Quantum Computing: Solving Complex Problems

David DiVincenzo, IBM

Fermilab Colloquium, 4/2007
Rules for quantum computing


Consider this form of two-bit boolean logic gate:

\[
\begin{array}{cccc}
1 & x & x & 1 \\
0 & y & y & 1 \\
\end{array}
\]

add the bits mod 2

= “controlled-NOT” (CNOT)
Rules for quantum computing


Quantum rules of operation :

\[
|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)
\]

one-qubit rotations – create superpositions

\[
\psi_{in} = \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle)
\]

\[
\psi_{out} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)
\]

“controlled-NOT” (CNOT)

Creation of entanglement
Fast Quantum Computation

P. Shor, AT&T, 1994

Classical factoring problem required 8 months on hundreds of computers

RSA 129
1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541

Factors
3490529510847650949
1478496199038981334
1776463849338784399
0820577

x
3276913299326670954
996198819834461413
1776429679929425397
98288533

Same Input and Output, but Quantum processing of intermediate data gives

Exponential speedup
for Factoring

Quadratic speedup
for Search
Physical systems actively considered for quantum computer implementation

- Liquid-state NMR
- NMR spin lattices
- Linear ion-trap spectroscopy
- Neutral-atom optical lattices
- Cavity QED + atoms
- Linear optics with single photons
- Nitrogen vacancies in diamond
- Electrons on liquid He
- Small Josephson junctions
  - “charge” qubits
  - “flux” qubits
- Spin spectroscopies, impurities in semiconductors
- Coupled quantum dots
  - Qubits: spin, charge, excitons
  - Exchange coupled, cavity coupled
Josephson junction qubit -- Saclay

Manipulating the quantum state of an electrical circuit

D. Vion, A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve and M.H. Devoret

Science 296, 886 (2002)

Oscillations show rotation of qubit at constant rate, with noise.

Where's the qubit?
Delft qubit:

- Coherence time up to $4\lambda$ sec
- Improved long term stability
- Scalable?

PRL (2004)
Simple electric circuit...

harmonic oscillator with resonant frequency
\[ \omega_0 = \frac{1}{\sqrt{LC}} \]

Quantum mechanically, like a kind of atom (with harmonic potential):

x is any circuit variable (capacitor charge/current/voltage, Inductor flux/current/voltage)

That is to say, it is a “macroscopic” variable that is being quantized.
Textbook (classical) SQUID characteristic: the “washboard”

1. Loop: inductance $L$, energy $\omega^2/L$
2. Josephson junction: critical current $I_c$, energy $I_c \cos \omega$
3. External bias energy (flux quantization effect): $\omega \Phi/L$
Textbook (classical) SQUID characteristic: the “washboard”

1. Loop: inductance $L$, energy $\omega^2/L$

2. Josephson junction:
   - critical current $I_c$,
   - energy $I_c \cos \omega$

3. External bias energy (flux quantization effect): $\omega \Phi/L$

Junction capacitance $C$, plays role of particle mass
Quantum SQUID characteristic: the “washboard”

Junction capacitance $C$, plays role of particle mass

Quantum energy levels

Josephson phase $\omega$

Energy
“Yale” Josephson junction qubit

Coherence time again c. 0.5 λs (in Ramsey fringe experiment)
But fringe visibility > 90%!
IBM Josephson junction qubit

“qubit = circulation of electric current in one direction or another (????)

Low-bandwidth control scheme for an oscillator stabilized Josephson qubit

IBM Watson Research Ctr., Yorktown Heights, NY 10598 USA
(Dated: November 16, 2004)
Good Larmor oscillations
IBM qubit
-- Up to 90% visibility
-- 40nsec decay
-- reasonable long term stability

What are they?
Integrated IBM qubit
May 2006 version

All components including junctions are integrated. Stack has two levels of metal and one crossover. Test fabrications on ordinary silicon wavers and wafers with embedded superconducting ground plane 60 um into the silicon.
Feb. 2007: D-wave systems announces 16 qubit processor

Great progress?  Hold on a minute…

They propose to use an alternative approach to quantum computing:

- 4x4 array of “flux qubits” (RF SQUIDs, tunable by flux biasing)
- DC SQUID couplers, also flux-tunable
Quantum Simulated Annealing

Adiabatic evolution of the quantum system in its ground state

Spins on a lattice, or other quantum two-level systems

Uniform transverse field

Variable out-of-plane field

Ferromagnetic exchange

Antiferromagnetic exchange

Optimization problems encodable in problem of finding lowest energy state of Ising spin glass.

Constraints on Adiabatic Computation

Possible gap scalings:

\[ \frac{1}{2^n} \]

\[ \frac{1}{(\sqrt{2})^n} \]

Very unlikely to be constant with \( n \).

Problems with small gaps:
- Landau-Zener tunneling
- Thermal excitations

\[ \frac{1}{n}, \quad \frac{1}{n^2}, \quad etc. \]
There are two ways that we can go about it. We can give up on our rule about what the computer was, we can say: Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws. Or we can turn the other way and say: Let the computer still be the same kind that we thought of before—a logical, universal automaton; can we imitate this situation? And I’m going to separate my talk here, for it branches into two parts.

4. QUANTUM COMPUTERS—UNIVERSAL QUANTUM SIMULATORS

The first branch, one you might call a side-remark, is, Can you do it with a new kind of computer—a quantum computer? (I’ll come back to the other branch in a moment.) Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements. It’s not a Turing machine, but a machine of a different kind. If we disregard

The question is, if we wrote a Hamiltonian which involved only these operators, locally coupled to corresponding operators on the other space-time points, could we imitate every quantum mechanical system which is discrete and has a finite number of degrees of freedom? I know, almost certainly, that we could do that for any quantum mechanical system which involves Bose particles. I’m not sure whether Fermi particles could be described by such a system. So I leave that open. Well, that’s an example of what I meant by a general quantum mechanical simulator. I’m not sure that it’s sufficient, because I’m not sure that it takes care of Fermi particles.
2007 Perspective:

Quantum simulation will be useful, *but* there will be limitations.
An overview of complexity

NC: logarithmic time
P: polynomial time
BPP: polynomial time, allowing for some error
NP: “nondeterministic polynomial”, answer can be confirmed in polynomial time
Classical Spin Glass: NP-complete

That is, Barahona '82:

\[ \lambda(H) \text{ is the ground-state energy.} \]

Is there a similar result for quantum spin glasses?

\[ \text{Definition 3 (ISING SPIN GLASS)} \]

Given is an interaction graph \( G = (V, E) \) with Hamiltonian

\[ H_G = \sum_{i,j \in E} J_{ij} Z_i \otimes Z_j + \sum_{i \in V} \Gamma_i Z_i. \]  

\( H_G \) is the ground-state energy.

Is there a similar result for quantum spin glasses?
Quantum complexity

MA/AM: “Merlin-Arthur” – NP with interaction
BQP: polynomial time on a quantum computer
QMA: answer can be confirmed in polynomial time on a quantum computer: quantum analog of NP
Decision Problems in Computational Complexity

Merlin.
The all-powerful prover which cannot necessarily be trusted. The goal of Merlin is to prove to Arthur that the answer to his decision problem is YES. If this can be achieved the proof is complete. If the answer is NO, Merlin can still try to convince Arthur that the answer is yes. The proof is sound if Arthur cannot be convinced.

Arthur.
A mere mortal who can run polynomial time algorithms only. Wants to solve the decision problem by possible interaction(s) with Merlin.
The bad news: finding the ground state energy of the “quantum spin glass”:

is QMA-complete. (Kitaev, Kempe, Regev, Oliveira, Terhal)

Implication: there are quantum simulation problems that we expect to be hard, even on a quantum computer.
Conclusions

-- Hardware for quantum computing is progressing steadily

-- Small working machines will be with us in the coming years

-- Simulation of hard quantum problems
   with a quantum computer is clearly possible

-- Some problems will be tractable, some intractable
   -- Progress will be empirical rather than rigorous