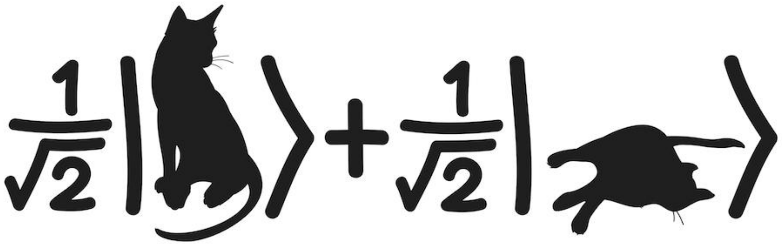
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

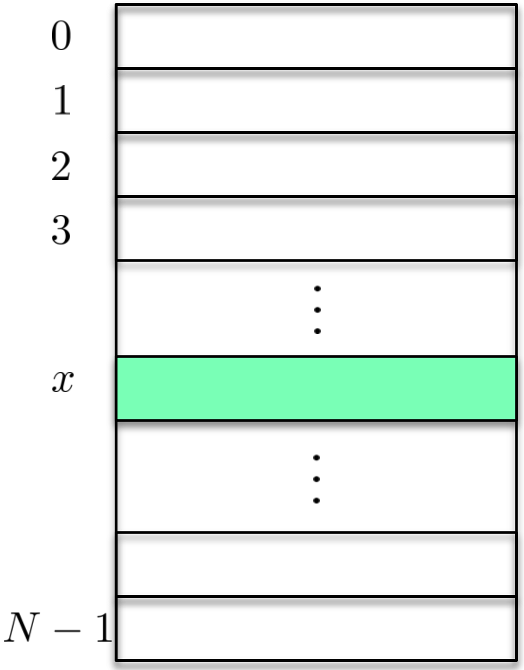


Lecture 16: Quantum Complexity Theory

Lower bound for quantum search

Unstructured search

"Digital haystack"

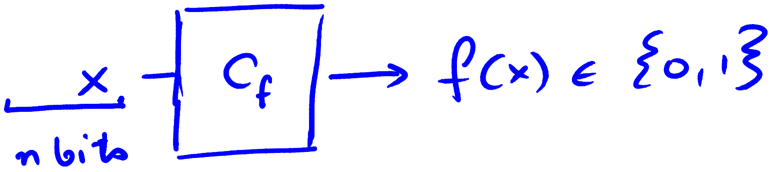


$N = 2^n$

Goal: Search for the marked entry.

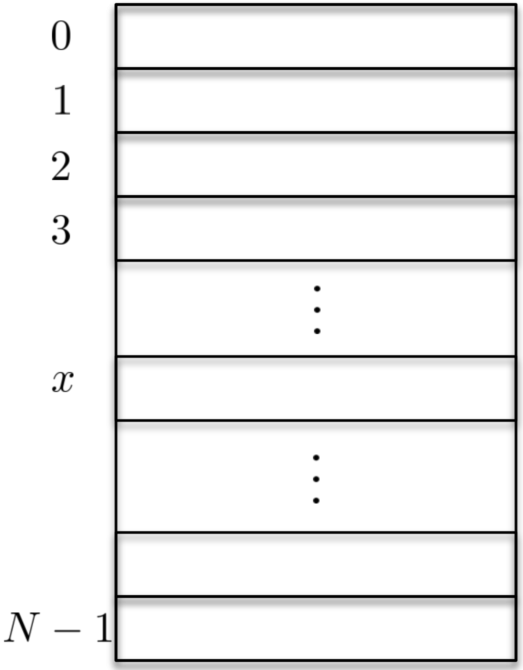
Theorem: Any quantum algorithm must take at least √N time. queries

$= 2^{n/2}$



Unstructured search

"Digital haystack"



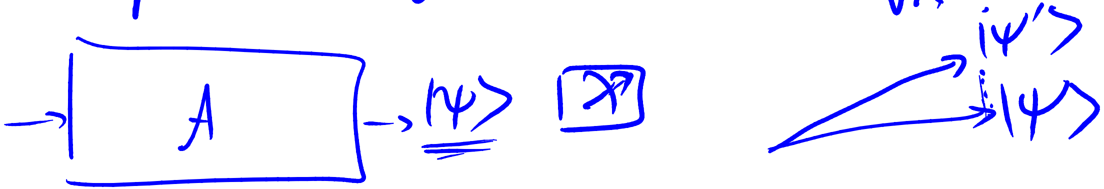
1 quantum query: no algorithm can guarantee success probability > c/N.

Perform test run with empty haystack.
Suppose algorithm makes query

$$\sum_x \alpha_x |x\rangle \qquad \sum |\alpha_x|^2 = 1 \qquad |\alpha_x|^2 \le \frac{1}{N}.$$

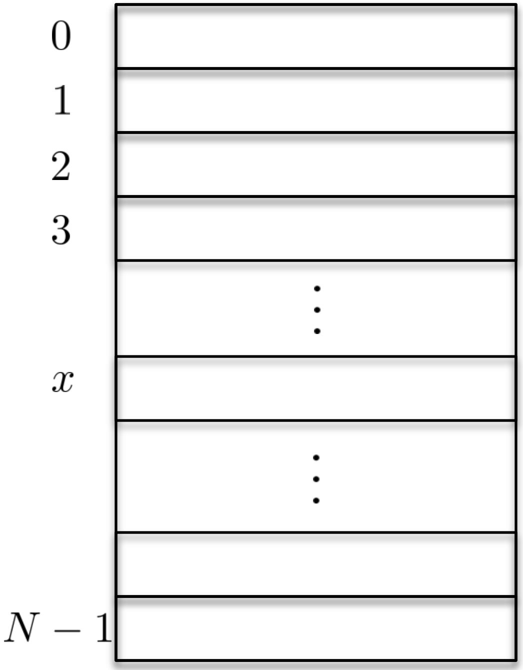
Place needle in location that gets queried with minimum squared amplitude.

amplitude queries $x^* \le \frac{1}{\sqrt{N}}$



Unstructured search

"Digital haystack"



t quantum queries:

Quantum Alg: t steps

$P[\text{success}] = \frac{O(t^2)}{N}$.

Perform test run with empty haystack.

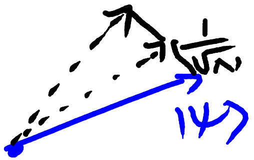
Place needle in location that gets queried with minimum squared amplitude.

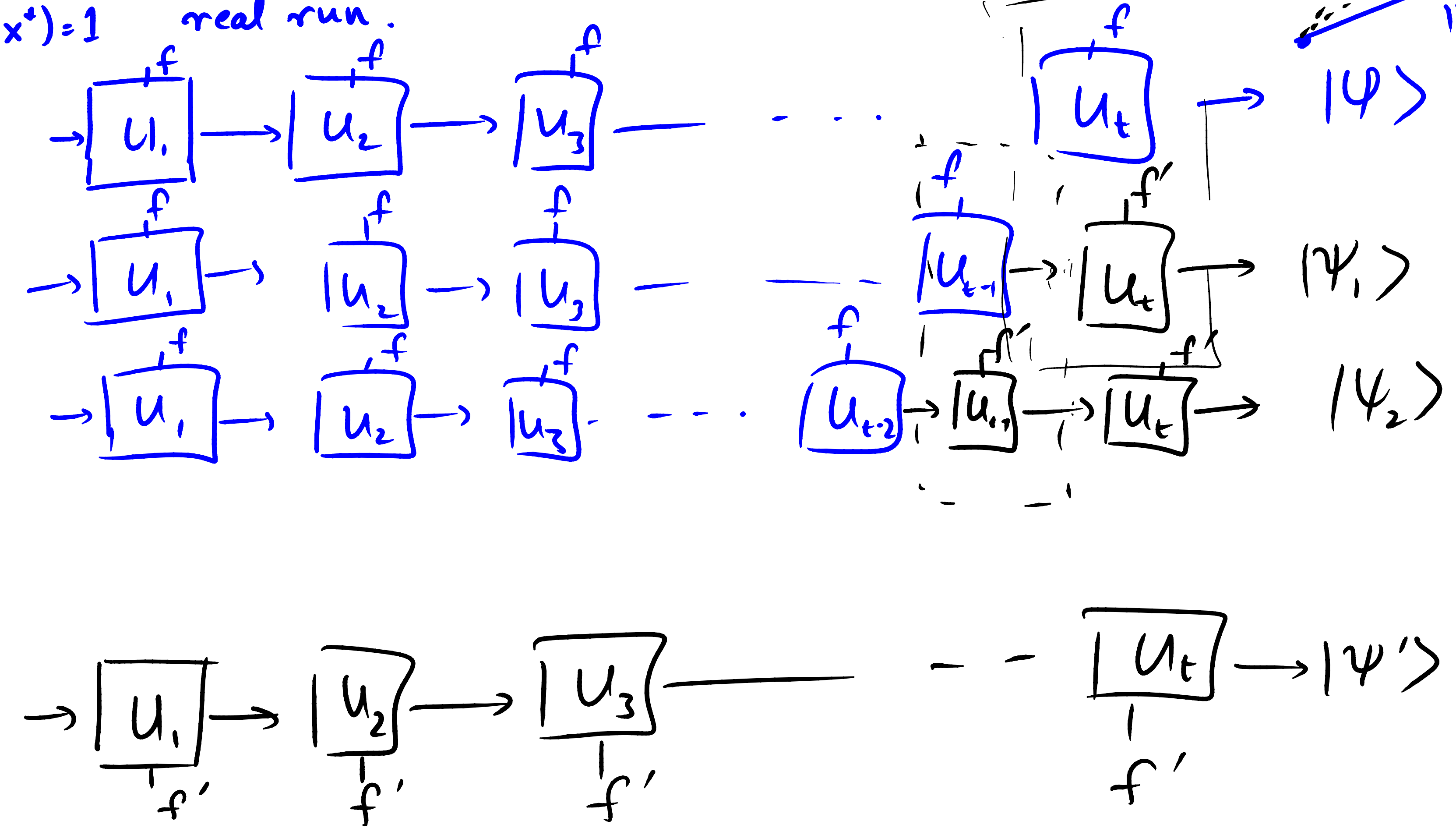
But subsequent queries amplitudes can change depending on previous answers.

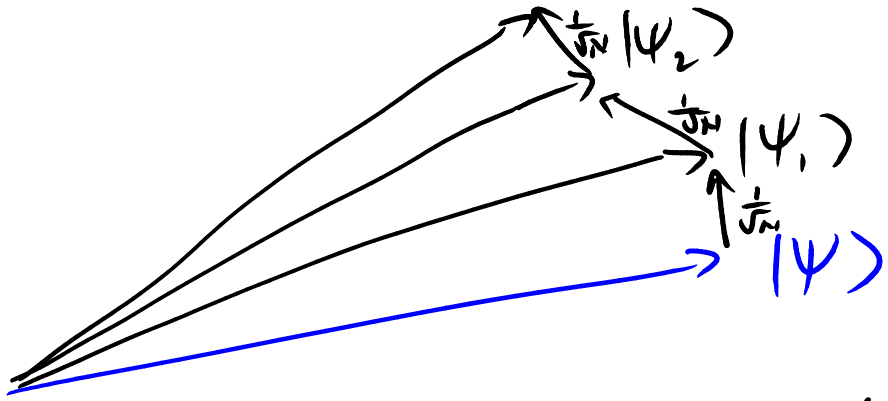
Hybrid Argument

$f \equiv 0$ test run.

$f'(x^*) = 1$ real run.







test run.

$$\frac{t}{\sqrt{N}}$$

Prob changes by $O\left(\frac{t^2}{N}\right)$.

Does this mean quantum computers cannot solve NP-complete problems in polynomial time? No.

Not necessarily. But it does mean that any quantum algorithm must use the structure of the problem.

[Farhi, et. al. Science 2001] Framework of adiabatic quantum optimization. Simulations on small examples seemed to show polynomial time for random instances of 3SAT.

http://arxiv.org/pdf/quant-ph/0001106v1.pdf

Isn't this ruled out by previous lowerbound?

Economist.com

Quantum computing

Orion's belter

Feb 15th 2007 | VANCOUVER

From *The Economist* print edition

The world's first practical quantum computer is unveiled

AS CALIFORNIA is to the United States, so British Columbia is to Canada. Both are about as far south-west as you can go on their respective mainlands. Both have high-tech aspirations. And, although the Fraser Valley does not yet have quite the cachet of Silicon Valley, it may be about to steal a march on its southern neighbour. For, on February 13th, D-Wave Systems, a firm based in Burnaby, near Vancouver, announced the existence of the world's first practical quantum computer.

Economist.com

Exponential Speedup for NP-Complete Problems?

Quantum computing

Orion's belter

Feb 15th 2007 | VANCOUVER

From *The Economist* print edition

Quantum computers provide a neat shortcut to solving a range of mathematical tasks known as NP-complete problems. They do so by encoding all possible permutations in the form of a small number of "qubits". In a normal computer, bits of digital information are either 0 or 1. In a quantum computer these normal bits are replaced by a "superposition" (the qubit) of both 0 and 1 that is unique to the ambiguous world of quantum mechanics. Qubits have already been created in the laboratory using photons (the particles of which light is composed), ions and certain sorts of atomic nuclei. By a process known as entanglement, two qubits can encode four different values simultaneously (00, 01, 10 and 11). Four qubits can represent 16 values, and so on. That means huge calculations can be done using a manageable number of qubits. In principle, by putting a set of entangled qubits into a suitably tuned magnetic field, the optimal solution to a given NP-complete problem can be found in one shot.

Adiabatic Quantum Optimization

$H_0 \longrightarrow H_f$

Gradually transform:

$H(t) = (1-t)H_0 + tH_f$

$|\psi_0\rangle$ Known ground state

$|\psi_f\rangle$ output

E_0 = ground energy

E_1 = 1st excited "

$g = E_1 - E_0$

- How fast? $T = \frac{1}{Min_t\, g(t)^2}$ where g(t) is the difference between 2 smallest eigenvalues of H(t)

3SAT as a local Hamiltonian Problem

$$f(x_1,\cdots,x_n) = c_1 \wedge \cdots \wedge c_m \qquad H_f = H_1 + H_2 + \cdots + H_m$$

- n bits ---> n qubits
- Clause $c_i = x_1 \vee x_2 \vee x_3$ corresponds to 8x8 Hamiltonian matrix acting on first 3 qubits:

$$h_i = \begin{bmatrix} 1 & & & & & & & \\ & 0 & & & & & & \\ & & 0 & & & & & \\ & & & 0 & & & & \\ & & & & 0 & & & \\ & & & & & 0 & & \\ & & & & & & 0 & \\ & & & & & & & 0 \end{bmatrix}$$

- Satisfying assignment is eigenvector with evalue 0.
- All truth assignments are eigenvectors with eigenvalue = # unsat clauses.

- How fast? $T = \frac{1}{Min_t \; g(t)^2}$ where g(t) is the difference between 2 smallest eigenvalues of H(t)

- Adiabatic optimization gives quadratic speedup for search, but exponential time in general: http://arxiv.org/pdf/quant-ph/0206003v1.pdf

- Exponential time for NP-complete problems, but can tunnel through local optima in certain special circumstances: http://ww2.chemistry.gatech.edu/~brown/QICS08/reichardt-adiabatic.pdf

- Anderson localization based arguments that it typically gets stuck in local optima: http://arxiv.org/pdf/0912.0746.pdf