QUICK INTRODUCTION TO QUANTUM COMPUTING

Bob Joynt
University of Wisconsin-Madison

Funding from NSF, ARO, fabrication using MRSEC-developed facilities

QUANTUM COMPUTING

- What do people mean by it?
  - Classical bits and algorithms
  - Hard and easy problems
  - Quantum bits and algorithms
  - Coherence and entanglement
- Why are people excited by it?
  - Cryptography and factorization
  - Deutsch problem
  - Quantum factorization (Shor algorithm)
  - Other possibilities
- What are people doing about it?
  - Atoms, nuclei, Josephson junctions, floating electrons, P impurities in Si, Quantum dots
- Are they gonna get there?

$2 + 3 = 5$

A classical computer proceeds as follows:

Converts to binary notation: $10 + 11 = 101$

$f_{add} : (\{0,1\}_1^{in}, \{0,1\}_2^{in}, \{0,1\}_3^{in}, \{0,1\}_4^{in}) \rightarrow (\{0,1\}_1^{out}, \{0,1\}_2^{out}, \{0,1\}_3^{out})$

"Addition" associates a definite output configuration
(out of $2^3 = 8$ possibilities) with each of $2^4 = 16$ input configurations.

All such operations can be constructed by stringing together these three:
AND gates: $(0,0) \rightarrow (0)$, $(1,0) \rightarrow (0)$, $(0,1) \rightarrow (0)$, $(1,1) \rightarrow (1)$;
NOT gates: $(0) \rightarrow (1)$, $(1) \rightarrow (0)$;
COPY gates: $(0) \rightarrow (0,0)$, $(1) \rightarrow (1,1)$.

An algorithm is a mapping (a matrix) from the input registers to the output registers. It is composed of elementary algorithms called gates.

Easy and Hard Problems:

Addition is an EASY problem:

$I_1 + I_2 = I_3$ involves only $\log_2 I$ operations.

Adding 100-digit numbers takes less than a microsecond !

Contrast this with a problem that requires a number of operations comparable to the number itself, such as checking some property of all numbers less than I. A computer might be able to do 10^{18} operations in a month. There is no hope of ever doing 10^{100}. This would be a HARD problem !

Cryptography using Number Theory – the RSA Code

- I choose 2 large primes p and q
- Their product $N = p\,q$ is a very large number
- I choose $c < (p-1)\,(q-1)$, and reveal N and c to the public
- Your credit card number is a
- You compute $b = f(a) = a^c \pmod{N}$ and send it to me
- There is a unique number d such that

  $cd=1\ [\bmod\ (p-1)(q-1)]$ AND
- $a = b^d \pmod{N}$ – d is the key !
- d is hard to find unless I know p and q

Qubits

A qubit is a physical device that is in a linear combination of two quantum states $|0>$ and $|1>$. Think of the spin of an electron:

$$\Psi = a_0 \, |0> + a_1 \, |1>$$

Hey , this contains far more information than a classical bit, relative phase and amplitude

Furthermore, if there are N qubits:

$\Psi = a_0 \, |0>_1 \, |0>_2 \, |0>_3 \ldots |0>_N + a_1 \, |1>_1 \, |0>_2 \, |0>_3 \ldots |0>_N + \ldots + a_X \, |1>_1 \, |1>_2 \, |1>_3 \ldots |1>_N$

with $X = 2^N - 1$. This looks like a huge amount of information, but how much is really available to us?

A MEASUREMENT DESTROYS IT ALL!

Quantum Algorithms

A classical algorithm is a matrix connecting the initial and final states of the computer – this naturally suggests the evolution of a quantum system.

A quantum algorithm is just a unitary transformation on the 2^N-dimensional register space!

All quantum algorithms can be constructed by taking the product of C-NOT gate matrices:

$|0>_1 |0>_2 \quad |0>_1 |0>_2 ; |1>_1 |0>_2 \quad |1>_1 |1>_2$, etc.

BUT CAN WE DO ANYTHING WITH THEM?

Deutsch Problem

Let f answer a decision problem: if I choose A or B, what will happen: C or D? f(0 or 1) = 0 or 1. I only care about whether f(0) = f(1) or not. (Does it matter what I do ?)

$U_f : |x\rangle_1 |y\rangle_2 \rightarrow |x\rangle_1 |y + f(x)\rangle_2$

$U_f : |x\rangle_1 (|0\rangle_2 - |1\rangle_2) \rightarrow |x\rangle_1 (|f(x)\rangle_2 - |1 + f(x)\rangle_2)$

$= |x\rangle_1 (-1)^{f(x)} (|0\rangle_2 - |1\rangle_2)$

$U_f : (|0\rangle_1 + |1\rangle_1) (|0\rangle_2 - |1\rangle_2)$

$\rightarrow [(-1)^{f(0)} |0\rangle_1 + (-1)^{f(1)} |1\rangle_1] (|0\rangle_2 - |1\rangle_2)$

$\sim |0\rangle_1 + |1\rangle_1$ **if** $f(0) = f(1)$

$\sim |0\rangle_1 - |1\rangle_1$ **if** $f(0) \neq f(1)$

So now we project onto the basis $|0\rangle_1 \pm |1\rangle_1$ (measure the spin of qubit 1 along the x-axis).

We get spin in the + x-direction if f(0) = f(1) and in the - x-direction if f(0) ≠ f(1).

Quantum Parallelism: The Essence of the Matter

- The input can be in any superposition of the classical inputs, so the algorithm (function) works on all the inputs at once.
- BUT, you only get to ask one question (make one measurement) at the end.
- By choosing both the input and the measurement carefully, you may be able to find out something valuable about the function that would require many classical evaluations of the function.
- Finding the period of a function is just such a problem, and its makes possible the factorization of large numbers.

Shor Algorithm

Let N be a product of distinct primes p and q.

Classical Answer: Divide N by 2. If this doesn't work, divide by 3, and so on up to $N^{1/2}$. Prohibitively expensive for $N > 10^{40}$

Quantum Answer: Choose $a < N$ at random.

Find GCD(a,N). If GCD(a,N) = $w \neq 1$, then we are done. Else define F(x) by $F(x) = a^x \pmod N$.

Find the period r: $F(x+r) = a^{x+r} \pmod N = F(x) = a^x \pmod N$.

The period may be of order N, so this is classical hard, quantum easy.

Now $a^r = 1 \pmod N$. This says that $a^r - 1 = 0 \pmod N$, or, finally $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \pmod N$.

GCD(N, $(a^{r/2} + 1)$) is the factor.

Schemes for Implementations of Quantum Computing

- Atoms
  - Choose two convenient energy levels for qubit
  - 1-qubit operations with laser light
  - 2-qubit operations with vibrational mode coupling (ion traps) or interchange of photons (cavity QED)
- Superconductors
  - Qubit is presence or absence of flux
  - 1-qubit operations with applied field
  - 2-qubit operations with exchange of flux
- Electrons on Liquid Helium
  - Electron spin as qubit
  - 1-qubit operations with applied fields
  - 2-qubit operations with spatial overlap
- Nuclear Magnetic Resonance
  - Nuclear spins as qubits
  - 1-qubit operations with applied fields
  - 2-qubit operations by means of naturally present exchange interactions