Quantum Computation: Why the Excitement?
25 Years of Computer Science
at Gustavus Adolphus College
July 17, 2004.

E. Rieffel and W. Polak: "An Introduction to Quantum Computing for Non-Physicists"
www.arxiv.org/pdf/quant-ph/9809016

Outline

1. What can classical computers do?
2. What can quantum computers do?
3. Basis for quantum computers: superposition and entanglement
4. Related development: quantum cryptography
5. State of the art.

Classical computers:

Easy:

1. is N prime?
2. find prime N (probabilistic)
3. unstructured search

Hard:

1. factor N
2. provably secure communications

"The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers."
Bill Gates, The Road Ahead,

Quantum Computers:

First rule: “Do no harm.” Quantum computers are at least as fast as classical computers (in terms of number of operations).

Easier:

1. unstructured search (Grover’s algorithm)

Easy:

1. factor N (Shor’s algorithm; probabilistic)
2. provably secure communications

Unknown:

1. NP hard problems

Consequence: Since factoring integers is easy, RSA will no longer be safe for internet communications, so we will all have to use quantum cryptography.

Quantum Computation: qubits.

Classical bit: 0, 1 (off or on).

Qubit: polarization (state) of a photon, or electron,
corresponds to a unit vector in a 2-dimensional space

Notation: $|0\rangle$, $|1\rangle$ (off or on). *However*:
a qubit can be a superposition of these two states:

$$|\psi\rangle = a|0\rangle + b|1\rangle; \quad |a|^2 + |b|^2 = 1.$$

(Partially on, partially off!)

Multiple qubits: superposition and entanglement.

Classical tuple: 01011

(one value, determined by each individual bit value)

Quantum tuple: $|01011\rangle$ OR:

$$a_0|00000\rangle + a_1|00001\rangle + a_2|00010\rangle + \cdots + a_{31}|11111\rangle$$

this quantum tuple is a superposition of all 32 possible (base) values!

Moreover the state of the tuple is *not* determined by the state of each qubit (*entanglement*).

Quantum computation:

1. Quantum gates: linear transformations (unitary matrices)
2. Measurements: (quantum physics wreaks havoc!)

Thought experiment: quantum parallel computations.

Consider the following quantum register with the following state:

$$|\psi\rangle = a_2|00010\rangle + a_3|00011\rangle + \cdots + a_{30}|11110\rangle + a_{31}|11111\rangle$$

$a_i = 1/\sqrt{30}$. This is a superposition of all numbers between 2 and 31.

Suppose there were a quantum gate (linear transformation) T which did the following:

$$T(|10010\rangle) = 1147 \mod 20 = |00111\rangle; T(20) = 7.$$

Note: $1147 = 31 \times 37$.

Here's what we'd get:

$$T(|\psi\rangle) = a_2|00001\rangle + a_3|00001\rangle + \cdots + a_{30}|00111\rangle + a_{31}|00000\rangle.$$

Now suppose there were a measurement we could take of $T(|\psi\rangle)$ which would tell us that $|00000\rangle$ corresponds to the 30th term in the superposition. We would then know that 31 divides 1147, in two quantum steps!

Point: quantum computer is fundamentally, a massive parallel processing computer.

This example is overly simplified Shor's algorithm.

Quantum Cryptography: One Time Pad

Take a message

"The dog is black."

and express in binary format.
Then take a sequence of randomly generated bits (the key).
Bitwise exclusive-or them together.

Encoding:

$$\begin{aligned} & 11011001\ldots0101 \\ XOR\ & \underline{10010001\ldots1100} \\ =\ & 01001000\ldots1001 \end{aligned}$$

Decoding:

$$\begin{array}{rr} & 01001000\ldots1001 \\ XOR & \underline{10010001\ldots1100} \\ = & 11011001\ldots0101 \end{array}$$

Advantage: provably secure...

Disadvantage: inefficient key distribution!

1. key size same as message size
2. different key used every single time
3. private key cipher

One Time Pad: provably secure.

Message: “The dog is black.”
Ciphertext: “The cat is brown.”

$$\begin{aligned} Pr(M = \text{“The dog is black”} \mid C = \text{“The cat is brown”}) \\ = Pr(M = \text{“The dog is black”}) \end{aligned}$$

What does this mean? The only attack is a brute force attack.
Ciphertext: “The cat is brown.”
Possible plaintexts:

1. “The cat is brown.”;
2. “The cat is black.”;
3. “The dog is brown.”;
4. “The dog is black.”;
5. “12345678909876543”.

Quantum Cryptography: efficient key distribution!
Alice wishes to send Bob a message securely. Ingredients:

1. quantum communications channel;
2. classical communications channel.

Procedure:

1. Alice sends Bob photons, whose polarization encodes randomly chosen bits.
2. Bob measures the photons, to obtain their polarizations, i.e. the value of the bits.
3. Bob's measurements will be correct 50% of the time, which they can determine over the classical communications channel.
4. The bits corresponding to the correct measurements form the key for the One Time Pad.

5. Alice then sends Bob the encoded message over the classical communications channel.

Eavesdropping on the quantum communications channel can be detected (quantum physics plays nice!).

State of the art.

Quantum computer:

1. 7 qubits
2. factor 15 using Shor's algorithm

Quantum cryptography: key exchange

1. 24 km over fiber optic cable
2. 730 m over free airspace @ 1 million bps

Road blocks:
Hardware: decoherence.
Software: probabilistic measurements.