Quantum Computing

Ian Glendinning

December 3, 2000

Outline

- Introduction
- Quantum Computation
- Quantum Algorithms
- Building Quantum Computers
- Deeper Implications
- Summary and Conclusion

Introduction

- What is Quantum Computing?
  - A fundamentally new mode of information processing that can be performed only by harnessing physical phenomena unique to quantum mechanics
- What is Quantum Mechanics?
  - "The mathematical description of the motion and interaction of subatomic particles in terms of quanta, incorporating the idea that particles can also be regarded as waves" (OED)
  - Fundamentally non-classical: e.g. wave-particle duality ⇒ interference; at the root of quantum computing's power

Quantum Mechanics

- The deepest theory of physics; the framework within which all other current theories (except general relativity) are formulated
- Early History:

1900 Max Planck: discrete energy levels (Dec. 14th)

1925 Werner Heisenberg: matrix formulation of QM

1926 Erwin Schrödinger: wavefunction formulation

1941 Richard Feynman: sum over histories formulation

A Brief History of Quantum Computing

1980 Paul Benioff: quantum mechanical model of computers

1982 Richard Feynman: quantum mechanics cannot be effectively simulated on classical computers

1985 David Deutsch: universal quantum Turing machine

1994 Peter Shor: polynomial-time quantum algorithm for prime factorization *(killer application!)*

1996 Lov Grover: square root speedup of unstructured search

1998 Isaac Chuang, Jonathan Jones: first quantum computer

The Power of Quantum Computing

- The security of public-key cryptosystems such as RSA relies on the difficulty of factorizing very large numbers
- This system is widely used by banks, for example, using numbers with around 250 digits
- In 1994 a 129 digit number known as RSA129 was factored in eight months using approx. 1600 workstations on the internet
- A quantum computer using Shor's algorithm with a clock speed of 100 MHz could factor RSA129 in a few seconds

The Power of Quantum Computing

- It would take roughly 800,000 years to factor a 250 digit number with the same computer power, and a 1000 digit number would take 10^{25} years (significantly longer than the age of the universe)
- Shor's algorithm can factor numbers in a number of steps that is is roughly quadratic in the input size, so factoring a 1000 digit number would require only a few million steps
- This explains the interest of various 'secret' government agencies around the world in the feasibility of building quantum computers!

Quantum Computing Limerick

If the computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.

Jennifer and Peter Shor

What will Quantum Computers be good at?

The most important applications currently known are:

- Factorizing large numbers very rapidly
- Cryptography: perfectly secure communication
- Simulating quantum-mechanical systems efficiently
- Searching

Quantum Information Processing

Quantum computing is actually a sub-discipline of quantum information processing, which deals with the theory and practice of using of quantum mechanics for communication and computation, and also covers the related fields of:

- Quantum information theory
- Quantum communication
- Quantum cryptography

Quantum Computation

- What makes quantum computers different from classical computers?
  - The basic unit of information in a classical computer is the bit, a 2-state device that can represent the values 0 or 1
  - The quantum analogue of a bit is a 2-state quantum system, e.g. electron spin or photon polarization w.r.t. to some axis
  - Such a 2-state quantum system is called a *qubit*
  - Not only can a qubit exist in the classical 0 and 1 states, it can also be in a *superposition* of both

Quantum Computation

- Where do quantum computers get their power?
  - A register with L qubits can be in a superposition of 2^L states, storing all numbers from 0 to $2^L - 1$ simultaneously!
  - Operations act on values 0 and 1 at the same time, and can act on all 2^L values simultaneously: Quantum Parallelism
  - That's what I call *really* high performance computing!
- Where's the catch?
  - Measurement yields only one of the 2^L states
  - Decoherence: disturbance from their environment

Qubits

The states of a qubit corresponding to the classical values 0 and 1 are written $|0\rangle$ and $|1\rangle$, and in general a qubit can take on any value

$$\alpha|0\rangle + \beta|1\rangle$$

where α and β are arbitrary complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1$$

A *measurement* of the state of a qubit always results in a value of either $|0\rangle$ or $|1\rangle$, with a probability of $|\alpha|^2$ for $|0\rangle$ and $|\beta|^2$ for $|1\rangle$

Qubits

In mathematical terms, the general state of a qubit is a vector in the two dimensional complex space C^2, and we can use an equivalent vector notation. If we define

$$|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

then the general qubit state is the complex vector

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Quantum Gates

The quantum analogue of a logic gate is a unitary operator, i.e. one with the property that

$$U^*U = 1$$

And if a qubit state is transformed with a unitary operator U

$$\begin{pmatrix} \beta' \\ \alpha' \end{pmatrix} = U \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

it is easy to show that

$$|\alpha'|^2 + |\beta'|^2 = 1$$

for arbitrary U, so the probability interpretation is preserved.

Quantum Gates

We can define quantum analogues of logical operators, such as the NOT operator:

$$U_{NOT}|1\rangle = |0\rangle, U_{NOT}|0\rangle = -|1\rangle$$

where the phase is for consistency of interpretation with a spin 1/2 particle, corresponding to a 180° spin rotation. In matrix notation:

$$U_{NOT} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Quantum Gates

- Transformations with unitary operators are linear and therefore reversible, unlike most classical gates
- Nevertheless, all the usual arithmetic operations can be implemented in terms of them

Quantum Gates

We can perform more general computations than on classical bits, such as unitary operations on linear combinations of states:

$$U_{NOT}\frac{1}{\sqrt{2}}\left(|1\rangle+|0\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

and also operations with no classical analogue, e.g. Deutsch's 'square root of NOT':

$$\begin{aligned}(U_{SRN})^2 &= U_{NOT}\\ U_{SRN}|1\rangle &= \tfrac{1}{\sqrt{2}}\left(|1\rangle+|0\rangle\right)\\ U_{SRN}|0\rangle &= \tfrac{1}{\sqrt{2}}\left(-|1\rangle+|0\rangle\right)\end{aligned}$$

which physically corresponds to a 90° spin rotation.

Quantum Registers

An n-qubit register is implemented as a multiparticle quantum system, which is represented a tensor product of its component qubits, e.g.:

$$|1\rangle \otimes |1\rangle \cdots \otimes |1\rangle \equiv |11\ldots1\rangle \equiv |2^n - 1\rangle$$

Once again, a register can be in a superposition of states:

$$\sum_{i=0}^{2^n-1} a_i |i\rangle$$

where the interpretation of the (complex) coefficients a_i is that $|a_i|^2$ is the probability that a measurement will yield the value $|i\rangle$

Quantum Registers

By conservation of probability we have:

$$\sum_{i=0}^{2^n-1} |a_i|^2 = 1$$

Such states are known as *coherent* states. In mathematical terms, the state of an n-qubit register is a vector in a space which is the tensor product of n spaces:

$$C^2 \otimes C^2 \otimes \cdots \otimes C^2$$

This is an example of a *Hilbert space* (David Hilbert). Quantum mechanics is a theory set in Hilbert space.

Hilbert

When mathematicians proved Heisenberg's matrix mechanics and Schrödinger's wave mechanics equivalent, Hilbert exclaimed:

> Physics is obviously far too difficult to be left to the physicists and mathematicians still think they are God's gift to science.

Tensor Products

The tensor product of two vectors **a** and **b** is:

$$\mathbf{a} \otimes \mathbf{b} = \begin{pmatrix} a_1 \mathbf{b} \\ a_2 \mathbf{b} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

Quantum Registers

For example, for 2-qubit states we have the four vectors

$$|00\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

which may also be written in the more compact notation

$$|0\rangle, |1\rangle, |2\rangle, |3\rangle$$

N-Qubit Quantum Gates

N-qubit quantum gates can be represented by $2^N \times 2^N$ matrices. E.g., applying a tensor product of our SRN (or Hadamard) transformation:

$$(U_{SRN} \otimes U_{SRN} \cdots \otimes U_{SRN})|11\ldots1\rangle$$
$$= (U_{SRN}|1\rangle) \otimes (U_{SRN}|1\rangle) \otimes \cdots \otimes (U_{SRN}|1\rangle)$$

we obtain a superposition of all 2^n states:

$$= \frac{1}{2^{N/2}}((|1\rangle + |0\rangle) \otimes (|1\rangle + |0\rangle) \otimes \cdots \otimes (|1\rangle + |0\rangle))$$

$$= \frac{1}{2^{N/2}}((|11\ldots1\rangle) + (|11\ldots0\rangle) + \cdots + (|00\ldots0\rangle))$$

Exponential Parallelism

- By applying a linear number of operations, we have generated a state with an exponential number (2^N) of terms
- We could now apply a function to all 2^N terms in parallel!
- It is tempting to think that this immediately implies exponential computational power, but sadly this is not the case...
- Because measurement reveals only one randomly selected value
- The solution is to use destructive interference between states
- The combination of *exponential parallelism* and *interference* is what makes quantum computation powerful

The Universal Gate

It can be shown that any $n \times n$ unitary matrix can be formed by composing the 2-qubit 'controlled-not' gate (U_{CN}), and general rotation of a single qubit $V(\theta, \phi)$, where

$$V(\theta, \phi) = \begin{pmatrix} \cos(\theta/2) & -ie^{-i\phi}\sin(\theta/2) \\ -ie^{i\phi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$U_{CN}|00\rangle = |00\rangle, U_{CN}|01\rangle = |01\rangle$$

$$U_{CN}|10\rangle = |11\rangle, U_{CN}|11\rangle = |10\rangle$$

and it has been shown that U_{CN} and $V(\theta, \phi)$ can be combined to make a controlled rotation, which is a single universal gate.

Entanglement

Consider the operation of U_{CN} on the following product state:

$$\begin{aligned} U_{CN}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle &= U_{CN}\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \end{aligned}$$

- The resulting state is a so-called *entangled* state, because it cannot be expressed as a tensor product
- Measuring one qubit forces the other one into a definite state *Even if the two qubits are physically separated!*
- This is the basis of 'quantum teleportation', and is one of the least intuitive features of quantum mechanics

Feynman on Quantum Mechanics

I am going to tell you what nature behaves like......

However do not keep saying to yourself, if you can possibly avoid it,

BUT HOW CAN IT BE LIKE THAT?

because you will get “down the drain” into a blind alley from which nobody has yet escaped.

NOBODY KNOWS HOW IT CAN BE LIKE THAT.

Richard Feynman (1965): The character of physical law.

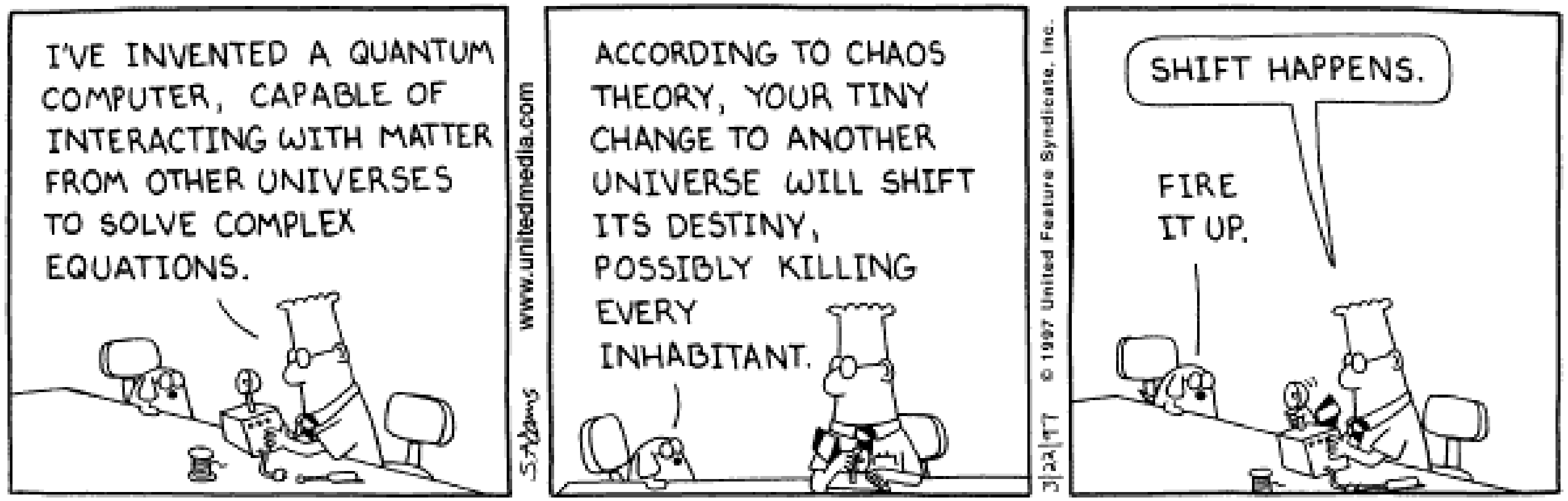
Neils Bohr on Quantum Mechanics

Anyone who is not shocked by quantum theory has not understood it!

Parallel Universes?

- In one interpretation of quantum mechanics, qubits in coherent superposition states exist simultaneously in two universes, as a 0 in one universe and as a 1 in the other
- In this interpretation, the computer you can see and touch is only one tiny facet of a far larger object, whose existence is only detectable indirectly, by the computational work it does for us
- It has the structure of many computers similar to the one we see, performing different computations which affect each other through quantum interference
- In this view the whole of reality behaves this way: *multiverse*

Dilbert on Quantum Computing



Quantum Algorithms

- The first quantum algorithm to be discovered which achieved advantage over classical algorithms was:

  1992 Deutsch and Josza: determines if a boolean function is constant or 'balanced'

- The most important algorithms currently known are:

  1994 Shor: factorizing large numbers

  1996 Grover: unstructured search

Grover's Algorithm

The problem: search a database with N names in a random order for the phone number of a friend. Classically this would require on average $N/2$ steps.

Grover's algorithm can search a quantum database in $O(\sqrt{N})$ steps.

The Abstracted Problem

- Let a system have $N = 2^n$ states, labelled $S_1, S_2 \ldots S_N$
- These states are represented as strings of n qubits
- Let there be a condition C(S) with the property that it is true for a unique state, say S_ν
  - $C(S_\nu) = 1$, whereas for all other states S, $C(S) = 0$
  - (assume that $C(S)$ can be evaluated in unit time)
- The problem is to identify the state S_ν

Grover's Algorithm

1. Initialize the system to the distribution:

$$\left(\frac{1}{\sqrt{N}}, \quad \frac{1}{\sqrt{N}}, \quad \frac{1}{\sqrt{N}} \cdots \frac{1}{\sqrt{N}} \right)$$

   i.e. each state has the same amplitude (this can be achieved in $O(\log N)$ steps, by applying the Hadamard gate to each qubit)

Grover's Algorithm

2. DO FOR $O(\sqrt{N})$ TIMES

   Apply the unitary operators:

   (a) U_ν defined by

   $U_\nu S_i = -S_i$ for $i = \nu$ (i.e. for $C(S_i) = 1$)

   $U_\nu S_i = S_i$ otherwise

   (b) 'Diffusion' operator D defined as the matrix with elements:

   $D_{ij} = \frac{2}{N}$ if $i \neq j$ and $D_{ii} = -1 + \frac{2}{N}$

3. END DO

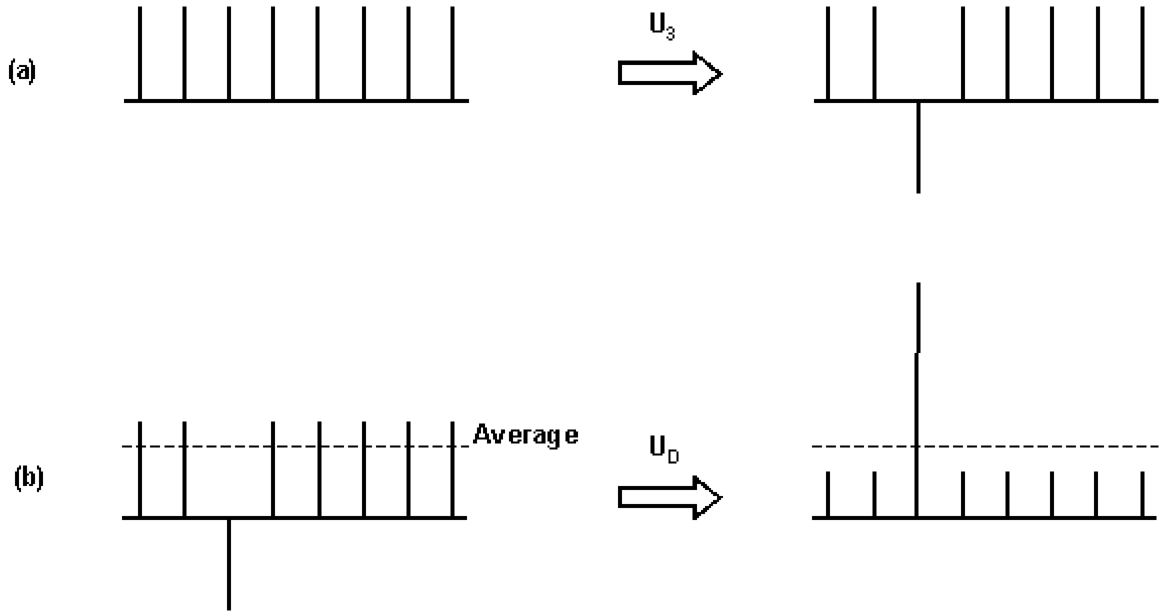
4. Measurement yields state S_ν with probability of at least 1/2

Grover's Algorithm

This may appear cryptic, but the effect is is actually rather simple

- The diffusion operator corresponds to a reflection of all the amplitudes about their mean
- Because the sign of the amplitude we want has been reversed, it is amplified at the expense of the others

Grover's Algorithm



Shor's Algorithm

1. Initialize two n-bit quantum registers x and y to $|0\rangle \otimes |0\rangle$
2. Apply a Hadamard transformation to each qubit in x, giving:

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle \otimes |0\rangle$$

   where $w = 2^n$

3. Apply a unitary operator which performs the operation

$$|x\rangle \otimes |0\rangle \mapsto |x\rangle \otimes |a^x \bmod N\rangle$$

   where N is to be factored and $a < N$ is chosen randomly, giving:

Shor's Algorithm

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle \otimes |a^x \bmod N\rangle$$

3. Measure the second register, giving u, and a total state:

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |d_u + jr\rangle \otimes |u\rangle$$

   where the $d_u + jr$ are the values of x for which $a^x \bmod N = u$

4. Apply a quantum Fourier Transform to get the period r

5. $\gcd(a^{r/2} - 1, N)$ is a non-trivial factor of N with high probability!

Tools for Algorithm Development

- QCE - Quantum Computer Emulator (University of Groningen)
  - Emulates ideal and physically realizable Quantum Computers
  - Ideal transformations used in theoretical work are difficult to implement on a physical realization of a Quantum Computer
- QCL - Quantum Computation Language (TU-Wien)
  - High level programming language for quantum computers, with a syntax derived from classical languages like C or Pascal
  - Allows for the implementation and simulation of quantum algorithms

Building Quantum Computers

The technologies being explored include:

- Ion traps
- Cavity Quantum Electrodynamics
- Nuclear Magnetic Resonance (NMR)
- Optical interferometers
- Macroscopic superconductivity (SQUIDs)
- Semiconductors

Recent Experimental Results

Very primitive quantum computers have already been built:

1995 Wineland: first Controlled-NOT gate, using a trapped ion

1998 Chuang / Jones: first 2-qubit computers at UCB / Oxford

1999 Chuang: first 3-qubit computer at IBM Almaden

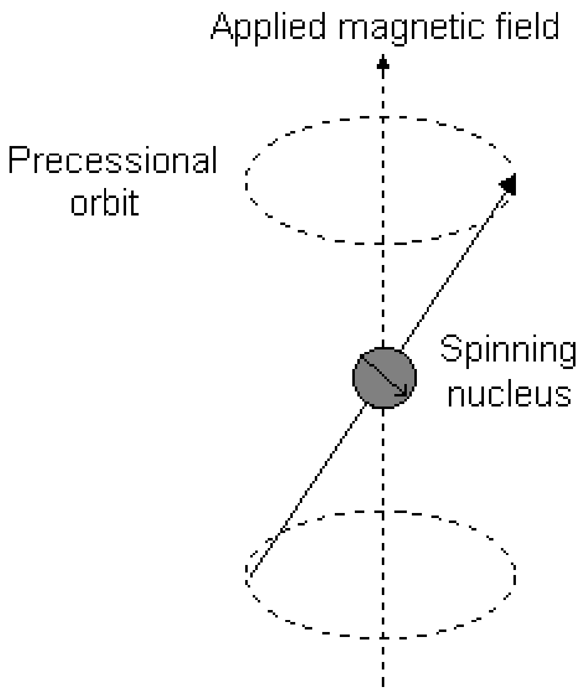
2000 Knill, Laflamme: coherence in 7-qubit molecule at Los Alamos

2000 Chuang: first 5-qubit computer at IBM Almaden (August)

Nuclear Magnetic Resonance

- Some atomic nuclei possess ‘spin’
- This is really a quantum mechanical phenomenon, but a classical analogy gives some feel for what happens in the quantum case
  - Because the nucleus is positively charged, the spin generates a small magnetic field, rather like a small bar magnet
  - In the presence of a strong external magnetic field, the nuclear spins precess around it

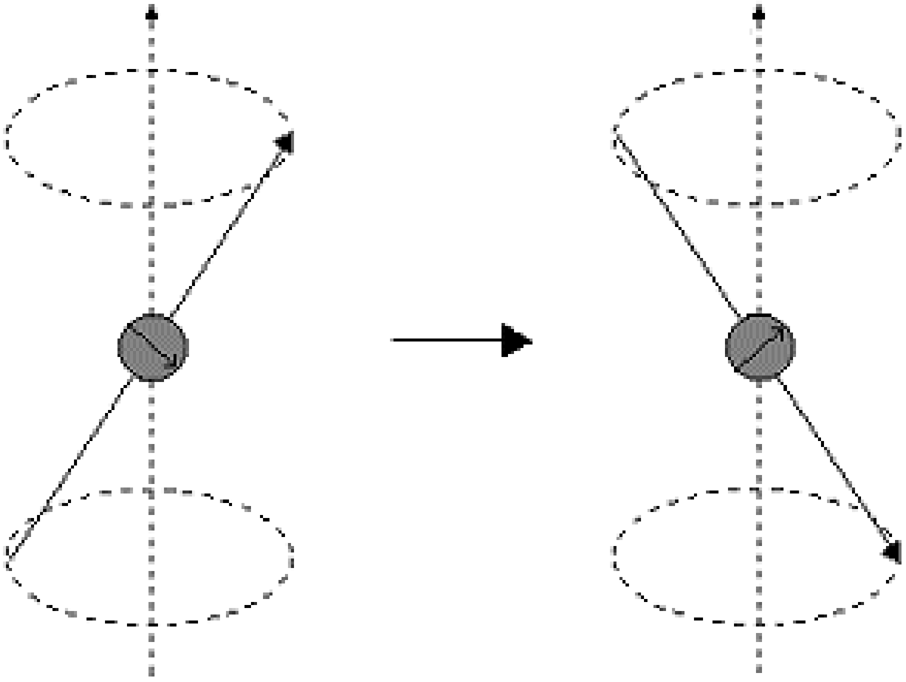
Nuclear Precession



Nuclear Magnetic Resonance

- The nuclear spin can point up or down with respect to the direction of the applied magnetic field (denoted the z-axis)
- These two states can represent qubit states $|0\rangle$ and $|1\rangle$
- The spin states are well isolated from their environment, and are not disturbed by the motion and collisions of the molecules containing them
- Radio-frequency (RF) pulses at the precession frequency, applied perpendicular to the applied magnetic field, can cause the nucleus to flip between the two states

Nuclear Spin Flipping



Nuclear Magnetic Resonance

- RF pulses change the angle of the spin axis of the nucleus relative to that of the magnetic field, according to their duration
- In the quantum picture, the nuclear spin state becomes a superposition of the states $|0\rangle$ and $|1\rangle$, so applying RF pulses in the $x - y$ plane implements single-qubit gates
- Different nuclei can be addressed, as their resonant frequency depends on which element they are, and on electron shielding
- There is also an interaction between nuclear spins in nearby atoms, which allows 2-qubit gates to be implemented

Chuang's 2-Qubit Computer

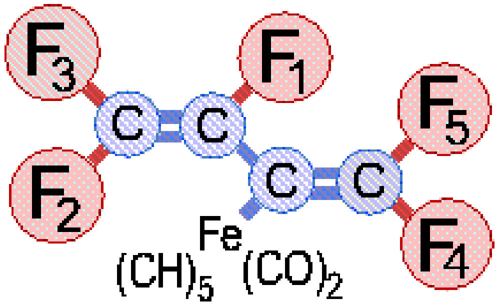
- Used carbon-13 labeled chloroform ($CHCl_3$) dissolved in acetone at room temperature and pressure
- The $O(10^{18})$ molecules in the sample acted as independent single quantum computers, all functioning simultaneously
- The Carbon and Hydrogen nuclei represented the two qubits
- Decoherence times were $\sim$ 20 s and $\sim$ 0.3 s (spin-spin) and pulses of frequencies $\sim$ 500 MHz & 125 MHz, duration 10-15 μs
- Longest computation took less than 35 ms

Chuang's 2-Qubit Computer

- Grover's algorithm was implemented for the simplest interesting case, of $N = 4$
- The system had all of the components of a complete computer architecture, including the rudiments of compiler optimizations!

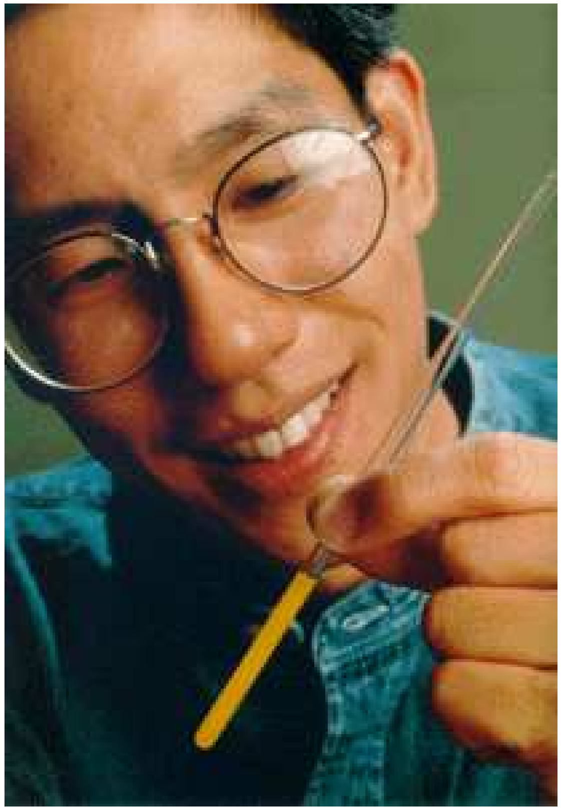
State of the Art: Chuang's 5-Qubit Computer

- A custom synthesized molecule was used as the quantum computer. The nuclei of its five ^{19}F atoms served as qubits



- An algorithm was implemented that generalizes Shor's algorithm to find the order of a permutation in fewer steps than is possible using a classical computer

Chuang and his 5-Qubit Computer



The Future of Quantum Computing Hardware

- The scalability of NMR quantum computers seems limited, as the signal falls exponentially with the number of qubits using current techniques
- Semiconductor-based devices are still some way off - which is why quantum effects still aren't a problem for conventional chips!
- It has been proven that quantum error correction is possible, so decoherence can be overcome and is no limitation in principle
- The only obstacles are technological, and I personally believe that that is a good ground for optimism

History Encourages Optimism

"Where a calculator on the Eniac is equipped with 18000 vacuum tubes and weighs 30 tons, computers in the future may have only 1000 tubes and weigh only 1 1/2 tons"

Popular Mechanics, March 1949

Deeper Implications - Computability

- The Church-Turing hypothesis (that all 'natural' models of computation are equivalent to each other), was never proved
- Its analogue in the quantum theory of computation (the Turing Principle, that the universal quantum computer can simulate the behaviour of any finite physical system) was straightforwardly proved in Deutsch's 1985 paper
- A stronger result, namely that such simulations can always be performed in at most a polynomial function of the time taken for the physical evolution, has since been proved in the quantum case

Deeper Implications - Mathematical Proof

- Performing any computation that provides a definite output is tantamount to proving that the observed output is one of the possible results of the given computation
- We can always translate such a proof into the proof of some mathematical theorem
- Henceforward, a proof must be regarded as a process – the computation itself, because quantum computers will prove theorems by methods that can never be checked step-by-step; if the steps for such a proof were printed out, the paper would fill the observable universe many times over

Deeper Implications - Consciousness

- The theory of quantum computation allows us to look at the question of consciousness from a new perspective, since every physical object can be regarded as a quantum computer and any physical process can be considered a computation
- If the brain can be regarded as a computer and consciousness as the result of a computation, then Deutsch's universality result means it must be possible to simulate conscious rational thought using a quantum computer
- Some believe that quantum computing could well be the key to cracking the problem of artificial intelligence but others disagree

Summary

- Quantum Computers can solve hard problems
  - There is a new complexity class
  - The class of problems for which quantum computers have a big advantage remains to be characterized
- Quantum errors can be corrected
  - The effects of decoherence can be overcome
- Quantum hardware can be constructed

Conclusion

- We are privileged to be witnessing the dawn of the age of coherent manipulation of information in the laboratory
- There is potential here for truly revolutionary innovation
- There is almost daily progress in developing ever more promising technologies for quantum computation and new quantum algorithms with advantages over their classical counterparts
- On 27th Nov. 2000, Goong Chen & Zijian Diao announced an *exponentially fast* quantum search algorithm
- These are exciting times!

Conclusion

Es ist meine persönliche Überzeugung, dass dieses Gebiet der Quanteninformatik zu revolutionär neuen Methoden der Informationsverarbeitung und Informationsübertragung führen wird, wobei wahrscheinlich die heutigen Konzepte noch zu konservativ sind, das heisst noch zu sehr angelehnt sind an die uns bekannten Ideen, was "computation" bedeutet. Die wirklich neuen Ideen, die die Eigenschaften der Quantenphysik voll ausnützen und damit auch beträchtlich über Einstein hinaus gehen werden, stehen uns wahrscheinlich noch bevor.

Anton Zeilinger, 'Neue Zürcher Zeitung' 30. Juni 1999, S. 55

Conclusion

Quantum computers raise interesting problems for the design of programming languages, which I shall not go into here. From what I have said, programs exist that would (in order of increasing difficulty) test the Bell inequality, test the linearity of quantum dynamics, and test the Everett interpretation. I leave it to the reader to write them.

David Deutsch,
Proc. Royal Society London A **400**, *pp. 97-117 (1985)*

Further Information: http://www.qubit.org/