Christopher Evans
Honors UP II Spring 2010
Dr. John Stewart and Justin Mitchell

Although classical information theory has revolutionized modern life, the discrete state of classical bits limits the computational capacities of the standard computer. Quantum information theory, or quantum computation, is an extension of the model for information theory that incorporates quantum physics and drastically alters the computational power in a way that allows for simultaneous calculations. Such an extension also introduces problems inherent in quantum physics, such as the Heisenberg uncertainty principle. This principle alone complicates the basic error-checking algorithms used for data channels, the way in which one duplicates data, and the way in which data is transmitted.

The classical Shannon bit, the foundation of modern computing, was the product of the first substantial consideration of information theory, or the theory of how information can be encoded and transmitted through physical channels. Developed by Claude Shannon, this most fundamental inquiry into information theory addressed issues such as the way in which information is encoded, the channels through which the data is transmitted, the maximum transmission rates of data, and the complications of 'noise' or interference on the communication channel. All of these issues present themselves in several levels of complexity within the field of quantum computation.

The basic unit of quantum information theory, the qubit, is a derivation of the classical Shannon bit. While the Shannon bit can exist in a state of 0 or 1, the qubit can be 0, 1, or in a superposition of those two states, i.e., it can be 0 and 1 simultaneously, with a probability associated with each value (Lomonaco 2009). The typical implementation models for quantum computation base themselves around the quantum polarization states of light, using a

photon as the basic building block of a bit. In this instance, a photon can have vertical polarization, $|\updownarrow\rangle$ which will be the equivalent of a 1 bit for the classical theory. The photon can also have horizontal polarization, $|\leftrightarrow\rangle$ which will be the quantum analog of a 0 bit. Alternatively, and this is the major departure from classical theory, the photon can be in a 'superposition' of these two states, essentially being 0 and 1 at the same time. Mathematically, ket vectors in a Hilbert space *H* describe the states of a quantum system. (Lomonaco 2009)

To begin this description, one chooses an orthonormal basis from a finite-dimensional vector space, such as: $\{|x_i\rangle : i \leq n\}$, this allows us to represent any state of our quantum system as a linear combination of the basis elements, with the restriction that the norm of the state is of unit length. One chooses the orthonormal basis freely, up to the restriction that it represents a physical observable of the system that can take up to *n* distinct values. The linear combination of the basis elements is what yields the superposition states of the system. Rigorously, the idea of a physical *observable* is self-adjoint operator on a Hilbert space (Lomonaco 2009). Now, to construct a *register* of quantum bits that will allow for computational manipulation of the bits, we enter the realm of multilinear algebra, and introduce the *tensor product.* If we want a quantum register of 8 bits, we take the 8-fold tensor product of Hilbert spaces as below:

$$H_1 \otimes H_2 \otimes H_3 \otimes H_4 \otimes H_5 \otimes H_6 \otimes H_7 \otimes H_8$$

For quantum computation, this construction is usually restricted to 2 dimensional Hilbert spaces, and for an arbitrary m-fold tensor product, a space of dimension 2^m is achieved. And since qubits can exist in superpostional states, m-qubits can hold 2^m values at one time, instead of only one of those values, which is the case with Shannon bits. This computational

quality has enormous benefits for algorithmic operations that require excessive computing power, such as modern-day cryptographic systems.

Modern day cryptography uses 'computationally difficult' problems to encode information. Most prominent of these problems is the factorization of large numbers. There is no known algorithm that can, in polynomial time on the size of the number, factor a number into its prime divisors. Admittedly, this is a simple problem for smaller numbers, but as number reach hundreds of digits, this becomes computationally unfeasible. Essentially, one is forced to check all prime divisors that lead up to a number, and since a classical processor can only perform one operation per bit at a time, the number of bit-operations becomes prohibitive. Quantum computation allows 8 qubits to store a total of 256 values at once. This also implies that performing an operation on 8 qubits allows you to perform 256 calculations simultaneously. This significantly reduces the memory and time capacities necessary to perform factorization of large numbers. Peter Shor developed an algorithm that utilizes this property and could theoretically perform factorization in polynomial time, this discovery provided the first real application of quantum computers that was otherwise impossible on classical computers, and created the first real push toward the construction of a working quantum computer (Steane, 1997).

Another common problem in computer science, searching algorithms, has interesting solutions in quantum computing utilizing the same advantages mentioned earlier. For *n* data elements stored in a random, unsorted fashion, it takes, on average, *n/2* computations to determine if a given element is in the set. This is the best a classical computer can do. For quantum computers; however, the results are far faster. Since quantum bits can utilize superpositional states, the quantum computer can search the same data set in $\sqrt{n}$ steps, based

on an algorithm published by Lov Grover (Steane, 1997). This achievement is possibly primarily because quantum computers do not need to evaluate the information bits nearly as often as classical computers do. They can simply perform operations, and evaluate the final result.

The cornerstone of any computational model is the set of logic gates used. For classical information theory, common gates like the NOT, XOR, AND, NAND, and OR gates are used in integrated chips. Logic gates such as these form the foundation of modern computing, interpreting classical bits as yes/no values and performing Boolean logic. Similarly, the theory of quantum computation involves its own set of quantum logic gates, some of which have direct analogues to classical logic gates, and others that are entirely distinct. Of particular interest are the single qubit logic gates. There is only one single bit logic gate for Shannon bits, the NOT gate that is an involution on the set $\{0,1\}$, but there are numerous single qubit gates, depicted below using matrix representations and a standard qubit $\alpha|0\rangle + \beta|1\rangle$.

The quantum NOT gate is represented as: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

With our standard vector, $\alpha|0\rangle + \beta|1\rangle$, in vector notation, $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

The X gate performs the following operation: $X\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$

(Lomonaco, 2009)

Now, the requirements for our quantum states specify that each vector have unit length, and the matrix operations that specify our quantum logic gates much preserve this unit length, which is equivalent to requiring that the matrix representation be a *unitary matrix*. Two more

important quantum logic gates are the Z gate and the Hadamard gate, whose matrix representations are given below (Chuang and Nielsen, 2001) :

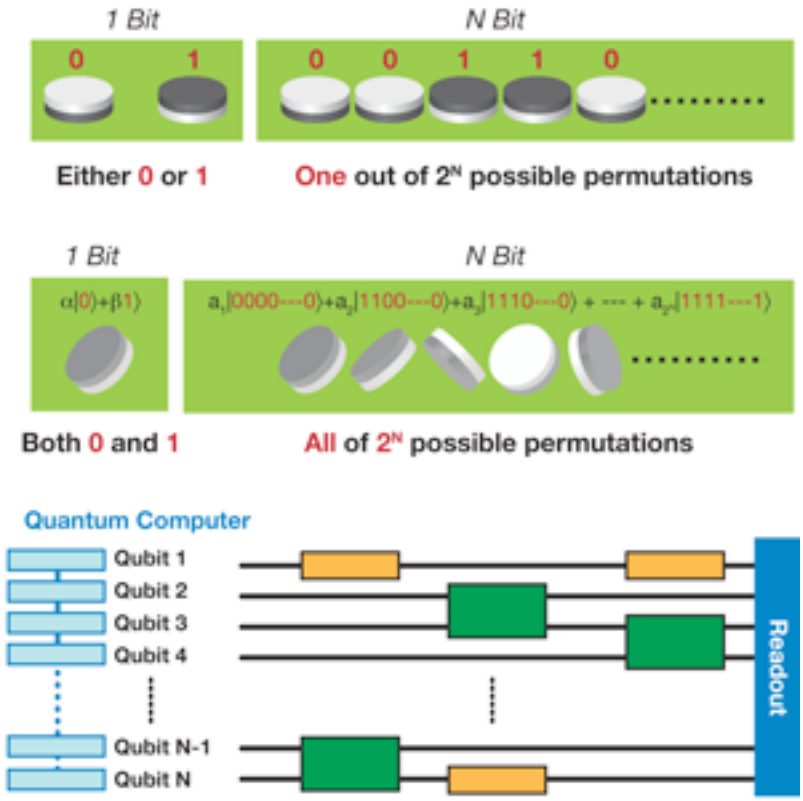
$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Now, the restriction that the matrix representation of a quantum logic gate be unitary delivers enormous power into the quantum computer because any unitary matrix is invertible, which implies that any quantum logic gates is also invertible. Most classical logic gates are not invertible, such as the XOR gate. That is, given the output of an XOR gate, it is impossible to deduce the given inputs. Another benefit of quantum logic gates is the following observation: the CNOT gate, depicted below, is the quantum analog of the NAND gate, that is, any compound quantum logic gate can be constructed from CNOT and single qubit gates.

The CNOT gate on the amplitudes $|00\rangle$ $|01\rangle$ $|10\rangle$ and $|11\rangle$: (Lomonaco, 2009)

$$|00\rangle \rightarrow |00\rangle;\ |01\rangle \rightarrow |01\rangle;\ |10\rangle \rightarrow |11\rangle;\ |11\rangle \rightarrow |10\rangle$$



The upper portion of the photo indicates the number of possible qubit states versus a classical bit, while the lower portion is a schematic model of quantum computation, where single qubit (orange) and double qubit (green) logic gates operate on quantum information. Photo courtesy of: http://physics.aps.org/articles/v1/35

However, quantum logic gates also introduce one of the foundational complications in quantum computing, the no-cloning theorem. In classical computation models, the duplication of information is simple and straightforward, you simply use a classical CNOT and an input *x* that returns two bits in the same state as *x*. It turns out that this is simply impossible to do with quantum information (Steane, 1997). In the field of quantum information theory this is known simply as the no-cloning theorem and is formally stated as follows: "An unknown quantum state cannot be cloned," and is easily proved:

Proof:

To copy a quantum state, a pair of quantum systems must have a unitary operator applied to them, independent of the actual states involved such that:

$$U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle \Rightarrow$$
$$U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle \; for \;\; |\beta\rangle \neq |\alpha\rangle$$

Now, suppose such an operator exists and consider the state:

$$|\gamma\rangle = \frac{|\alpha\rangle + |\beta\rangle}{\sqrt{2}} \Rightarrow$$
$$U(|\gamma\rangle|0\rangle) = \frac{|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle}{\sqrt{2}} \neq |\gamma\rangle|\gamma\rangle$$

And the supposed method of cloning fails. (Lomonaco, 2009)

When quantum mechanics were first proposed, Einstein, Podolski, and Rosen presented what is now known as the EPR paradox. The EPR paradox concerns the phenomena of quantum entanglement, where two particles that are non-interacting and separated by space have qualities that are dependent on each other (Bouwmeester, Ekert, Zeilinger, 2000). This paradox initially appeared to present a problem with non-relativistic quantum mechanics, but together with the no-cloning theorem, the EPR paradox solidifies the theory of quantum information theory, since without the no-cloning theorem, the EPR paradox would allow for communication past the speed of light (Steane, 1997). In another paradigm, the no-cloning theorem produces an excellent result. The primary problem with the no-cloning theorem is that one cannot read, or measure, quantum information without altering its superposition in the process. This similarly implies, that on quantum information channels, the presence of an eavesdropper would create an excessive level of error in the quantum channel, and revealing themselves. This is not the case with classical information channels, which almost exclusively

allow individuals to eavesdrop on the data being transmitted without alerting the users of the information channel (Hayden, 2009).

Nonetheless, quantum computation has more issues to deal with. Classical information theory understood the problem of transmitting data along noisy channels, where interference corrupts data transmission. Since all channels will have some noise, finding a way to counteract random and predictable noise was necessary. In the classical world, the field of coding theory deals with propagation along noisy channels and error-correction. While contemporary algorithms are more sophisticated, they typically have foundations in Hamming coding theory. Simplified Hamming coding theory is fairly elementary in that it simply takes the information a bit at a time, makes several copies of each bit, and then sends all of those copied bits together. At the receiving end, the computer reads a string of bits, and selects the most frequent one. In this way, random error is corrected, since the probability of most of the bits being altered is (generally) lower than the probability that most of the bits arrived uncorrupted (Gottesman, 2009). But, due to the no-cloning theorem and the Heisenberg uncertainty principle, even this most simple of error correcting codes is useless, since the data can neither be interpreted to see which data has been corrupted, nor can it be duplicated in the first place.

Error in quantum channels comes primarily from three sources. The bit-flip error, the phase change error, decoherence, and accidental rotation:

$$\text{Bit Flip X: } X|0\rangle = |1\rangle, \;\; X|1\rangle = |0\rangle$$

$$\text{Phase change Z: } Z|0\rangle = |0\rangle, \;\; Z|1\rangle = -|1\rangle$$

Decoherence is the total disruption of the quantum state, and rotations are simply rotations. (Gottesman, 2009)

The solution to this fundamental problem lies in quantum logic gates. One can use quantum logic gates to measure not the data, but the difference in the data. In other words, if you send several versions of the same bit, the individual or device receiving that bit can simply use a quantum circuit to deduce which of the bits are different from each other, without disrupting the superpositions. This preserves the data that is encoded in the bit, and still allows one to measure error and correct it. This method also circumvents the no-cloning theorem. Instead of copying the bits involved, we simply replicate the computational basis, instead of copying the entire bit. In formulae:

$$\alpha|0\rangle + \beta|1\rangle = \alpha|000\rangle + \beta|111\rangle \neq 3\left(\alpha|0\rangle + \beta|1\rangle\right)$$ (Gottesman, 2009)

This is a very simplistic error-correcting code that only works only on channels with minimal noise levels, and only corrects errors in which a single bit of data accidentally becomes interchanged. Combining this code with the Hadamaard logic gate mentioned previously allows one to simultaneously fix two of the major sources of error: bit-flip and phase-change errors. Correcting other sources of error becomes more complicated, but it is worth noting that theoretically feasible codes do exist which mitigate the noisy-channel problem (Gottesman, 2009).

The issue of outside interference is a critical problem to the actual realization of quantum computers. (Steane, 1996) This is particularly problematic due to the nature of quantum mechanics. Classical computers can operate with some high levels of interference, since the distinction between the discrete states of classical bits is conducive to higher levels of interference, while the more continuous nature of quantum states is far more sensitive means that even small fluctuations in the quantum state produce large changes in the actual value. Quantum noise affects all levels of quantum computation from implementing logic

gates to transmission of information over distances. The accuracy, or fidelity, of quantum information decreases as the distance over which data transmission occurs is increased (Steane 1997). This is due to more prolonged exposure to noise and interference, which provides more opportunities for the superposition of the qubits to be altered, resulting in decoherence. The concepts of entanglement and quantum teleportation are of critical importance to transmission of quantum information (Sloqvist 2008). The National Institutes of Standards and Technology has used an 'ion trap,' pictured below, along with laser manipulations to transfer quantum information from one atom to another using these principles.

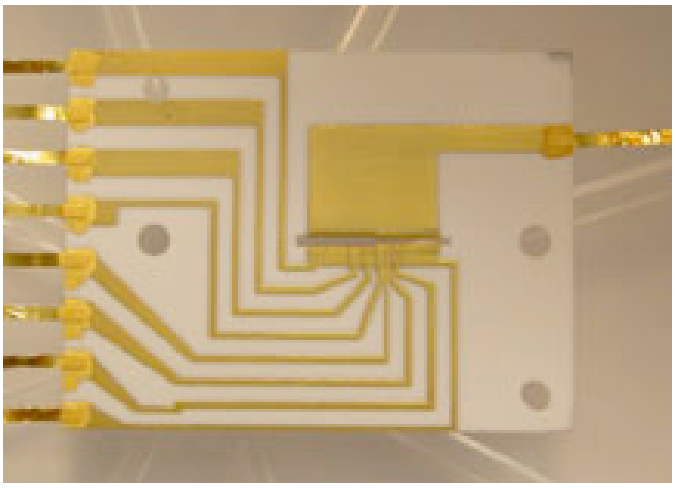


Photo from: http://www.nist.gov/public_affairs/releases/teleportation.htm

A schematic of a large network of these 'ion traps' that has been proposed is also given below:

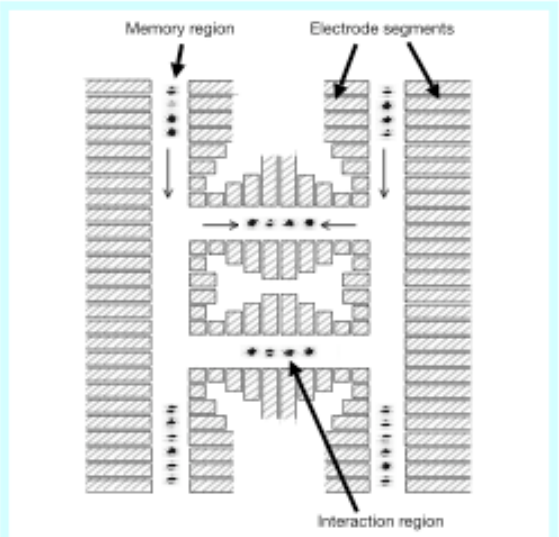


Figure 1 Diagram of the quantum charge-coupled device (QCCD). Ions are stored in the memory region and moved to the interaction region for logic operations. Thin arrows show transport and confinement along the local trap axis.

Photo from: Nature, volume 417, 13 June 2002. P. 709

This diagram, which uses small ion-trap quantum registers uses Coulomb interaction between ions to transfer quantum information, and make the realization of quantum logic gates a reality. This concept, unlike photon-coupling, has been experimentally tested (as discussed above) (Klelpinskl, Monroe, Wineland; 2002).

The field of quantum computation is highly dependent on discoveries and innovations in quantum physics, and the development of technology that will allow the isolation of quantum computers from outside interference, a technology that will be far more complicated than the steel shells that provide shielding for modern computers. While advances in the physics of photons appears to provide promising results for quantum transmission channels, many physicists remain pessimistic concerning the construction of quantum computers (Cambride, Center for Quantum Computation). Steane offers a good synopsis of ion-traps and nuclear magnetic resonance that constitute the primary research areas in quantum computers (Steane, 1997). The potential benefits of quantum computers will provide benefits across

society, from intelligence agencies interested in cryptanalysis, to mathematicians and engineers facing computationally difficult problems, and to organizations wishing to capitalize on the security benefits of quantum information transmission.

Bibliography

Bouwmeester, D., Ekert A., Zeilinger, A. *The Physics of Quantum Information* (Germany: Springer-Verlag, 2000).

Chuang I., Nielsen M., *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press, 2001)

Gottesman, Daniel. "Quantum Error Correction and Fault Tolerance" Lecture, AMS Short Course on Quantum Computation, Washington D.C. January, 2009.

Hayden, Patrick. "Concentration of Measure Effects in Quantum Computation" Lecture, AMS Short Course on Quantum Computation, Washington D.C. January, 2009

Klelpinskl, D., Monroe C., Wineland, D.J., "Architecture for a large-scale ion-trap quantum computer" Nature, vol. 417. 13 June 2002 p. 709

Lomonaco, Samuel J., Jr. "A Rosetta Stone for Quantum Mechanics with an Introduction to Quantum Computation" Lecture, AMS Short Course on Quantum Computation, Washington D.C. January, 2009.

Sjoqvist, Erik. *Physics- A new phase in quantum computation* American Physical Society http://physics.aps.org/articles/v1/35

Steane, A. *Quantum Error Correction* Centre for Quantum Computation: Cambridge, UK http://cam.qubit.org/node/64

Steane, A. "Quantum Computing [1997]." Preprint, Department of Atomic and Laser Physics, University of Oxford.

University of Cambridge *A short introduction to Quantum Computation* Center for Quantum Computation: Cambridge, UK http://cam.qubit.org/node/60