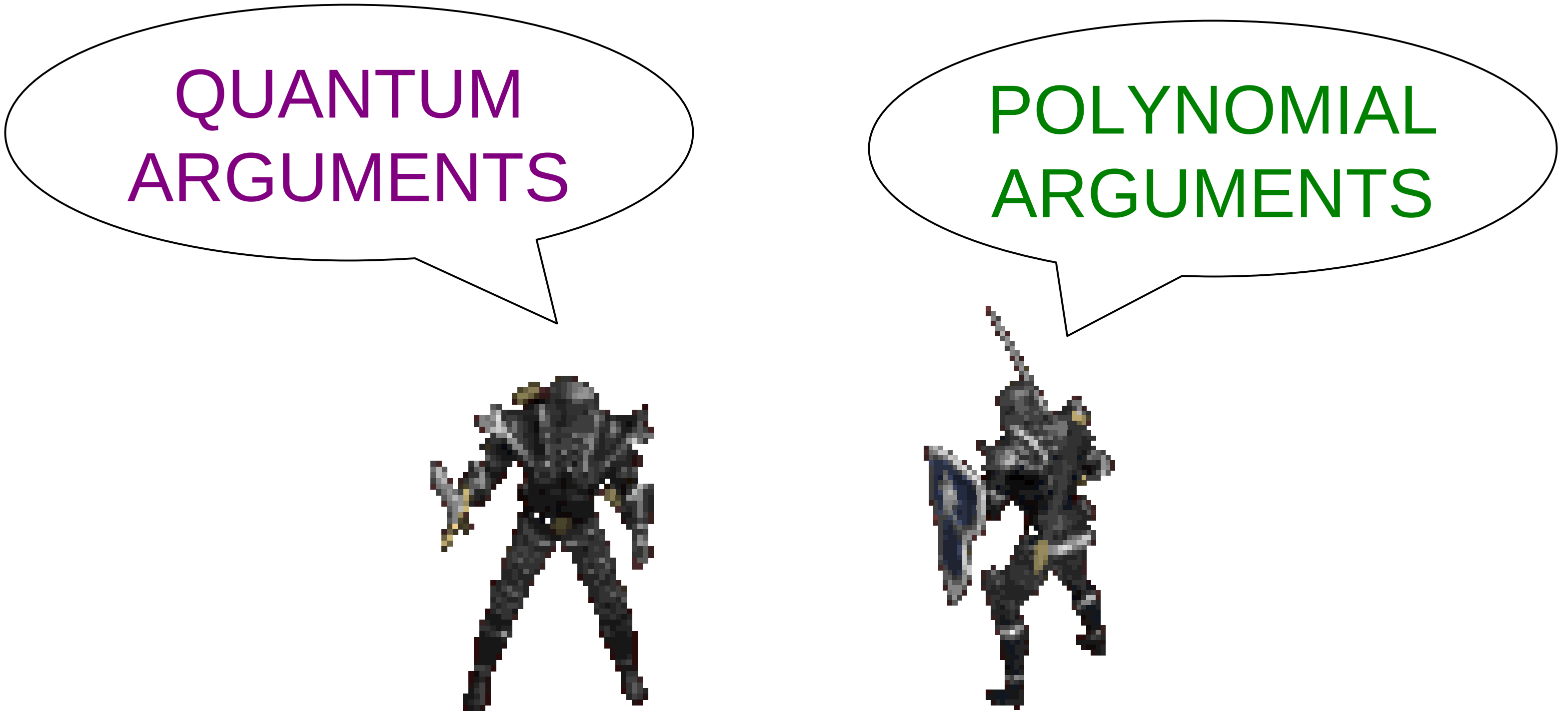
Quantum Lower Bounds You probably Haven't Seen Before

(which doesn't imply that you don't know OF them)

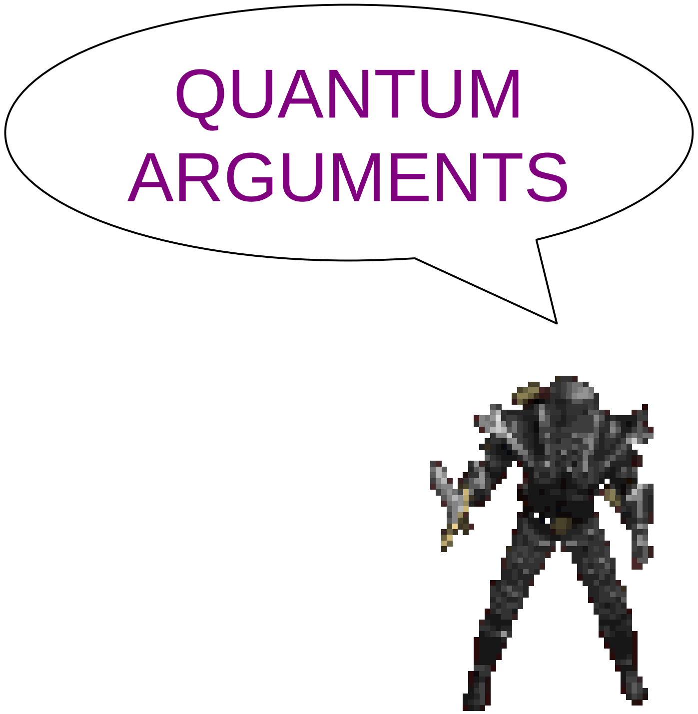
Scott Aaronson, UC Berkeley

9/24/2002

A History of Quantum Lower Bounds

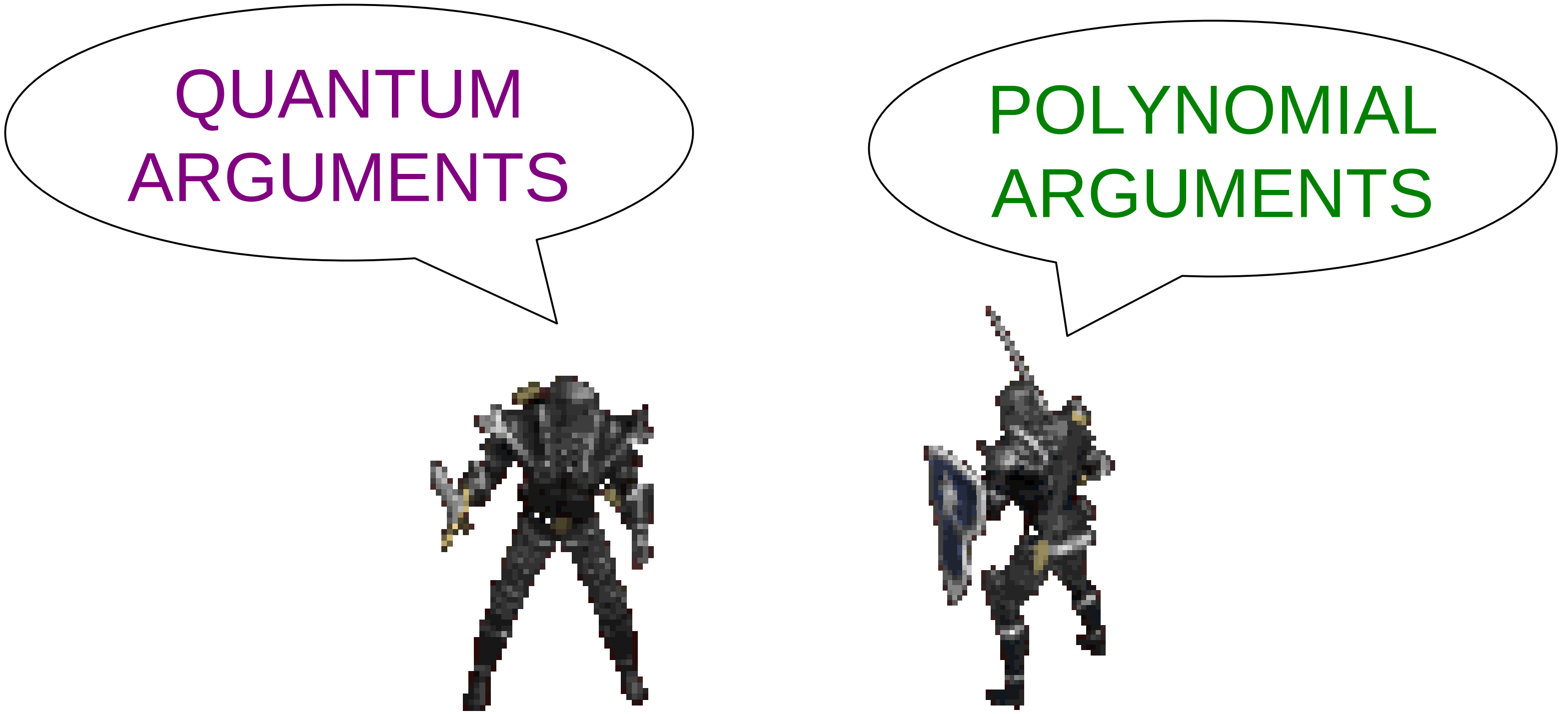


A History of Quantum Lower Bounds



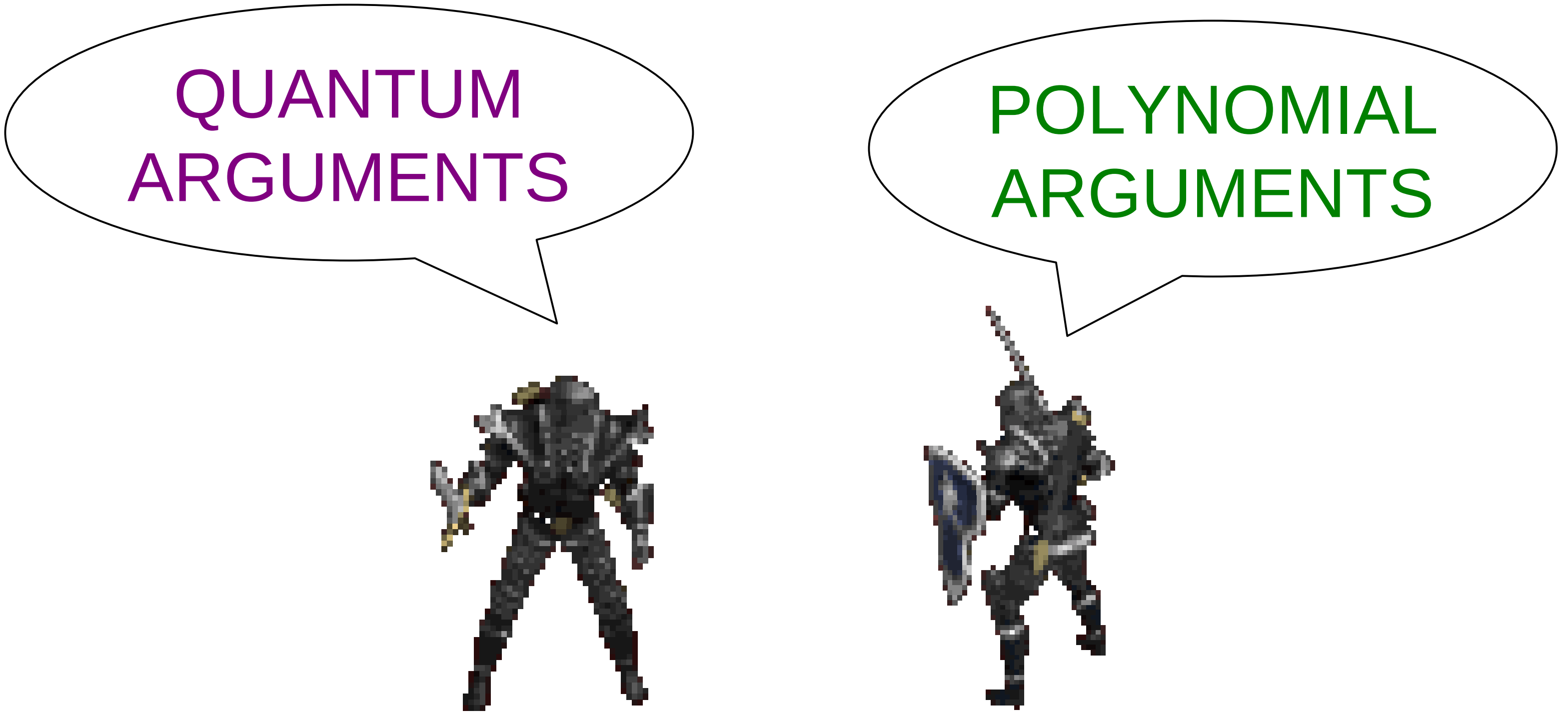
BBBV'94: $\Omega(\sqrt{n})$ lower bound for searching a list of n elements (i.e. Grover's algorithm is optimal)

A History of Quantum Lower Bounds



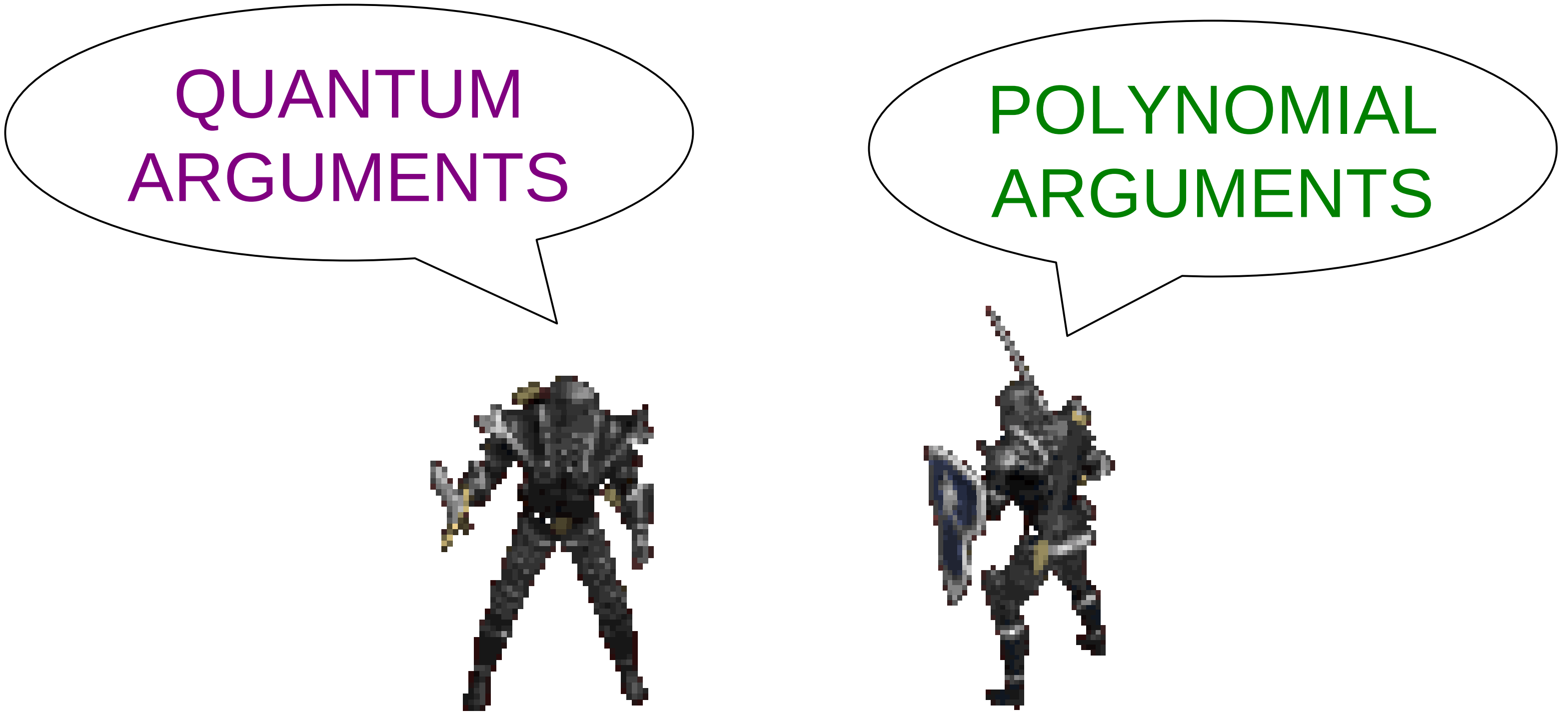
BBCMW'98: $\Omega\left(\sqrt{(k+1)(n-k)}\right)$ bound for *any* symmetric Boolean function f(|X|) with f(k)≠f(k+1)

A History of Quantum Lower Bounds



Ambainis'00: $\Omega(\sqrt{n})$ bounds for evaluating an AND-OR tree and for finding the '1' in a permutation

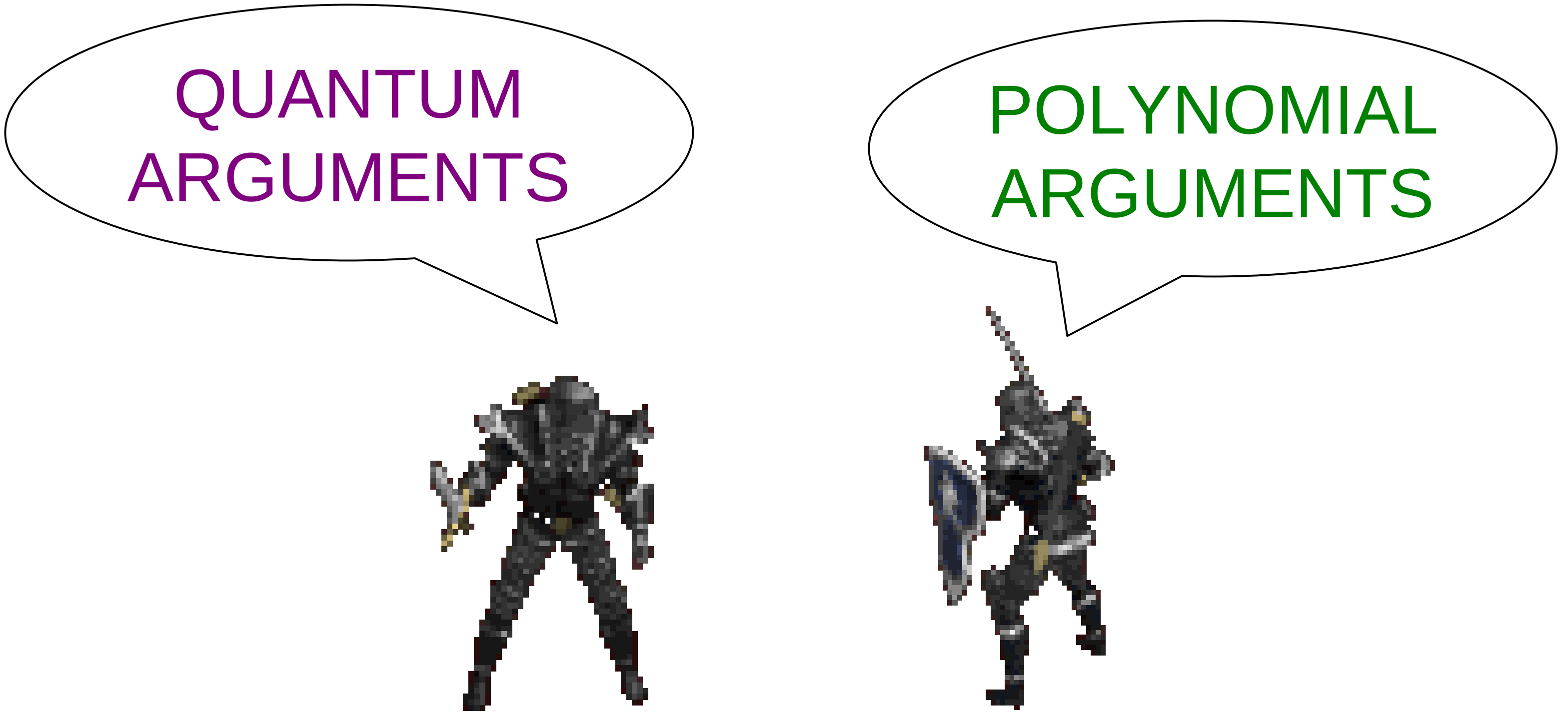
A History of Quantum Lower Bounds



A'02: $\Omega(n^{1/5})$ bound for the collision problem (deciding whether f:{1…n}→{1…n} is 1-to-1 or 2-to-1)

Shi'02: $\Omega(n^{1/3})$ bound for collision with large range, $\Omega(n^{2/3})$ for element distinctness

A History of Quantum Lower Bounds



Other results, including what I'll talk about today

True

Henceforth polynomial arguments shall be used for highly symmetric problems and for zero-error bounds, and quantum arguments otherwise.

Whosoever disobeys, must post to quant-ph.

Talk Outline

1. Quantum Certificate Complexity

2. Recursive Fourier Sampling

3. Query Complexity & Quantum Gravity
   (special treat for Dave Bacon)

Quantum Certificate Complexity

Background

$f:\{0,1\}^n \rightarrow \{0,1\}$ is a total Boolean function

$D(f)$	(deterministic query complexity)
$\geq R_0(f)$	(zero-error randomized)
$\geq R_2(f)$	(bounded-error randomized)
$\geq Q_2(f)$	(bounded-error quantum)
$\leq Q_0(f)$	(zero-error quantum)
$\leq Q_E(f)$	(exact quantum)

Example

$$f = OR(x_1, \ldots, x_n)$$

$$D(OR) = n$$

$$R_0(OR) \approx n$$

$$R_2(OR) \approx \frac{1-2\varepsilon}{1-\varepsilon} n$$

$$Q_E(OR) = \Theta(n)$$

$$Q_0(OR) = \Theta(n)$$

$$Q_2(OR) = \Theta(\sqrt{n})$$

Certificate Complexity $C(f) = \max_X C^X(f)$

$C^X(f)$ = min # of queries needed to distinguish X from every Y s.t. $f(Y) \neq f(X)$

Block Sensitivity $bs(f) = \max_X bs^X(f)$

$bs^X(f)$ = max # of disjoint blocks $B \subseteq \{x_1, \ldots, x_n\}$ s.t. flipping B changes f(X)

Example: For $f = MAJ(x_1, x_2, x_3, x_4, x_5)$, letting X=11110,

[111]10	**[11][11]0**
$C^X(MAJ)=3$	$bs^X(MAJ)=2$

Randomized Certificate Complexity $RC(f) = \max_X RC^X(f)$

$RC^X(f)$ = min # of *randomized* queries needed to distinguish X from any Y s.t. $f(Y) \neq f(X)$ with ½ prob.

Quantum Certificate Complexity $QC(f)$

Example: For $f=MAJ(x_1,\ldots,x_n)$, letting $X=00\ldots0$,

$$RC^X(MAJ) = 1$$

Different notions of nondeterministic quantum query complexity: Watrous 2000, de Wolf 2002

Adversary Method
(special case)

Let D_0,D_1 be distributions over $f^{-1}(0)$, $f^{-1}(1)$ s.t.
D_0 looks "locally similar" to every 1-input, and
D_1 looks "locally similar" to every 0-input:

$$\forall X \in f^{-1}(0), i \in \{1,\ldots,n\} \qquad \Pr_{Y \in D_1}\left[x_i \neq y_i\right] \leq \alpha$$

$$\forall Y \in f^{-1}(1), i \in \{1,\ldots,n\} \qquad \Pr_{X \in D_0}\left[x_i \neq y_i\right] \leq \beta.$$

Then

$$Q_2(f) = \Omega\left(\frac{1}{\sqrt{\alpha\beta}}\right).$$

Claim: $QC(f) = \Theta\left(\sqrt{RC(f)}\right)$

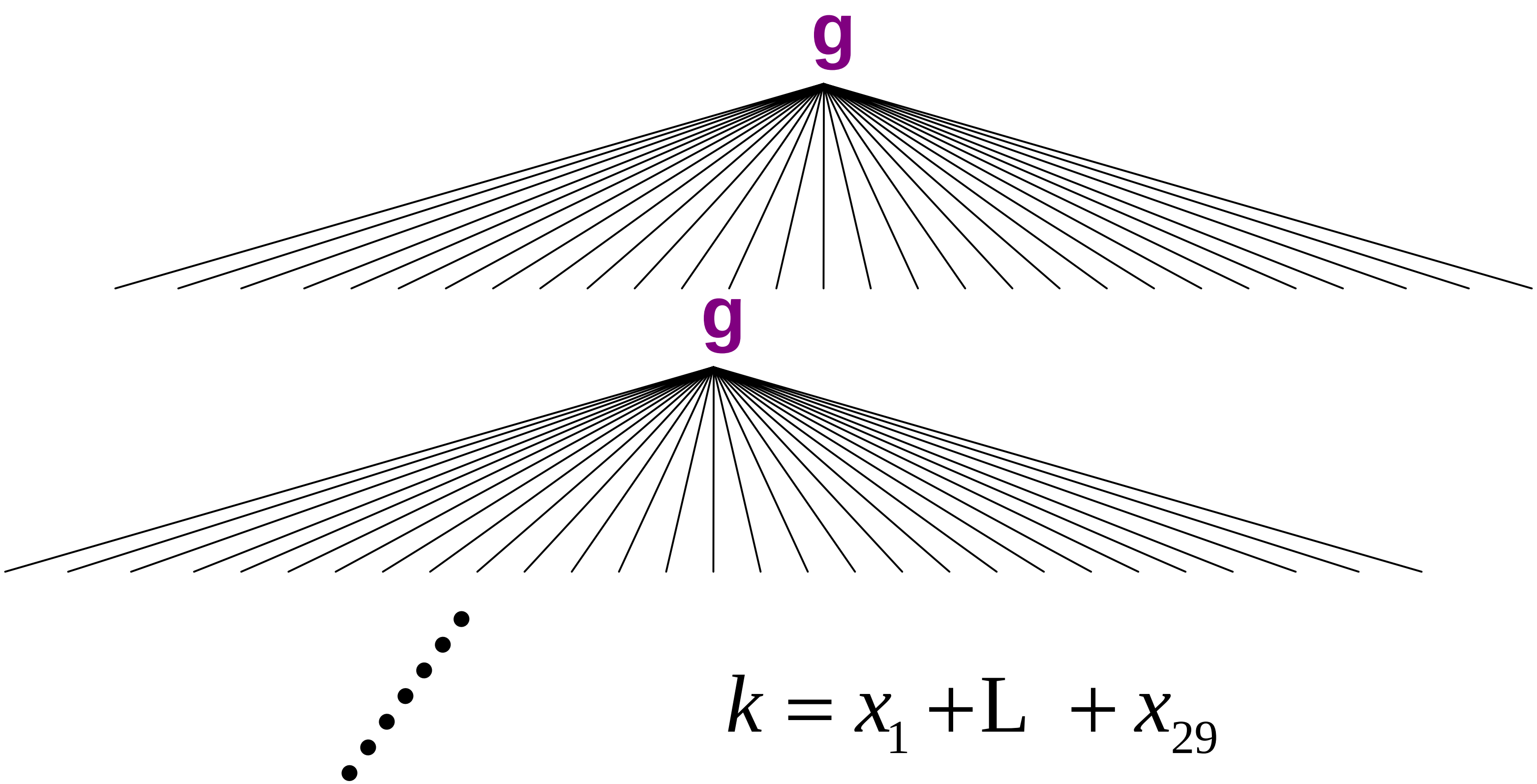
- Any randomized certificate for input X can be made *nonadaptive*

- By minimax theorem, exists distribution over {Y:f(Y)≠f(X)} s.t. for all i, $x_i \neq y_i$ w.p. O(1/RC(f))

- Adversary method then yields $\Omega\left(\sqrt{RC(f)}\right)$

- For upper bound, use “weighted Grover”

Example where $C(f) = \Theta(QC(f)^{2.205})$



$$k = x_1 + \ldots + x_{29}$$

$$g(k) = \begin{cases} 0 \text{ if } k \le 12 \\ 1 \text{ if } k = 13,14,15,16 \\ 0 \text{ if } k \ge 17 \end{cases}$$

New Quantum/Classical Relation

For total f,

$$R_0(f) = O\left(RC(f)\,ndeg(f)\log n\right)$$

$$= O\left(Q_2(f)^2\, Q_0(f)\log n\right)$$

where ndeg(f) = min degree of poly p s.t.

$p(X)\neq 0 \Leftrightarrow f(X)=1$

Previous: $D(f)=O(Q_2(f)^2 Q_0(f)^2)$ (de Wolf),
$D(f)=O(Q_2(f)^6)$ (Beals et al.)

Idea (follows Buhrman-de Wolf):

Let p be s.t. $p(X) \neq 0 \Leftrightarrow f(X)=1$

$x_1x_2 - x_2 + 2x_3$: x_1x_2, $2x_3$ are "maxonomials"

Nisan-Smolensky: For every 0-input X and maxonomial M of p, X has a sensitive block whose variables are all in M

Consequence: Randomized 0-certificate must intersect each maxonomial w.p. $\geq$ ½

Randomized algorithm: Keep querying a randomized 0-certificate, until either one no longer exists or p=0

Lemma: O(ndeg(f) log n) iterations suffice w.h.p.

Proof: Let S be current set of monomials, and

$$\omega(S) = \sum_{M \in S} \deg(M)!$$

Initially $\omega(S) \leq n^{ndeg(f)}$ ndeg(f)!

We're done when $\omega(S)=0$

Claim: Each iteration decreases $\omega(S)$ by expected amount $\geq \omega(S)/4e$

Reason: $\geq 1/e$ of $\omega(S)$ is concentrated on maxonomials, each of which decreases in degree w.p. $\geq$ ½

Recursive Fourier Sampling

(quant-ph/0209060)

Fourier Sampling

Given A:{0,1}^{n}→{0,1}

Promise: A(x)=s·x(mod 2) for some s

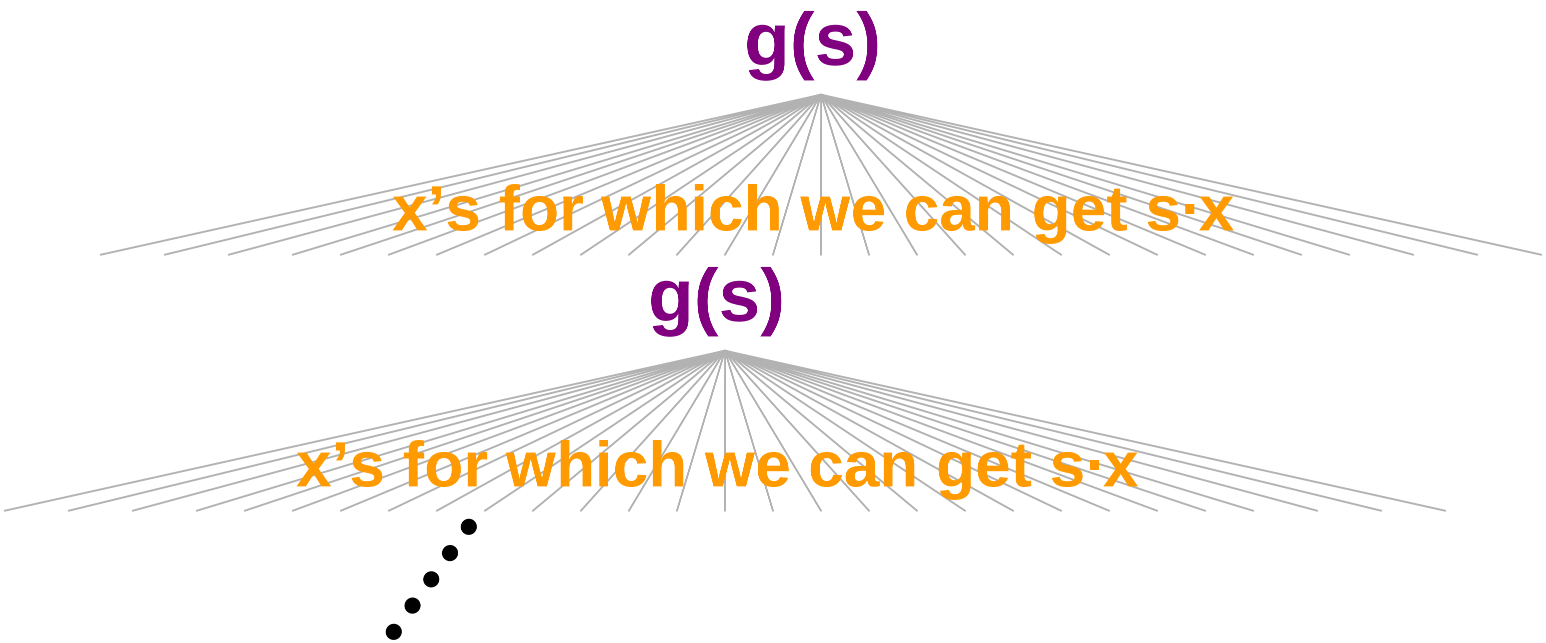
Return: g(s), for some known g:{0,1}^{n}→{0,1} (possibly partial)

Classically: n queries needed

Quantumly: 2 queries

$$2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{A(x)} |x\rangle \xrightarrow{H_2^{n}} |s\rangle$$

Recursive Fourier Sampling (RFS)



Fourier sampling composed log n times

Classically: $n^{\log n}$ queries

Quantumly: $2^{\log n} = n$ queries—or fewer?

Overview

- **Bernstein-Vazirani 1993:** RFS puts BQP $\not\subset$ MA relative to oracle
- Candidate for BQP $\not\subset$ PH
- Could it put (say) BQP $\not\subset$ PH[polylog]?
- **Is uncomputing necessary? Why?**
- **Goal:** Show $Q_2(\text{RFS}) = \Omega(c^d)$ for $c>1$
  d = tree depth
- **Trouble:** Suppose g(s) is a parity function
  Then $Q_2(\text{RFS}_g) = 1$

Plan of Attack

- We define a **nonparity coefficient** of the function g,

  $\mu(g) \in [0, 3/4]$

- Measures how uncorrelated g is with parity of any subset of input bits

  Examples: $\mu(\text{Parity})=0$, $\mu(\text{Mod } 3)=3/4-O(1/n)$

- We then prove a lower bound:

$$Q_2\left(RFS_g\right) = \Omega\left(\left(\frac{1}{1-\mu(g)}\right)^{(\log n)/2}\right)$$

- If $\mu(g)$ is close to 0, this bound is useless. But we show that **if $\mu(g)<0.146$ then g is a parity function**

The Nonparity Coefficient μ(g)

Max μ* s.t. for some distributions D_0 over $g^{-1}(0)$,
D_1 over $g^{-1}(1)$,

for all $z \neq 0^n$, $t_0 \in g^{-1}(0)$, $t_1 \in g^{-1}(1)$,

$$\Pr_{s_0 \in D_0,\, s_1 \in D_1}\left[s_0 \cdot z \equiv t_1 \cdot z \pmod{2} \vee s_1 \cdot z \equiv t_0 \cdot z \pmod{2} \right] \geq \mu^*$$

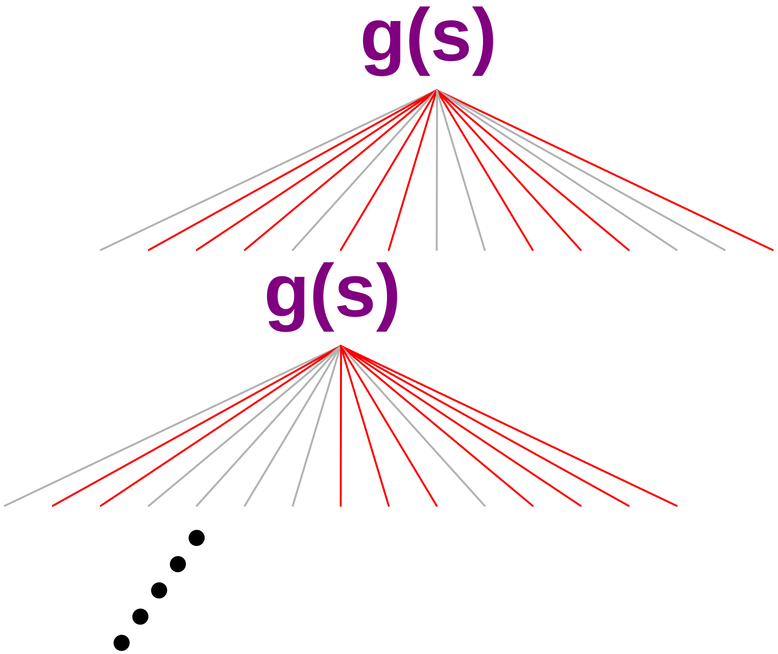
Theorem: $$Q_2\left(RFS_g\right)=\Omega\left(\left(\frac{1}{1-\mu(g)}\right)^{(\log n)/2}\right)$$

Proof Idea: Uses Ambainis' "most general" bound

Let $(x,y)\in R$ if $x\in f^{-1}(0)$, $y\in f^{-1}(1)$ **"differ minimally"**

Weight inputs by D_0,D_1 from nonparity coefficient

Then for all i and $(x^*,y^*)\in R$,



$$\Pr_{x\in D_0\,:\,(x,y^*)\in R}\left[x_i\neq y_i^*\right]\Pr_{y\in D_1\,:\,(x^*,y)\in R}\left[x_i^*\neq y_i\right]\leq(1-\mu)^h$$

“Pseudoparity” Functions Don’t Exist

Theorem: If $\mu(g) < \frac{2-\sqrt{2}}{4} \approx 0.146$

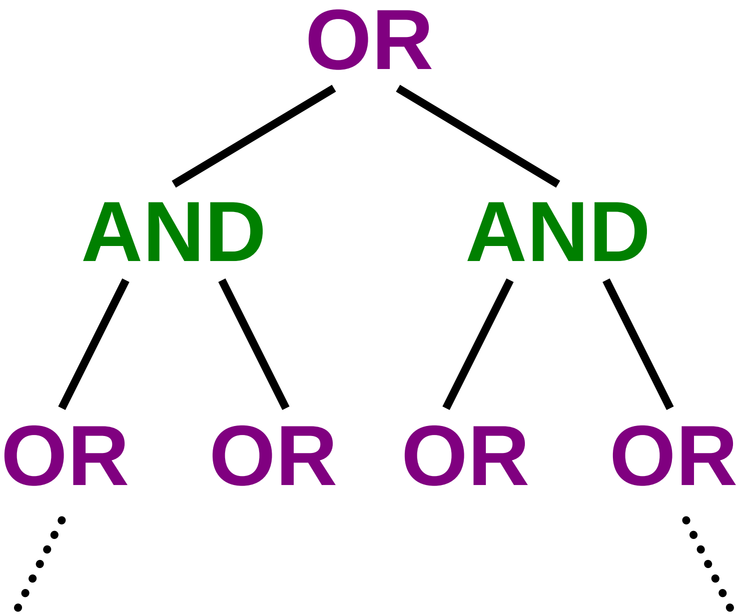
then μ(g)=0 (i.e. g is a parity function)

So either

(1) the adversary method gives a good quantum lower bound, or

(2) there exists an efficient classical algorithm

In general, when can we do better for tree functions than by recursing on subtrees?

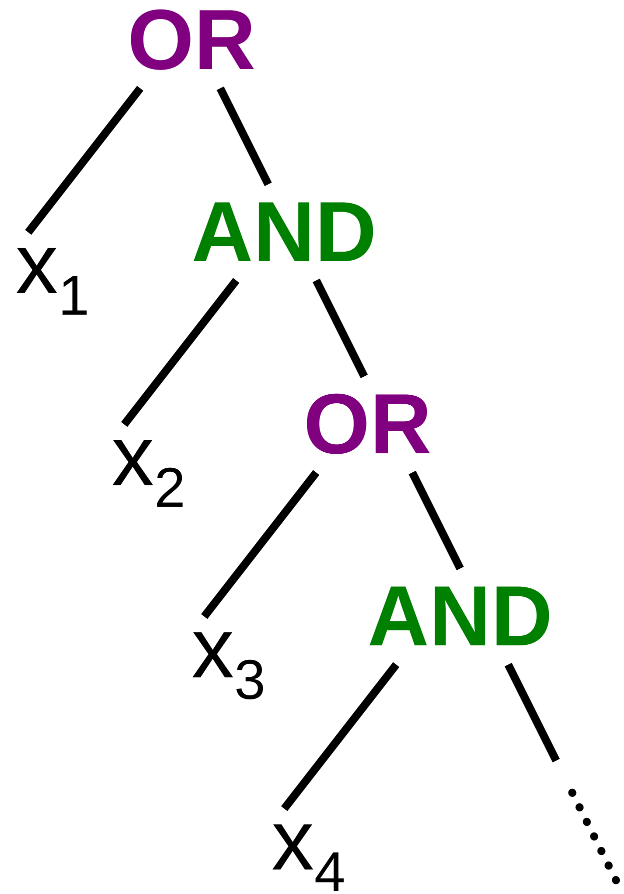


$$R_2(f) = \Theta\left(n^{0.753}\right)$$

(Saks-Wigderson, Santha)

$$Q_2(f) = \Omega\left(\sqrt{n}\right)$$

(Barnum-Saks: holds for any AND-OR tree)

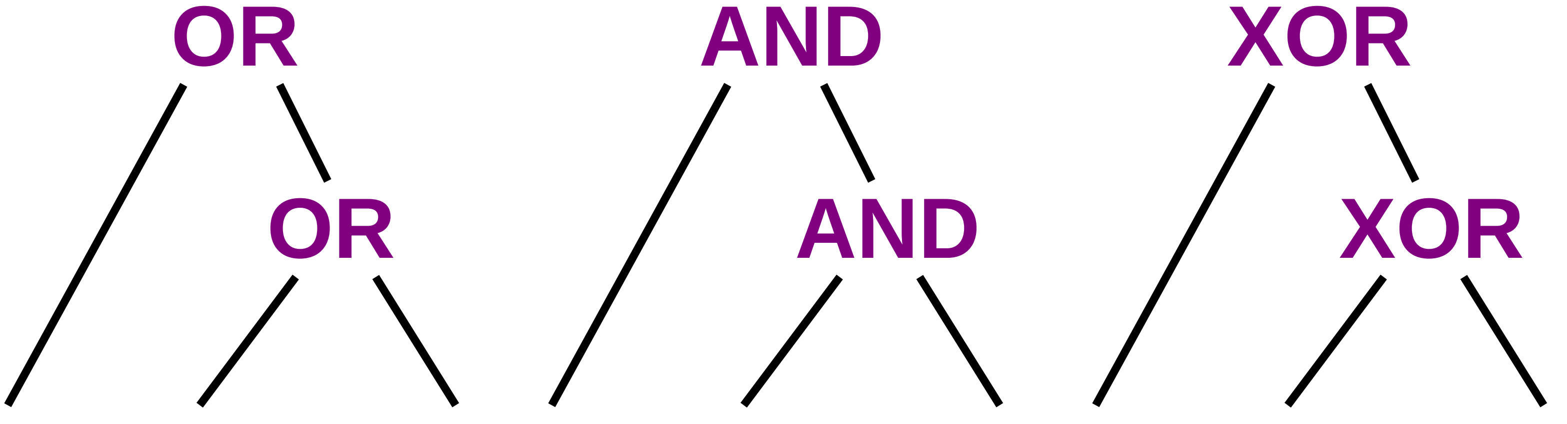


$$Q_2(f) = \Theta\left(\sqrt{n}\right)$$

(Dürr-Høyer)

Does every Boolean function *have* a unique tree?

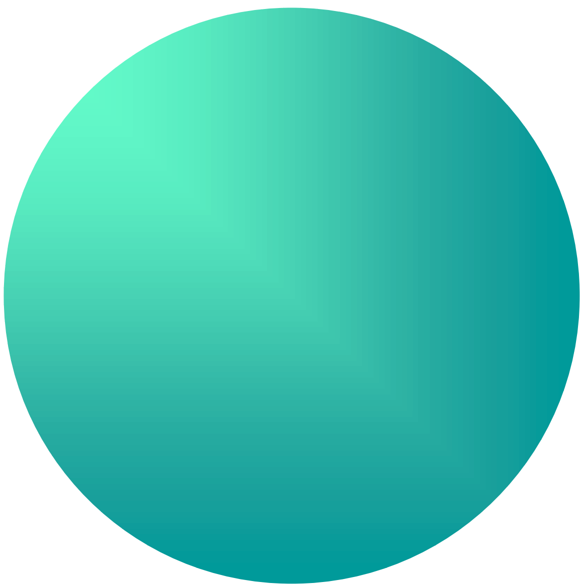
Theorem (A'2000): Yes, modulo three "degeneracies" …



Query Complexity & Quantum Gravity

The Holographic Principle

(‘t Hooft, Susskind, Bekenstein, Bousso…)



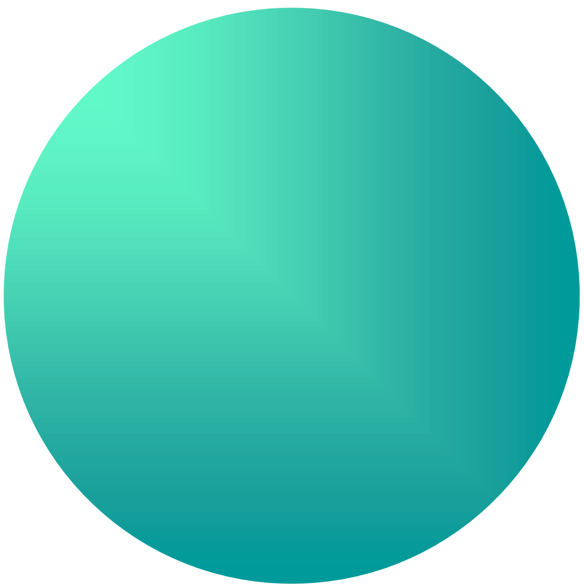
$$N \leq \frac{A}{4 \ln 2}$$

A = surface area of 3D region (in Planck areas, 7.1×10^{-70} m^2)

N = # of bits it contains

Tight for black holes

The Query Complexity Holographic Principle

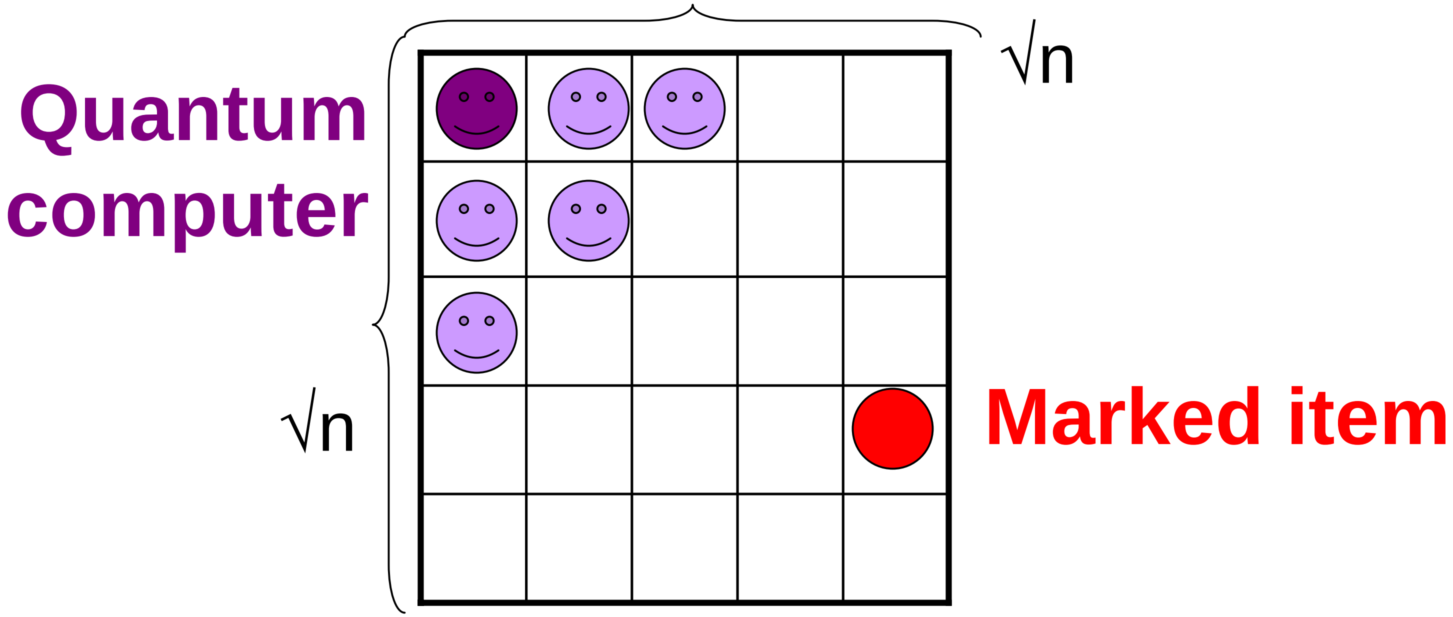


$$T = O(A)$$

A = surface area of 3D region

T = time needed to search it for a marked item (given finite speed of light)

Grover Search on a 2D Lattice



- Can do in $O(n^{3/4})$ time: searching a row classically takes $\sqrt{n}$ time; combining the results using Grover takes $n^{1/4}\cdot\sqrt{n}$

- In d dimensions, can do in $O(n^{1/2+1/2d})$

- Implies "query complexity holographic principle"—when d=3, $n^{1/2+1/6}=n^{2/3}$ is O(A), in the case where A is minimized (a sphere)

- **Conjecture:** $n^{1/2+1/2d}$ is optimal. Would imply "holographic" bound is tight for spheres (such as black holes…)