USC Viterbi
School of Engineering

USC

Secrets of Quantum Information Science

Todd A. Brun

Communication Sciences Institute

USC

Quantum computers are in the news

FIRST IN A 2-PART SERIES ON QUANTUM COMPUTING

THE TRAP TECHNIQUE

TOWARD A CHIP-BASED QUANTUM COMPUTER

BY DANIEL STICK, JONATHAN D. STERK & CHRISTOPHER MONROE

COMPUTERS TODAY are fast approaching some fundamental limitations. Perhaps their biggest problem is that they exploit the classical physics that governs the hurly-burly rush of countless billions of electrons through nearly as many transistors. And the chips at the heart of today's computers are running out of room for classical physics to work.

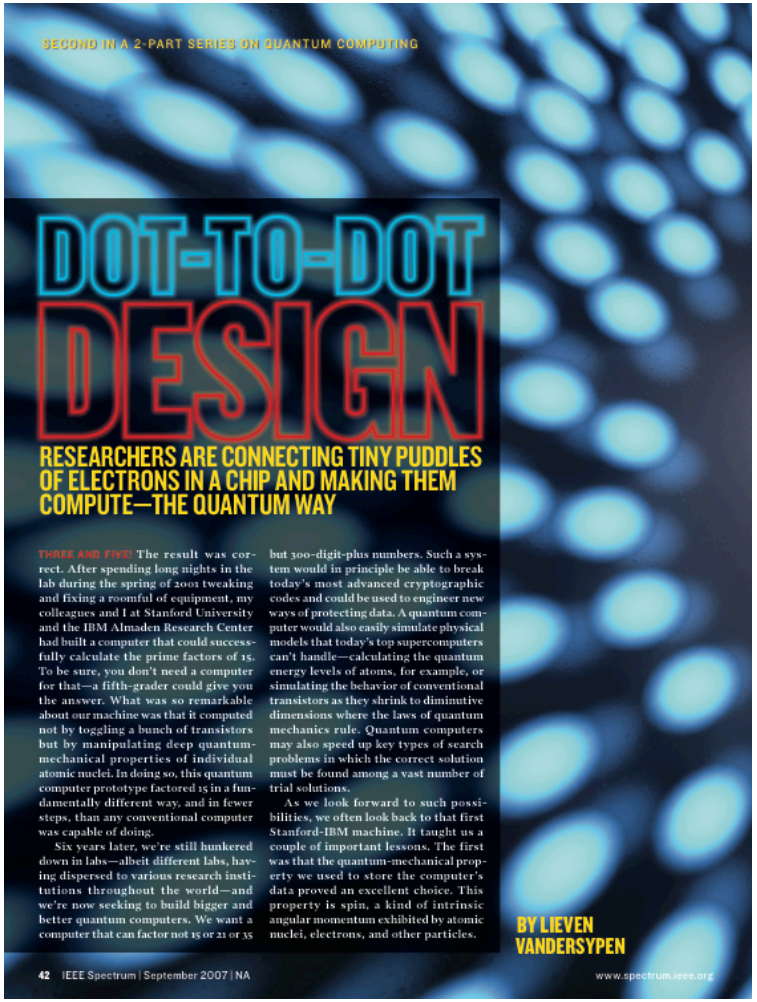
To make those chips' transistors switch faster, we've primarily relied on making the devices smaller. But when they begin to approach 10 nanometers or so—and it is the goal of the semiconductor industry to get there in the next decade—very odd things will happen. Formerly well-behaved electrons will start revealing their quantum nature—darting across the transistor on the dictates of probability, regardless of whether the device is switched on or off. When transistors reach those infinitesimal dimensions and electrons start showing their true colors, computer makers will have two choices: try to fend off the quantum weirdness with radically new types of semiconductors and transistors, or embrace the weirdness.

We say: surrender to the weirdness. Working with the quantum nature of things instead of against it will open up vast new frontiers for computing. And achievements during the past couple of years at university and government laboratories around the world have made it clear that a large-scale, practical quantum computer could be built, probably in the next 25 to 30 years. These achievements have demonstrated that the semiconductor manufacturing technologies underpinning modern computing, which were developed over nearly half a century, need not be abandoned. On the contrary, they will be instrumental in making quantum computers a practical reality.

These machines will take computing where it's never been before. Most notably, there are classes of problems for which a conventional computer can do little more than try out all the possible solutions one at a time until it stumbles on the answer. Say, you have a phone number and want

www.spectrum.ieee.org

August 2007 | IEEE Spectrum | NA 37



SECOND IN A 2-PART SERIES ON QUANTUM COMPUTING

DOT-TO-DOT DESIGN

RESEARCHERS ARE CONNECTING TINY PUDDLES OF ELECTRONS IN A CHIP AND MAKING THEM COMPUTE—THE QUANTUM WAY

BY LIEVEN VANDERSYPEN

THREE AND FIVE! The result was correct. After spending long nights in the lab during the spring of 2001 tweaking and fixing a roomful of equipment, my colleagues and I at Stanford University and the IBM Almaden Research Center had built a computer that could successfully calculate the prime factors of 15. To be sure, you don't need a computer for that—a fifth-grader could give you the answer. What was so remarkable about our machine was that it computed not by toggling a bunch of transistors but by manipulating deep quantum-mechanical properties of individual atomic nuclei. In doing so, this quantum computer prototype factored 15 in a fundamentally different way, and in fewer steps, than any conventional computer was capable of doing.

Six years later, we're still hunkered down in labs—albeit different labs, having dispersed to various research institutions throughout the world—and we're now seeking to build bigger and better quantum computers. We want a computer that can factor not 15 or 21 or 35 but 300-digit-plus numbers. Such a system would in principle be able to break today's most advanced cryptographic codes and could be used to engineer new ways of protecting data. A quantum computer would also easily simulate physical models that today's top supercomputers can't handle—calculating the quantum energy levels of atoms, for example, or simulating the behavior of conventional transistors as they shrink to diminutive dimensions where the laws of quantum mechanics rule. Quantum computers may also speed up key types of search problems in which the correct solution must be found among a vast number of trial solutions.

As we look forward to such possibilities, we often look back to that first Stanford-IBM machine. It taught us a couple of important lessons. The first was that the quantum-mechanical property we used to store the computer's data proved an excellent choice. This property is spin, a kind of intrinsic angular momentum exhibited by atomic nuclei, electrons, and other particles.

42 IEEE Spectrum | September 2007 | NA

www.spectrum.ieee.org

USC

Quantum computers represent a new paradigm for computing devices: computers whose components are individual quantum systems, and which exploit the properties of quantum mechanics to make possible new algorithms and new ways of processing information.

Quantum computers are just one part of the new field of quantum information science, that combines physics with computer science, information theory, and engineering. This may lead to new technology, and it has already led to new ways of understanding quantum mechanics.

USC

Quantum Mechanics and its properties

- Quantum mechanics is the theory that describes the behavior of microscopic systems, such as atoms, molecules, and photons
- This theory, which has been extensively tested by experiments, is probabilistic in nature. The outcomes of measurements on quantum systems are random. And choosing to do one measurement disturbs the outcome of others (uncertainty).
- Between measurements, quantum systems evolve according to linear equations (the Schrödinger equation). This means that solutions to the equations obey a superposition principle: linear combinations of solutions are still solutions.
- These superpositions can interfere with each other (like a wave), either constructively or destructively.
- Quantum states can exhibit strangely powerful correlations, called entanglement.

USC

Superpositions

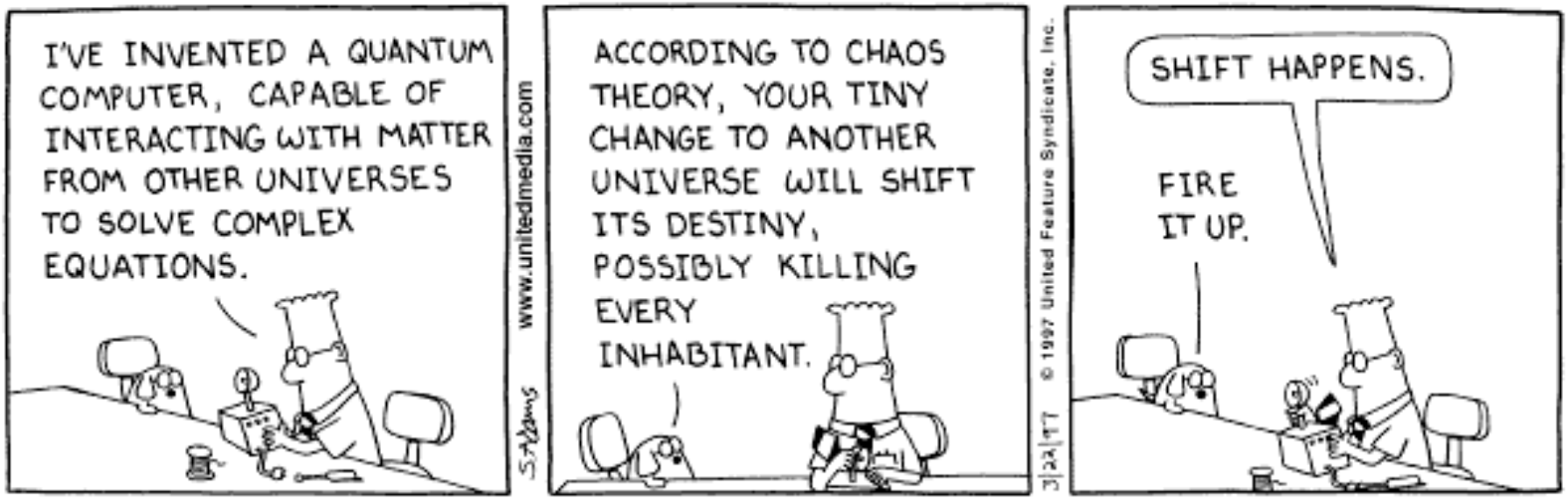
The classic example of superposition is Schrödinger's Cat. Since both a living and dead cat are obviously valid solutions to the laws of quantum mechanics, a superposition of the two should also be valid. Schrödinger described a thought experiment that could give rise to such a state.

α  $+$ β 

If this state is measured, we see only one or the other state (live or dead) with some probability.

USC

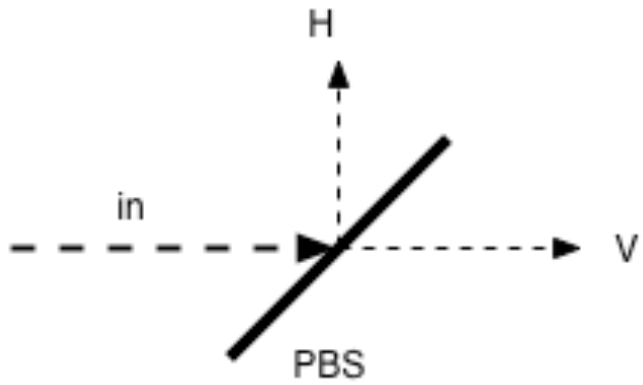
One school of thought believes the entire universe is in a giant superposition of all possible states…



Copyright © 1997 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited

(Even Schrödinger's Cat is no match for Dilbert's Dog.)

Schrödinger's Photons

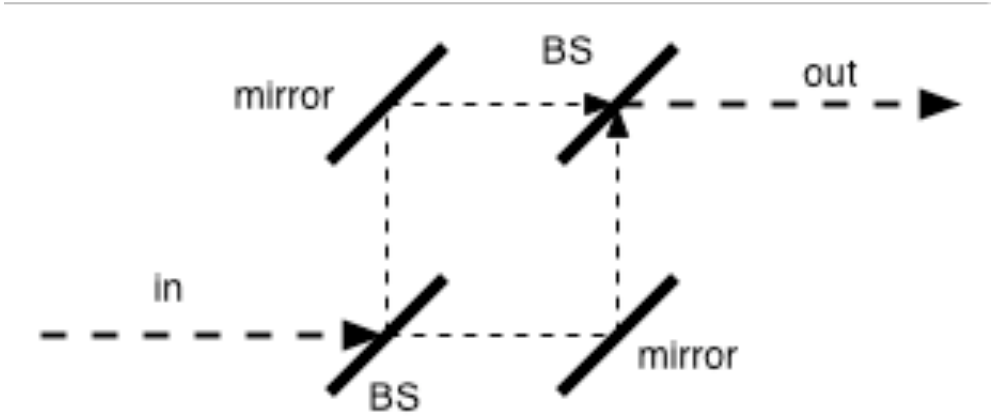


- A polarizing beam splitter is a device which reflects all light of one polarization (say H) and transmits all light of the other polarization (say V).
- If light polarized 45° to H and V arrives, half of it is reflected and half transmitted.
- If a single photon at 45° arrives, it will be reflected or transmitted with 50/50 probability. Such a photon is a superposition of H and V: (|H>+|V>)/sqrt(2). If we rotated the PBS by 45°, this photon would always be transmitted .

USC

Interference

However, it is not just a simple matter of a photon going one way or the other with equal probability. If we pass the two beams through a pair of beamsplitters, we find that the photon can recombine in such a way that the probability to go in one direction cancels out. This is interference.



USC

Q-bits

A physical system of this type, with two distinguishable states, is called a quantum bit or q-bit (or qubit). We label the two distinct states $|0\rangle$ and $|1\rangle$. Unlike a classical bit, though, a q-bit can be in any linear combination of these states:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

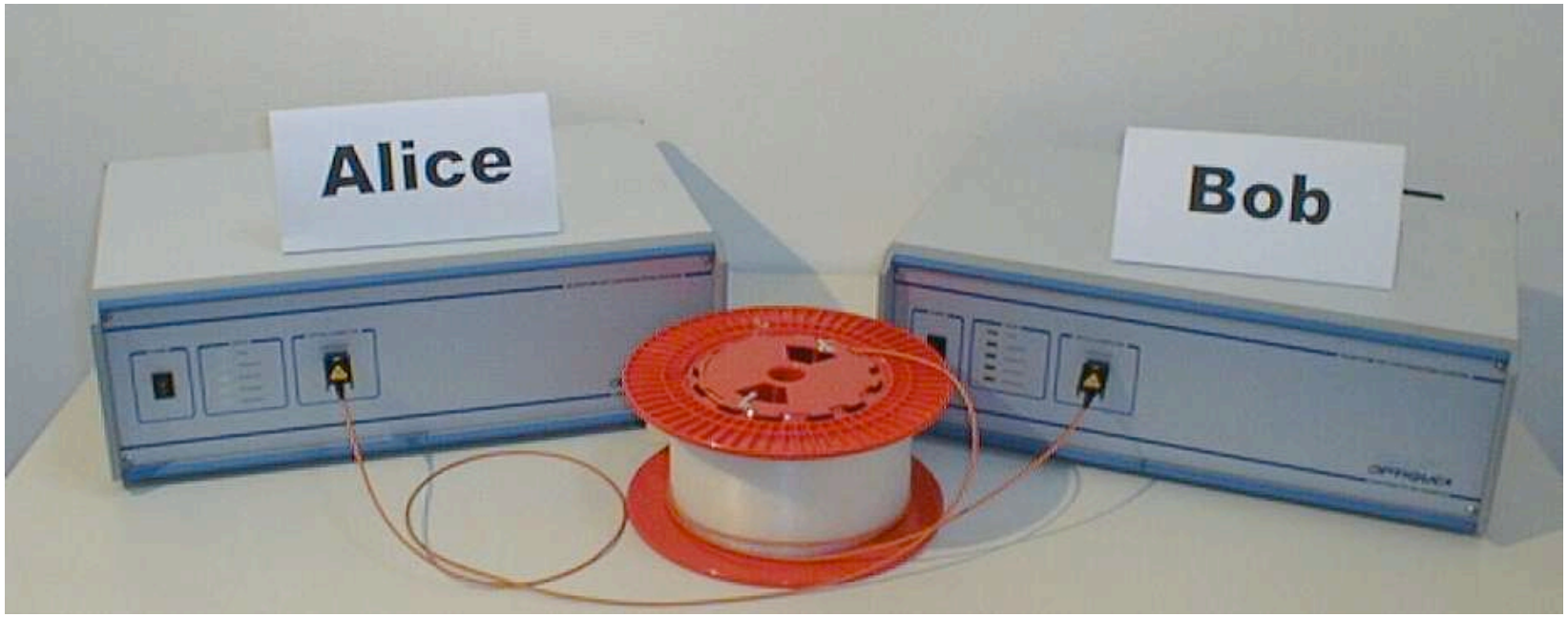
where α and β are complex numbers. (For photons, these would represent not only linear polarizations, but also circular and elliptical.) If the q-bit is measured it will be found in state 0 or 1 with probabilities $|\alpha|^2$ or $|\beta|^2$, and the system will then be left in the state $|0\rangle$ or $|1\rangle$. The act of measurement disturbs the state!

USC

Quantum Cryptography

- Alice and Bob wish to establish a secret key, but the communication lines between them may be compromised. Alice sends random q-bits to Bob. Each bit is encoded either as {|0>,|1>} or {|0>±|1>}.
- Bob randomly chooses a measurement for the bit (either horizontal/vertical or at 45°). If he guesses wrong, he gets a random bit.
- If an eavesdropper Eve tries to intercept the q-bits, she also can only guess the encoding. If she guesses wrong, the bit she passes on to Bob will have been disturbed.
- After N bits, Alice and Bob compare notes as to which encoding they used. All bits where their choices didn't match are discarded. The remainder should be perfectly correlated.

USC



This is what the actual device looks like. The coil is of ordinary optical fiber.

USC

Multiple Q-bits

What can be done with single q-bits is very limited. For more ambitious information processing, multiple bits must be used and manipulated. If we have n bits, we can think of them as representing the binary expression for an n-bit integer x between 0 and 2^n-1, or as the memory of an entire n-bit computer! The most general state of n q-bits can be written

$$|\Psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle$$

We can think of this as a superposition of all possible states of a classical computer! So a quantum computer, in a certain sense, can do many different computations at once. This is called quantum parallelism. It is not as powerful as true parallelism! But if exploited cleverly, it can still make a quantum computer more powerful than a classical one.

USC

Entanglement

- **Some states of multiple q-bits can be written as products of states of individual q-bits:**

  $(\alpha_1|0> + \beta_1|1>)(\alpha_2|0> + \beta_2|1>)...(\alpha_n|0> + \beta_n|1>)$

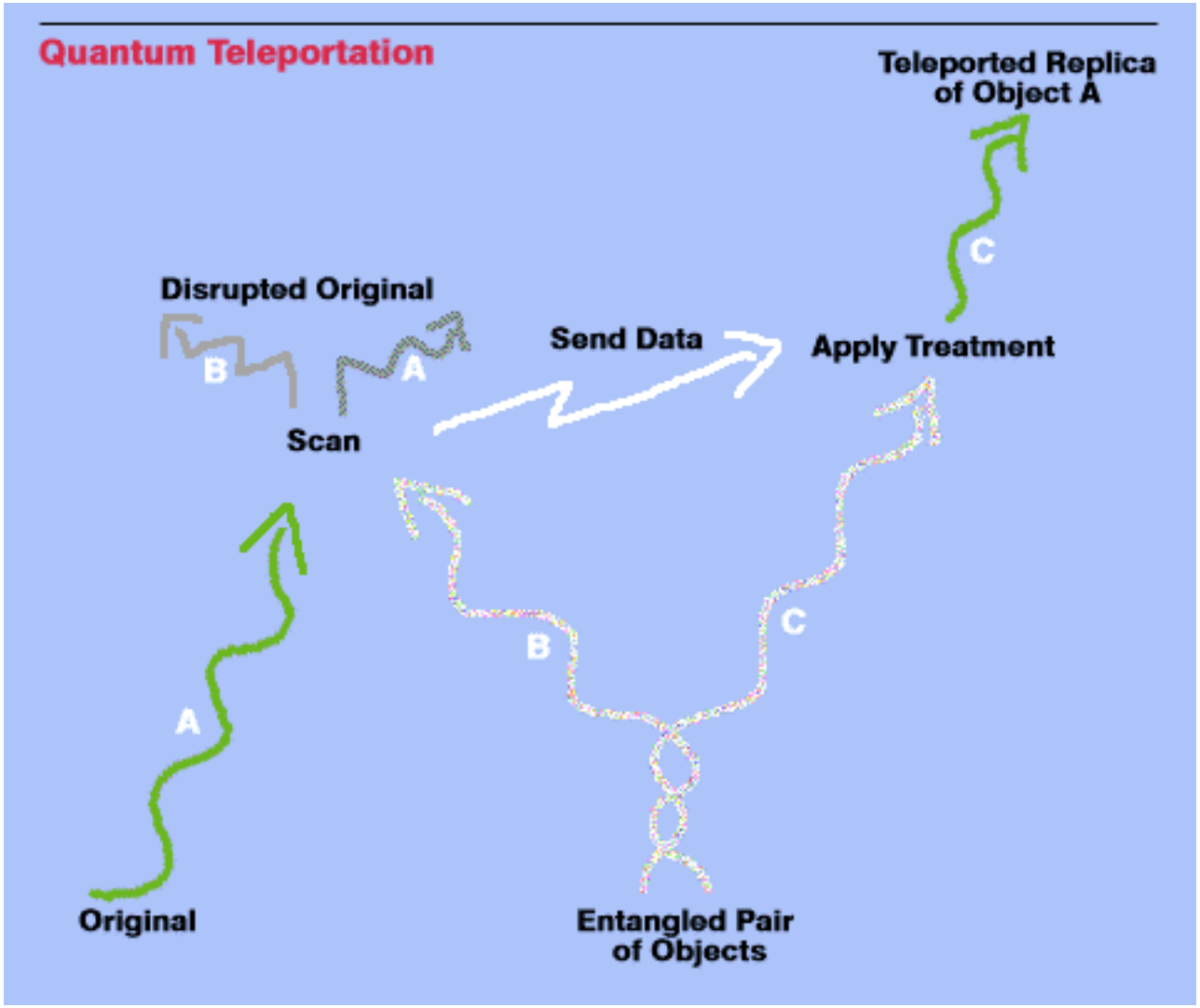
- **However, most states can't be written this way. We call such states entangled.**

  $\alpha|00> + \beta|11>$

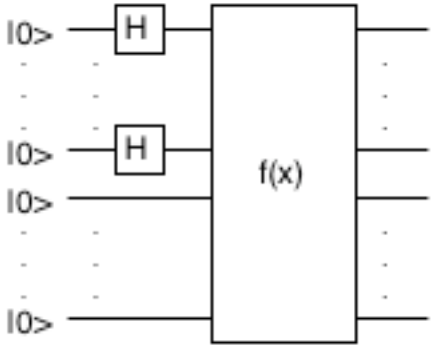
- **Measurements on such entangled states are correlated. This correlation is (in a certain sense) more powerful than ordinary classical correlation, and it can be used for new kinds of tricks.**

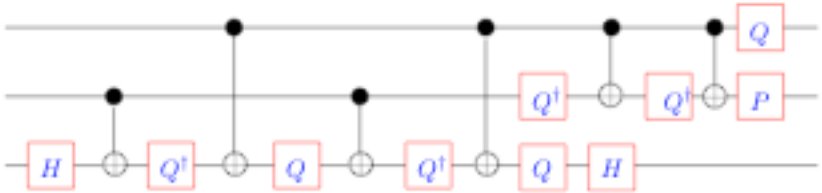
USC

Quantum teleportation

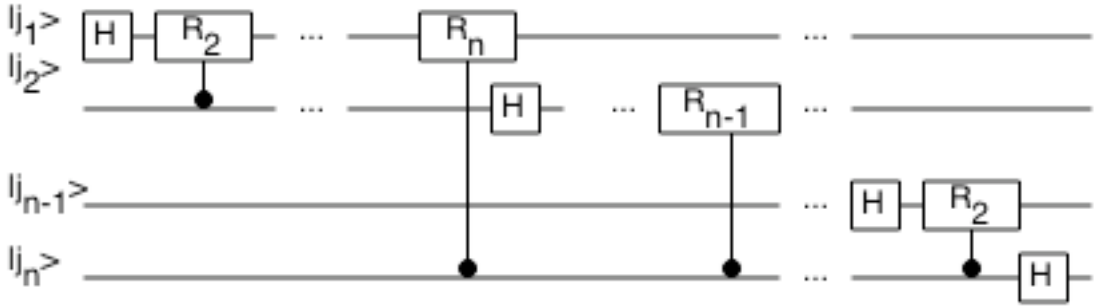


Quantum Circuits





where, $P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, Q = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$.



USC

Quantum Algorithms

With quantum circuits (such as those described above), we can construct new algorithms that operate on fundamentally new principles. The most famous of these are Shor's Factoring Algorithm (Shor, 1994), which is $O(L^3)$ in the length of the number to be factored; and Grover's Unstructured Search Algorithm (Grover, 1996), which is $O(N^{1/2})$ in the number of locations to be searched. Many problems with related structures have also been solved. (Shor's algorithm attracted tremendous attention because it could break the RSA public-key encryption system widely used in Internet commerce.)

All quantum algorithms create superpositions of all possible values of a function, and use interference to reinforce the probability of desired solutions while suppressing incorrect answers. Finding new algorithms is a very difficult open problem.

USC

Experimental Implementations

Many implementations of q-bits have been proposed:

- Spins of electrons in quantum dots
- Spins of nuclei in molecules (molecules)
- Spins of electrons floating over liquid helium
- Electronic states of atoms or ions in traps
- Excitonic states of nanocrystals
- Polarization of photons ("flying qubits")
- Occupation level of an optical microcavity
- Spins of impurity nuclei
- "Dual-rail" photon qubits
- Ions in optical lattices
- Collective spins of atom clusters

All of these proposals have their own advantages (and disadvantages), and are being actively experimentally pursued.

USC

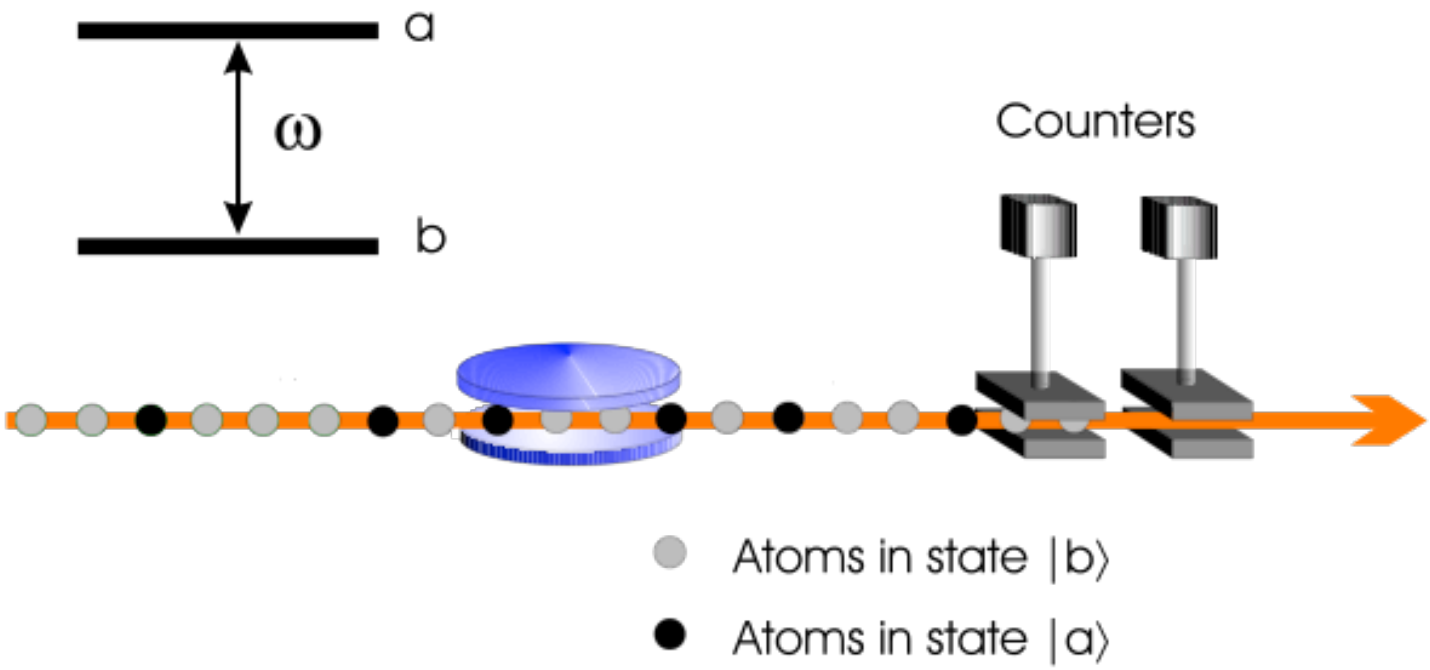
The DiVincenzo Criteria

In order to function as a quantum computer, a physical system must satisfy a number of stringent requirements. These were summarized by David DiVincenzo of IBM in a highly influential 1996 paper.

- Existence of qubits (division into subsystems)
- One- and two-bit unitary gates
- Initializable into a standard starting state
- Measurable bits
- Low intrinsic decoherence

USC

An implementation may be simple in theory...

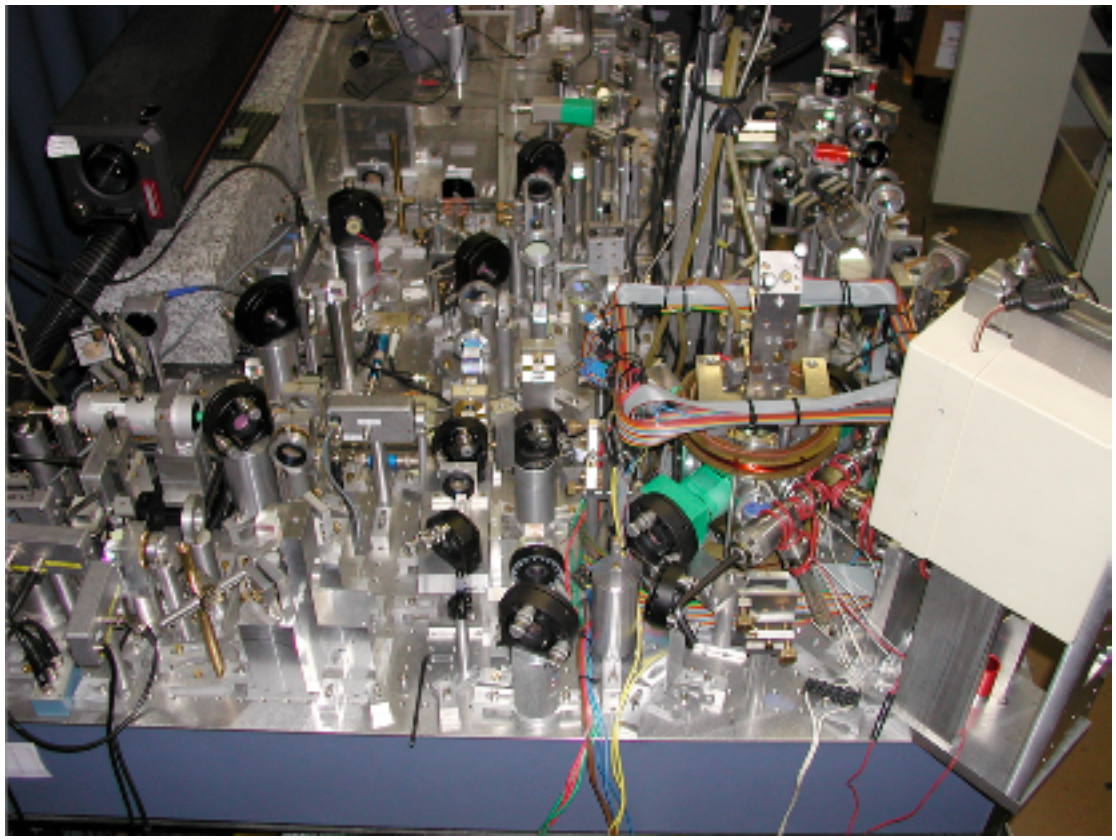


This is a schematic picture of a quantum information experiment...

Figure 1 - Kist - PRA

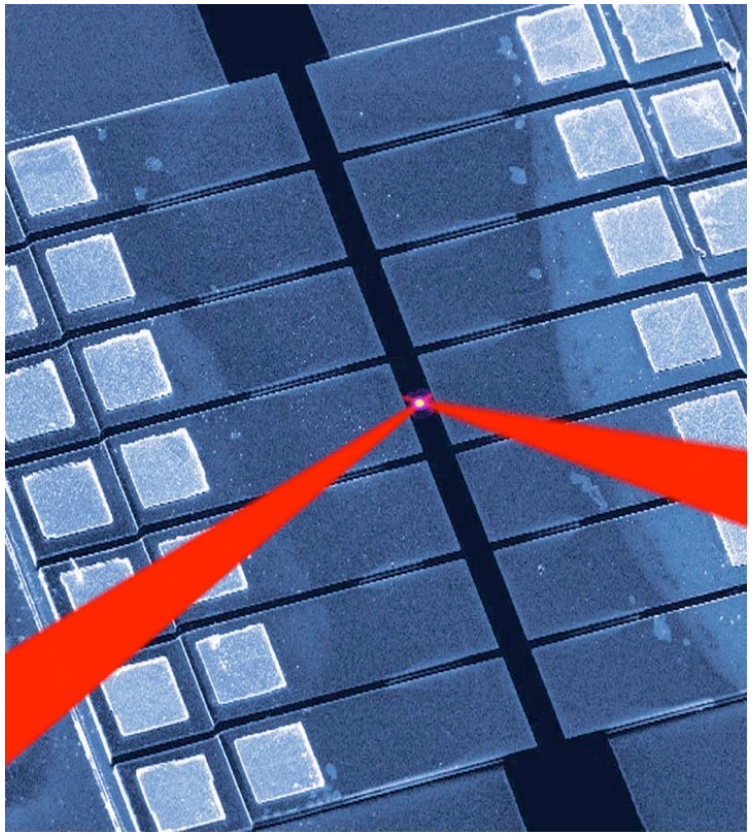
USC

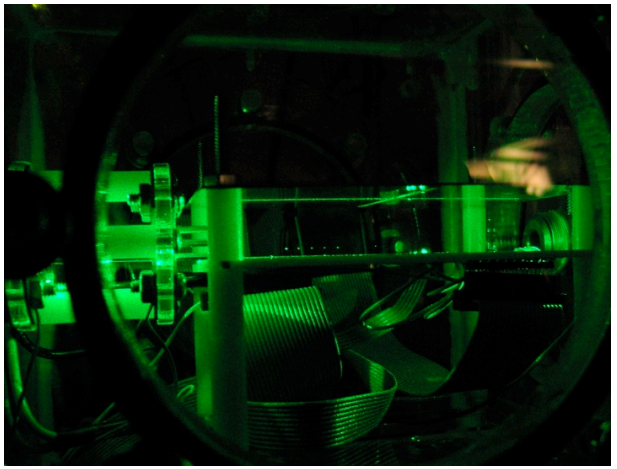
...but the reality can be messy

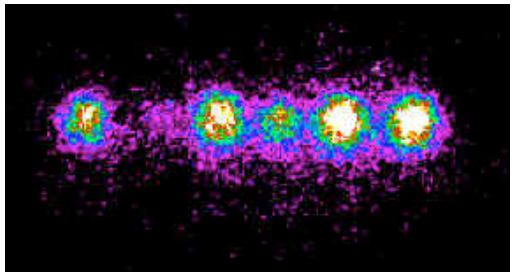


...and this is a photo of the actual laboratory.

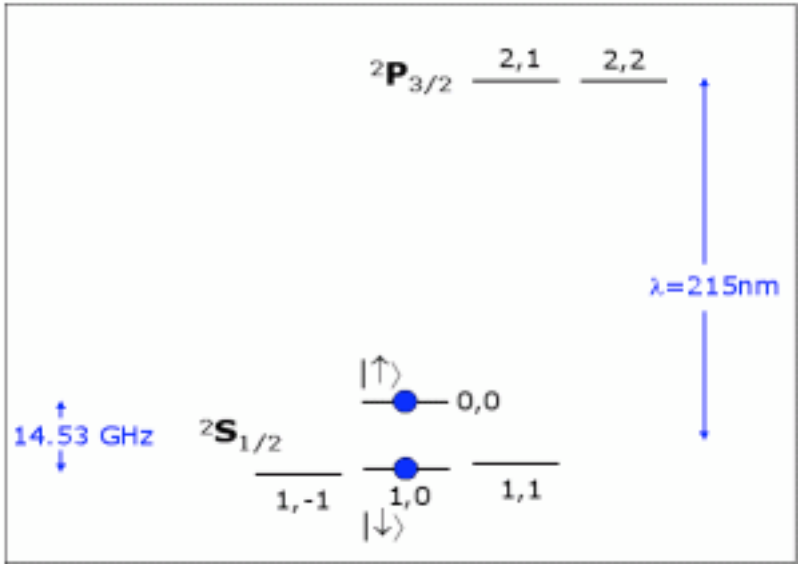
The Ion Trap







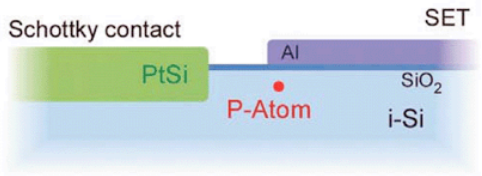
$^{111}Cd^{+}$ atomic structure



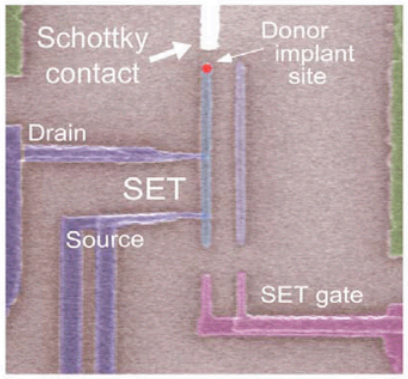
USC

Solid State Quantum Dots

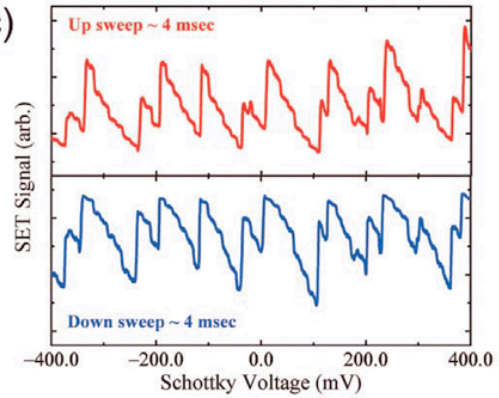
(a)

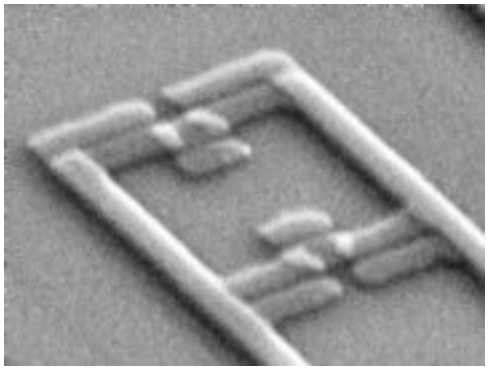


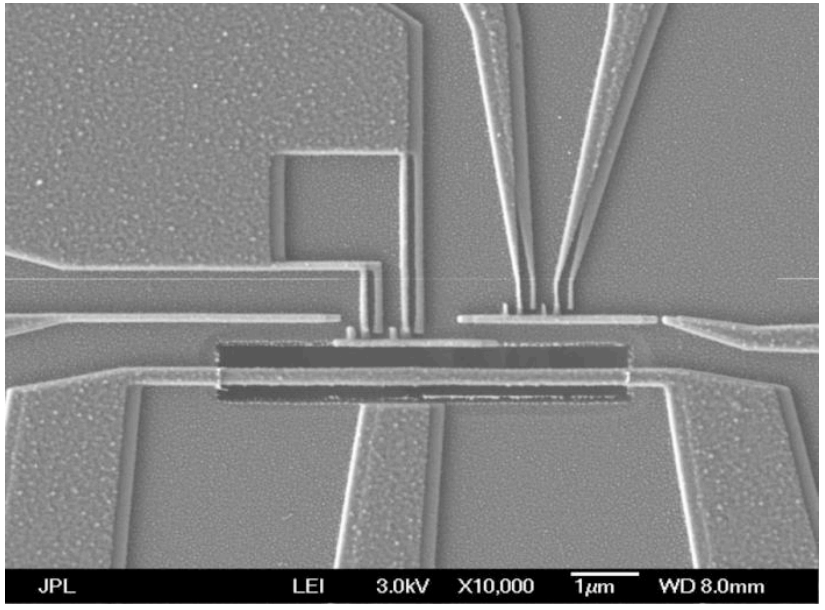
(b)



(c)



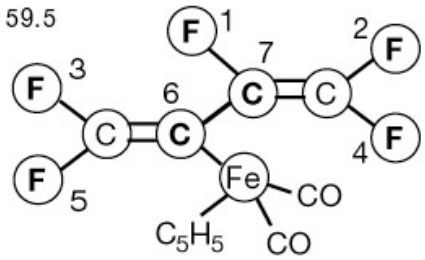


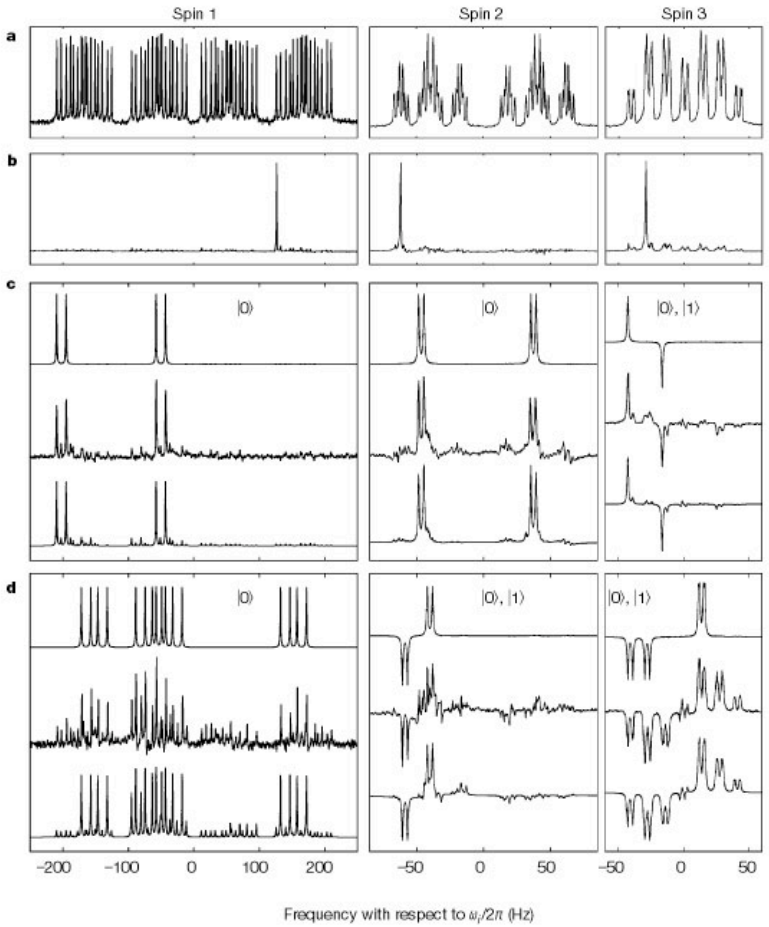


USC

Liquid-State NMR

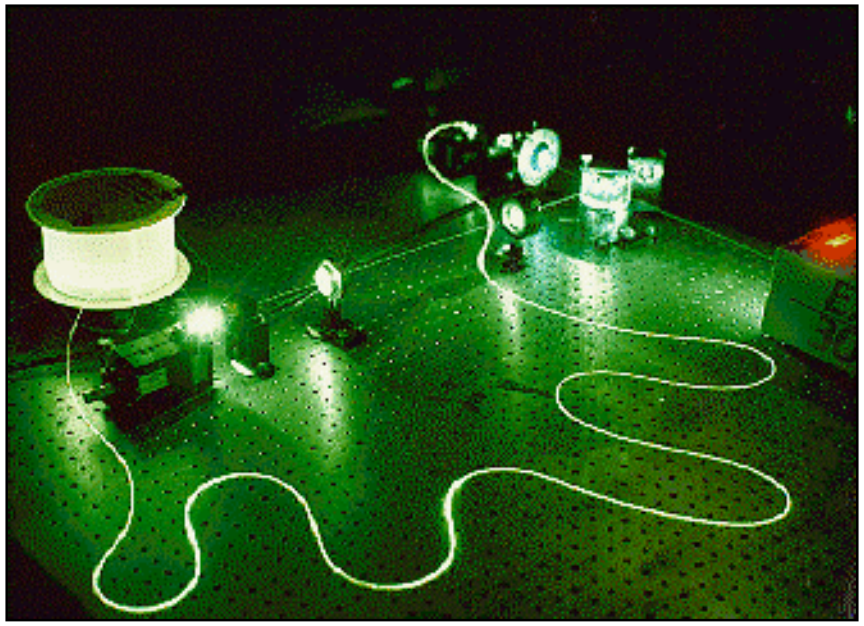
i	$\omega_i/2\pi$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	–22052.0	5.0	1.3	–221.0	37.7	6.6	–114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	–3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	–13.5	41.6	12.9		
4	–4918.7	10.0	1.7	54.1	–5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	–4519.1	45.4	2.0	68.9					
7	4244.3	31.6	2.0						

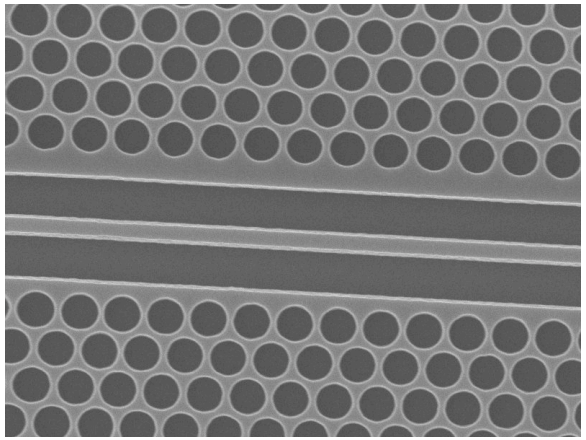




USC

Optical implementations





The Future

Quantum computing technology will only continue to improve. At the moment we are at the dawn of the vacuum-tube era. It is impossible even to predict what technology will win out in the long term. This is still science--but it may become technology sooner than we expect!

Theory also continues to advance. Researchers are actively looking for new algorithms and communication protocols to exploit the properties of quantum systems.

Quantum computers can be used to efficiently simulate other quantum systems. Perhaps some day quantum computers will be used to design the next generation of classical computers!

USC

More Information

List of books on Quantum Information http://qserver.usc.edu/confs/books.html

A Very Basic Tutorial on Quantum Computers http://arxiv.org/abs/quant-ph/0305045

Qwiki (Quantum information Wiki) http://qwiki.stanford.edu/wiki/Main_Page

Institute for Quantum Information (Caltech) http://www.iqi.caltech.edu/

Qubit.org (Oxford and Cambridge) http://www.qubit.org/

Institute for Quantum Computing, Waterloo, Ontario http://www.iqc.ca/

Center for Extreme Quantum Information Technology at MIT http://xQIT.mit.edu/

USC

My Homepage http://almaak.usc.edu/~tbrun/

tbrun@usc.edu

Evolution of quantum systems

Quantum states evolve in time according to the Schrödinger equation:

$$d|\psi\rangle/dt = -i\hat{H}(t)|\psi\rangle/\hbar,$$

which implies that time evolution is described by unitary (linear) transformations:

$$|\psi\rangle \rightarrow \hat{U}|\psi\rangle.$$

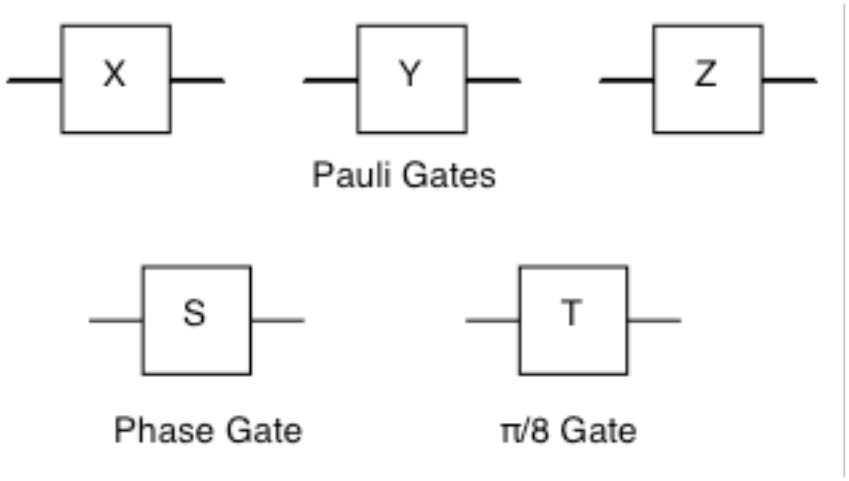
$$d\hat{U}(t)/dt = -i\hat{H}(t)\hat{U}(t)/\hbar.$$

...while this is a photo of an actual laboratory.

USC

Quantum Circuits

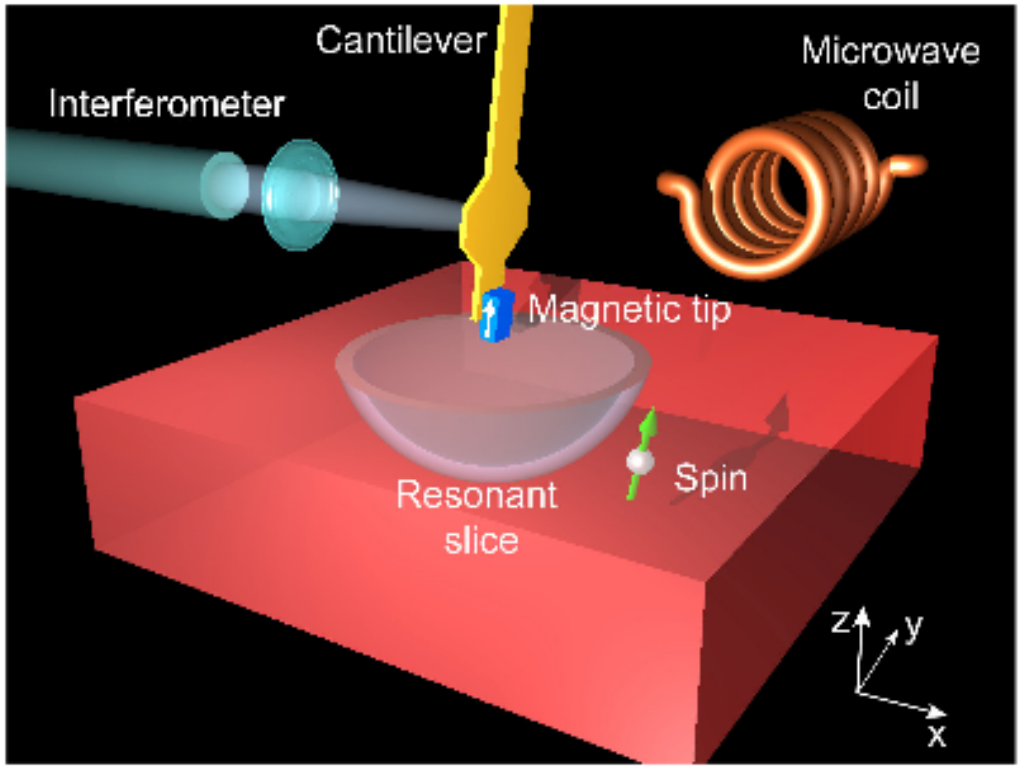
Quantum circuits are a way of representing unitary transformations as a composition of simple unitaries acting on one or two q-bits at a time. These simple unitaries, by analogy with classical logic gates like AND, OR and NOT, are called quantum gates.



$$\hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \hat{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

USC

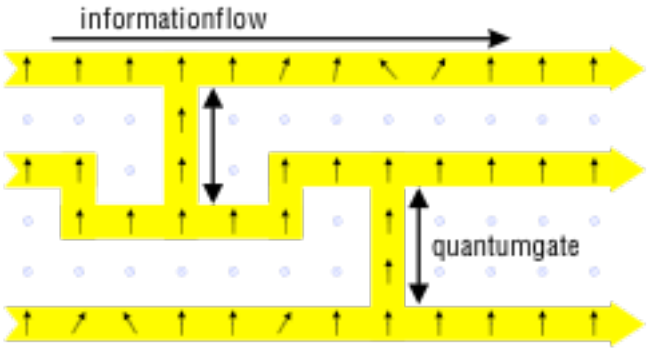
Magnetic Resonance Force Microscopy (MRFM)



MRFM is an experimental technique for measuring the spin of a single electron on a solid surface.

USC

Other models of quantum computation



In cluster state quantum computing, the q-bits are prepared in a massive entangled state, and the computation is done by a sequence of one-bit measurements.

In adiabatic quantum computing, the q-bits are prepared in the (known) ground state of a Hamiltonian, and the Hamiltonian is then slowly and continuously altered to become a new Hamiltonian, whose ground state represents the solution to a problem.

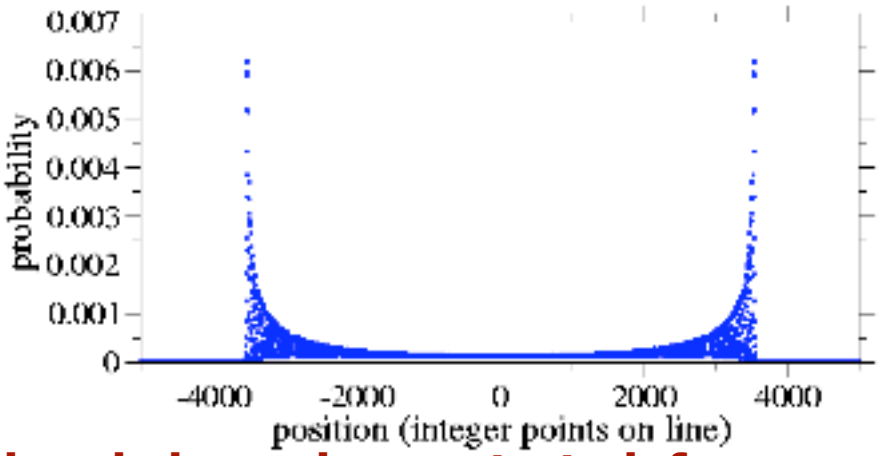
Both of these are equivalent in power to the circuit model, but give new ways of looking for algorithms.

USC

Quantum Walks

Quantum walks are unitary analogues of classical random walks, in which a quantum system moves in a superposition of all directions! Interference can then reinforce the probability of arriving at a desired location, while reducing the probability to arrive at undesired locations.

Many classical probabilistic algorithms are built around random walks (such as the algorithm for 3-SAT). It is hoped that quantum walks will lead to new, faster algorithms as well.



At least one such algorithm has already been demonstrated, for element distinctness, with a polynomial speed-up over the best classical algorithm (Ambainis, 2004).

USC