Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 14: Quantum Complexity Theory

Limits of quantum computers

Quantum speedups for NP-Complete Problems?

Satisfiability:

Finding a solution to an NP-complete problem can be viewed as a search problem.

$$(x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_5 \vee x_6) \wedge \cdots$$

Is there a configuration of $x_1, x_2, \cdots$ that satisfy the above formula?

There are 2^n possible configurations.

$N = 2^n$

Quantum speedups for NP-Complete Problems?

Satisfiability:

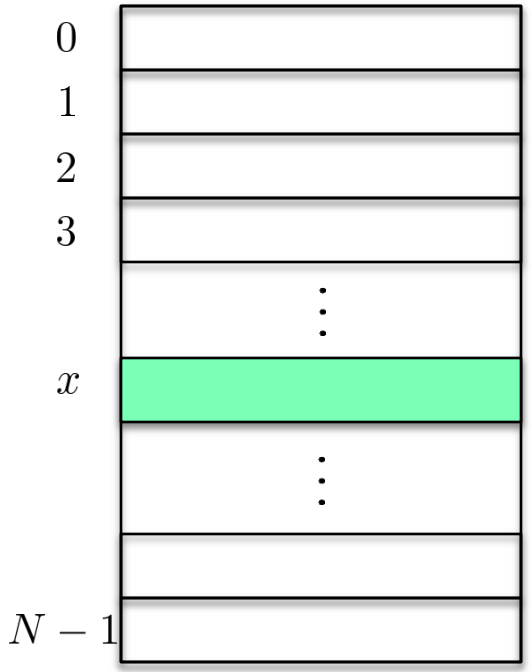
Finding a solution to an NP-complete problem can be viewed as a search problem.

$$(x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_5 \vee x_6) \wedge \cdots$$

Is there a configuration of $x_1, x_2, \cdots$ that satisfy the above formula?

There are 2^n possible configurations.

"Digital haystack"

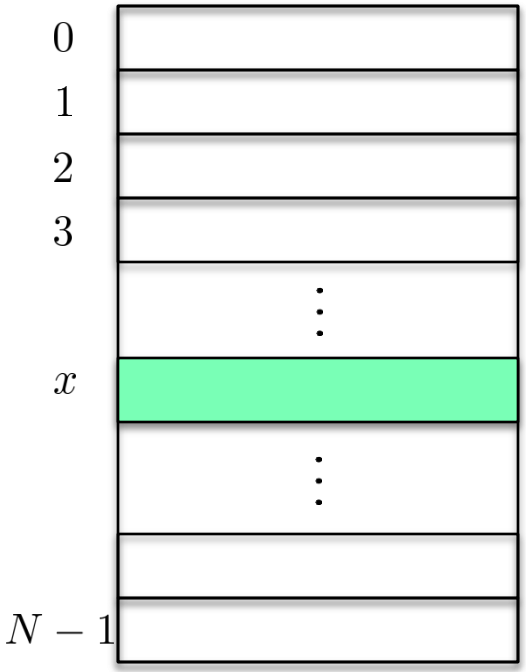


$O(\sqrt{N})$
$= O(2^{n/2})$

N = 2^n

Unstructured search

"Digital haystack"



Grover's Algorithm: Quantum algorithm for unstructured search that takes $O(\sqrt{N})$ time.

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

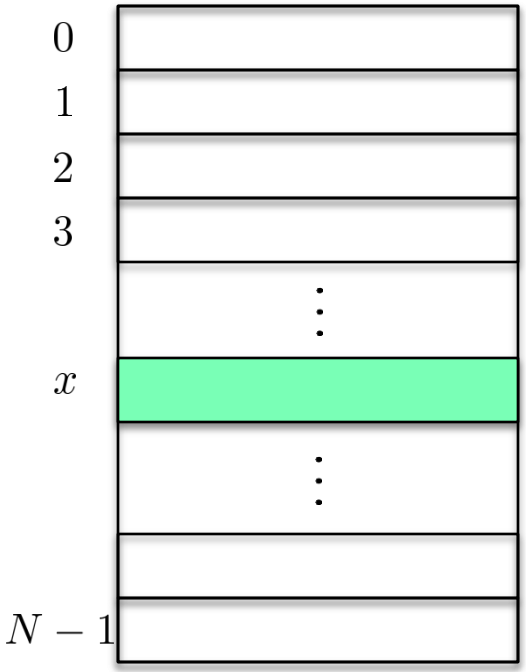
Feb 15th 2007 | VANCOUVER

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.

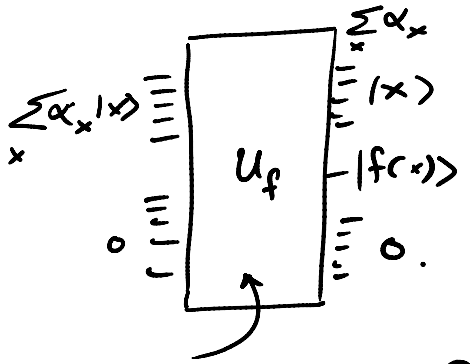
Unstructured search

"Digital haystack"



Theorem: Any quantum algorithm must take at least $\geq c \cdot \sqrt{N}$ time.

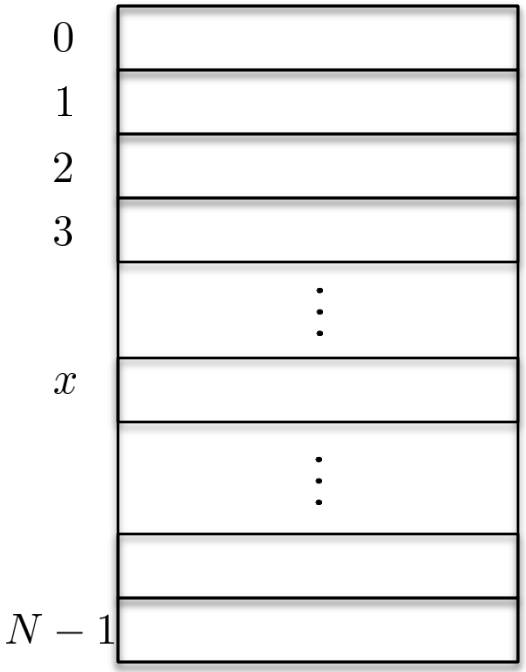
$f : \{0, \ldots, N-1\} \to \{0, 1\}$.



Related Problem $\exists x : f(x) = 1$?

Unstructured search

"Digital haystack"



$\forall x \quad f(x) = 0$ $\quad \sum_x \alpha_x(t)\,|x\rangle$

t quantum queries: $\sum_x |\alpha_x(t)|^2$ total query magnitude.

Perform test run with empty haystack.

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

$f^*(x) = 1$ where x^* minimizes $\sum_{t=1}^{T} |\alpha_{x^*}(t)|^2$.

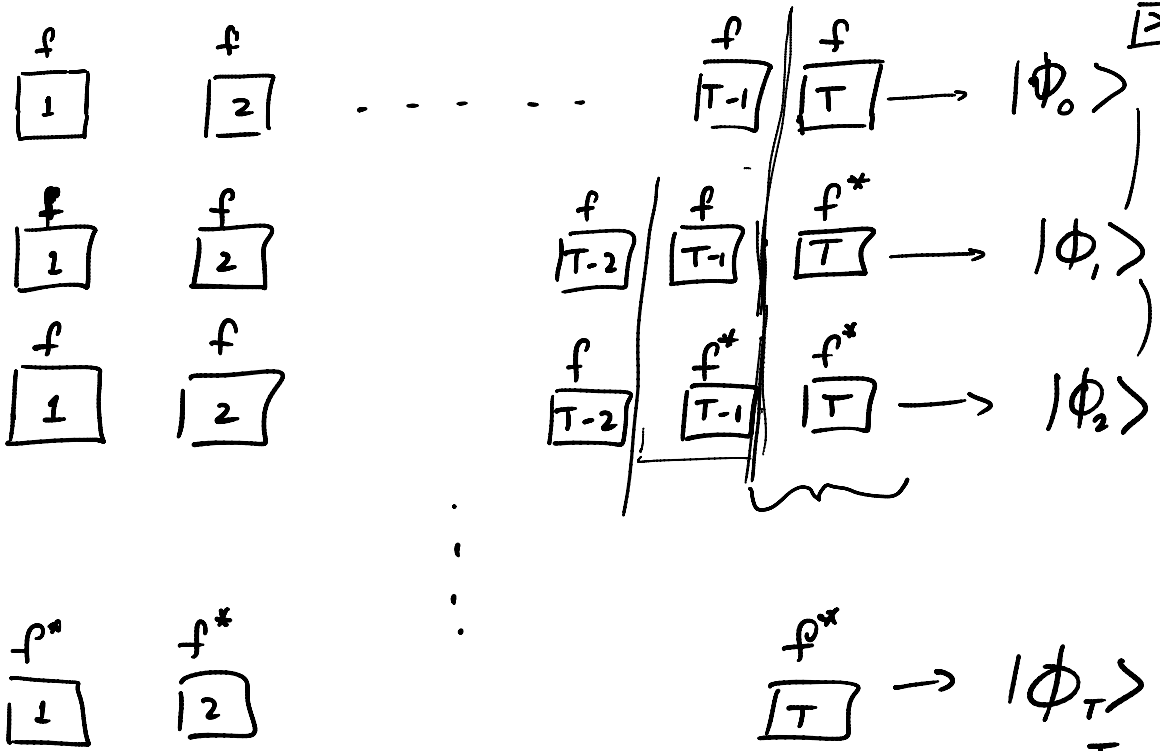
But subsequent queries amplitudes can change depending on previous answers.

$P[\text{algorithm correct on } f^*] = O\left(\frac{T^2}{N}\right)$

$T \ll \sqrt{N}$.

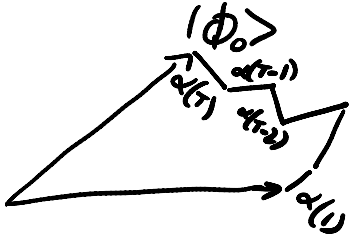
Hybrid Argument:

x^* o whp



$|\alpha_{x^*}(T)|$

$|\alpha_{x^*}(T-1)|$



$$|\alpha(1)| + |\alpha(2)| + \cdots + |\alpha(T)| \leq \frac{T}{\sqrt{N}}$$

$$\sum_{t=1}^{T} |\alpha(t)|^2 \leq \frac{T}{N}$$

$T \sim \sqrt{N}$ to get constant prob success.

Quantum Mechanics & Quantum Computation

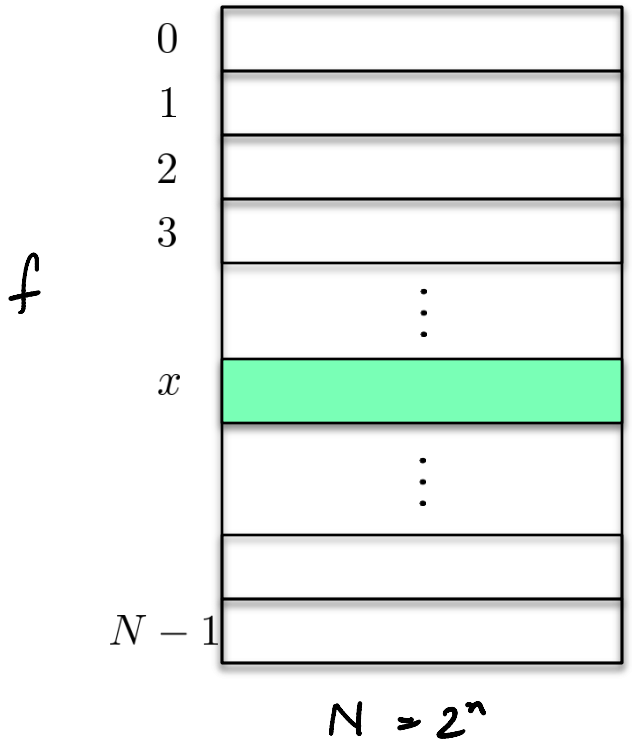
Umesh V. Vazirani
University of California, Berkeley

Lecture 14: Quantum Complexity Theory

Adiabatic Quantum Computation

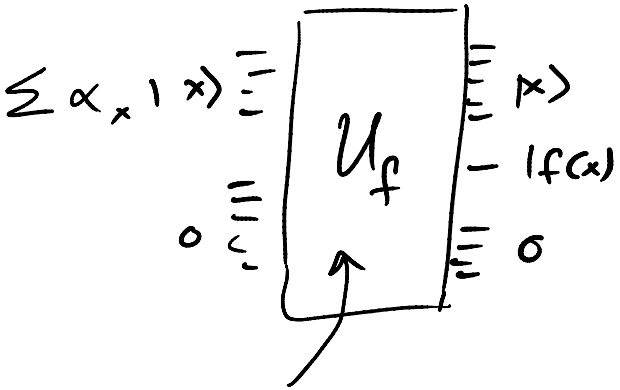
Unstructured search

"Digital haystack"



Theorem: Any quantum algorithm must take at least $\sqrt{N}$ time.

$= 2^{n/2}$



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

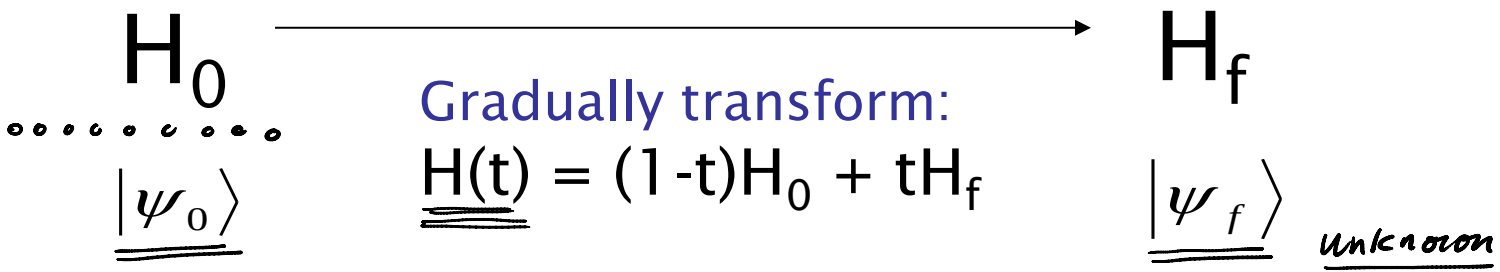
Not necessarily. But it does mean that any quantum algorithm must use the structure of the problem.

[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?

Adiabatic Quantum Optimization



Adiabatic Theorem: slowly enough then track ground state.

- 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

$$f(x_1, \cdots, x_n) = c_1 \wedge \cdots \wedge c_m$$

$$H = h_1 + h_2 + \cdots + h_m$$

- 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:

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

- 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)

Grover's Alg.

- 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

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.

D-Wave sells first commercial quantum computer

June 1, 2011 by Lisa Zyga weblog

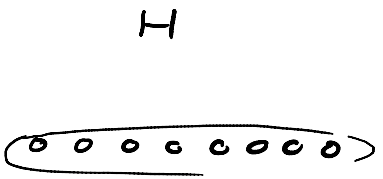
Dr. Geordie Rose, CTO and co-founder of D-Wave Systems, with the D-Wave One system. Image credit: D-Wave.

(PhysOrg.com) -- Last week, Burnaby, British Columbia-based company D-Wave Systems, Inc., announced that it sold its first commercial quantum computer. Global security company Lockheed Martin, based in Bethesda, Maryland, bought the quantum computer for a rumored $10 million, which includes maintenance and other services for several years.

Lockheed Martin communications manager Thad Madden said that the company spent a year reviewing the computer, called the D-Wave One, before purchasing it. The company plans to use the computer to build "cyber-physical systems," which integrate software with environmental sensors.

Lockheed Martin communications manager Thad Madden said that the company spent a year reviewing the computer, called the D-Wave One, before purchasing it. The company plans to use the computer to build "cyber-physical systems," which integrate software with environmental sensors.

The announcement comes just a few weeks after D-Wave researchers published a paper in *Nature* describing **how D-Wave's devices work**, using a process called quantum annealing. The paper demonstrated quantum behavior in a system with eight qubits made from superconducting loops, by showing that (classical) thermal fluctuations could not be responsible for flipping the qubits' spins.



D-Wave One uses 16 of these eight-qubit cells in its 128-qubit chip. However, due to the complexity of the 128-qubit chip, some experts in the quantum computing field are still not fully convinced that D-Wave's commercial system works with quantum effects.

"There is an enormous gap between demonstrating some kind of quantum effect in eight qubits, as they have done here, and saying that they have a 128-qubit chip that can perform a computationally interesting task faster than a conventional computer," Scott Aaronson, a computer scientist at MIT, told *Nature News*.

The sale to Lockheed Martin is not the first time that D-Wave has worked with the technology industry. In 2009, D-Wave partnered with Google to develop software that can recognize automobiles within images. Some cell phones now use the machine-learning algorithms created by D-Wave's computers.

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 14: Quantum Complexity Theory

BQP

P
polynomial time

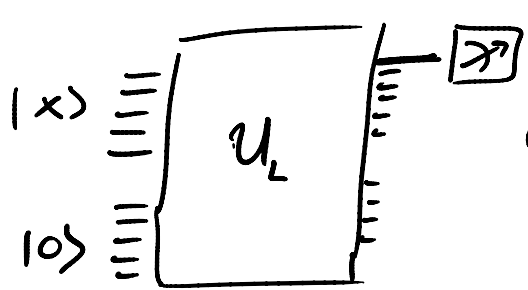
BPP
probabilistic
polynomial time.

BQP

Input x
Output Yes/No.

Primality.
SAT
$L = \{x : \text{answer yes}\}$
$L_{\text{primality}} = \{x : x \text{ is prime}\}$.

$L \in BQP$ if there is a sequence of quantum ckts



$\begin{cases} 1 & \text{wp} \geq \frac{2}{3} \quad \text{if } x \in L \\ 0 & \text{wp} \geq \frac{2}{3} \quad \text{if } x \notin L. \end{cases}$

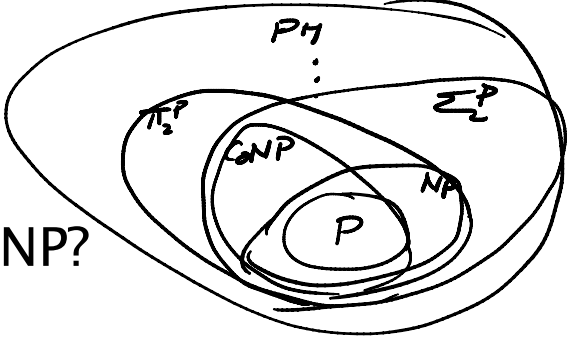
gates in U_L $= O(\text{poly}(n))$.

$$P \subseteq \underline{\underline{BPP}} \overset{?}{\subseteq} BQP \subseteq PSPACE.$$

? UI ??

NP

$$P = PSPACE \ ?$$



Could BQP contain problems much outside NP?

BQP vs PH: central open question in quantum complexity.

Conjecture (1993): Recursive Fourier sampling $\notin$ PH

New conjecture: [Aaronson 09] Fourier checking $\notin$ PH
http://www.scottaaronson.com/papers/bqpph.pdf

v, w random unit vectors in R^N $N= 2^n$
Distinguish f = sgn(v) & g = sgn(Hv) from f = sgn(v) & g = sgn(w)
Where f,g:$\{0,1\}^n \rightarrow \{1,-1\}$