Quantum Computing: A Survey

Siddhartha Kasivajhula
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA - 30332, USA
siddhartha@gatech.edu

ABSTRACT

Computers today become faster by becoming smaller. By reducing the size of transistors, engineers are able to fit more of them on a given size microprocessor, thus increasing the processor's computational power. This process cannot continue forever. It has been estimated that sometime within the next two decades, at the current rate, engineers will be faced with the problem of building something that is smaller than an atom. This is as far as our current "classical" computing paradigm will take us. *Quantum computing* is a potential solution to this problem. This paradigm of computing seeks to directly exploit quantum mechanical phenomena to perform calculations or in some way boost computational efficiency. Some problems can theoretically be solved on a quantum computer exponentially faster than on a classical computer. An overview of the subject is provided here with emphasis on quantum information processing and physical realizations of a quantum computer. Included is a brief history of the subject, a discussion of quantum computing notions such as *parallelism* and *entanglement* and their use in quantum algorithms, and conjecture on the prospects and pitfalls of this theory.

Categories and Subject Descriptors

F.0 [**Theory of Computation**]: General

General Terms

Design, Theory

Keywords

quantum computing, qubit, quantum logic, quantum algorithms, quantum parallelism, NMR, entanglement, EPR, decoherence

1. INTRODUCTION

The physicist Richard Feynman famously remarked in 1981 that nature was "not classical," and therefore, a *quantum* computer – a computer whose working would be based on quantum mechanics rather than classical mechanics – would be far more powerful than conventional "classical" computers. Close to thirty years later, the field of quantum computation and quantum information is now at a crossroads. Much has been accomplished, but a great deal more remains to be done. These thirty years have seen mathematical demonstrations of the superiority of quantum computation over classical computation, with the discovery of superior quantum algorithms such as Shor's factoring algorithm for factoring numbers and Grover's search algorithm for searching databases. These algorithms are faster than any known classical algorithms that perform the same tasks. That there is great potential in this field, there can be no doubt. But *when* that potential can be realized (if at all) is a subject of debate.

2. INFORMATION, MEASURED.

One of the major breakthroughs in twentieth century science was the quantification of information. The mathematician Claude Shannon, in his landmark 1948 paper, "A Mathematical Theory of Communication,"[3] infused the term "information" with mathematical meaning and measure. In doing so, Shannon fathered the field of information theory. The most fundamental unit of information in information theory is, of course, the *bit*. A single bit of information can represent two values – binary 0 and binary 1. All of classical information theory entails encoding information into, transmitting, and decoding these binary states.

There is a quantum analogue to the bit – the *qubit*. The qubit is represented mathematically as a two-dimensional *vector*. Unlike its classical counterpart, the qubit is not limited to only two values. In fact, it can occupy an infinity of states between "0" and "1"[1]. The quantum "0" and "1" states are duly represented as vectors, and they form the canonical basis[2] for the qubit. The state of any qubit will be some superposition of these two basis vectors. For simplicity, vectors will from here onwards be represented by the following notation (known as Dirac notation):

---

[1] However, this does not mean that a single qubit can hold infinite information. It has been proven that a single qubit can usefully hold only as much information as one classical bit[1]

[2] The canonical basis, for our purposes, is the simplest set of basis vectors for a given vector space.

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

To clarify the notation: $|x\rangle$ is equivalent to $\vec{x}$

The state of a qubit is represented as a linear combination of $|0\rangle$ and $|1\rangle$. That is, a qubit $|\psi\rangle$ will be represented as:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{1}$$

One of the vagaries in the qubit that follows from the laws of quantum mechanics is that, when measured, the qubit will simply "collapse" to either a $|0\rangle$ or a $|1\rangle$ state, no matter what state it was in *before the measurement*. *Which* of these two states it collapses into is determined by the coefficient of the corresponding vector, which is the *probability amplitude* (see Appendix A) of the qubit collapsing into that state when measured. So, in equation (1) above, the probability of obtaining a $|1\rangle$ state upon measurement of the qubit is $|\beta|^2$. This ability of a qubit to be "both a 0 and a 1 at the same time" before measurement is known as *superposition*.

2.1   Qubit Representations

Qubits are represented in the physical realm by any two-level quantum system. The most popular example is the "spin" of an electron. Any electron is uniquely defined by four *quantum numbers*. One of these, the *spin* quantum number, can have the values $\pm\frac{1}{2}$. The positive value is referred to as the "spin-up" state, and the negative value the "spin-down" state. These represent the $|1\rangle$ and $|0\rangle$ state, respectively. On an interesting sidenote, two electrons can occupy the same point in space at exactly the same time if only they have opposite spins! Clearly, quantum mechanical systems follow different rules than the more-familiar classical systems.

3.   TOWARD A THEORY OF QUANTUM IN-FORMATION

Classical information theory is a well-developed field. Many of the concepts from that theory translate directly into quantum information theory, but many more ideas have to be introduced into this theory to take advantage of quantum effects.

3.1   Quantum Logic

Computations on classical computers are carried out through the use of logical operations which are represented as *gates*. The familiar classical gates are NOT, AND, OR, NAND, NOR, and XOR. The equivalent gates for performing similar operations on qubits have been developed, and are represented (in the linear algebra formalism of quantum mechanics) by 2x2 *unitary* matrices (see Appendix A). The simplest of these is the quantum NOT gate, which is known as the "X" gate. This gate operates by reversing the probabilities for obtaining a 1 or a 0. That is, by *swapping the co-efficients of the basis vectors* in the qubit state. The X matrix, and its operation on the qubit defined in equation (1) are shown below:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X|\psi\rangle = X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle \tag{2}$$

For more information about quantum gates, please consult Appendix B. For now, suffice it to say that it has been proven (though I will not prove it here) that every classical gate can be derived from a fundamental quantum gate[1] through the use of a gate known as the *Toffoli gate*.

4.   ENTANGLEMENT: EINSTEIN'S BUGBEAR

Entanglement is the strange phenomenon whereby quantum mechanical systems become deeply interdependent. For completely entangled systems, measuring the state of one system immediately determines the state of the other, even when no measurement is conducted on the other system. This phenomenon holds true even for systems that are spatially separated by arbitrary distances! Einstein did not like this idea in the least because it seemed to imply that information could be sent faster than the speed of light. In 1935, along with Boris Podolsky and Nathan Rosen, Einstein published a famous paper that presented what came to be known as the "EPR paradox," which was an attempt to show how quantum entanglement, and therefore quantum physics, were inconsistent with accepted theories of physics.

Consider the following two-qubit state:

$$|\psi_B\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3}$$

Here, the $\frac{1}{\sqrt{2}}$ multiplier implies that both the $|00\rangle$ state and the $|11\rangle$ state are equiprobable (P(obtaining $|00\rangle$) = P(obtaining $|11\rangle$) = $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$). Now, if the first qubit is measured and found to be a 1, that immediately means that the system is in state $|11\rangle$, and therefore the state of the second qubit is 1 as well. The same holds for if the measurement results in a 0, in which case the second qubit would have to be a 0 as well. The qubits are said to be entangled. The state described above can be created by passing a qubit through a Hadamard gate and then through a CNOT gate[1] (see Appendix B), and this state is known as a "Bell pair," or "EPR pair." The EPR paradox involves just such a pair, and proves that a measurement made on one qubit in the pair can have an instantaneous effect on the other qubit in the pair, *irrespective of the distance between the two qubits*. Although intended to debunk quantum theory, this paradox only served to strengthen it, and established entanglement as one of the most powerful tools in quantum computation.

It is interesting to note, however, that to achieve this apparent faster-than-light communication across vast distances, the qubits must first be moved away from each other at finite (sub-light) speeds. In an attempt to rationalize this concept of entanglement, we could then liken it to two people, Alice and Bob, making a pact and agreeing to perform a certain ritual at some precise time in the future. In this case, the two conspirators will, to an uninformed observer, appear to be communicating at faster-than-light speeds when they are observed to perform the same ritual at the same time. To fully cement the illusion, Alice and Bob cleverly decide on a certain algorithm that they will follow to decide at what times to perform the ritual in the future. The observer, assuming he has the ability to perceive the simultaneity of Alice and Bob's actions, would be convinced that there is, in fact, some faster-than-light communication taking place

between Alice and Bob. However, if the observer were to interact with either Alice or Bob, preventing them from performing the ritual, the other person would not know of it and would continue to perform the ritual at the decided-upon time, thus destroying the illusion. That is, *unless* of course, Alice and Bob could correctly and precisely anticipate every interaction that would take place in their own futures, so that their "plan" could account for all of them and still maintain simultaneity in their actions. If we apply this analogy to the qubit case directly, we are left with a picture where a qubit avoids breaking the speed of light law laid down by Einstein in his monumental theory of relativity, by having a complete knowledge of it's own future! It is absurd implications such as this one that caused Einstein to dislike quantum physics so. But experiment has repeatedly confirmed quantum theory as the most successful physical theory that we have, its counter-intuitive nature notwithstanding. Surely, we should be able to take advantage of the possibilities that it offers.

4.1 Decoherence

"Measurement" in quantum mechanics is largely *any* interaction of a quantum mechanical system with the rest of the universe. Since measurement forces such a system to collapse into a single state from a superposition of states, any interaction of a qubit with the rest of the universe can cause loss of information. As a consequence of this, it is extremely important to shield qubits from outside influences for a quantum computer to be useful. Decoherence poses one of the most difficult challenges to quantum computing. Fortunately, error-correcting codes have been developed that allow qubits to withstand a certain amount of decoherence.

5. QUANTUM ALGORITHMS

Quantum algorithms are different from classical algorithms in one key respect: they make use of a concept known as *parallelism*. Parallelism may be defined as the ability of a quantum computer to perform an operation on multiple inputs *simultaneously*. This is a critically important concept. It is the opinion of this author that it is this idea, if anything, that is the essence of quantum computing. And it is this that represents the fundamental difference between classical and quantum computing.

Some of the notable quantum algorithms already discovered that are faster than classical algorithms that perform the same tasks are Shor's factoring algorithm and Grover's search algorithm. The problem of factoring may be stated as: "Given a positive composite number *N*, What prime numbers when multiplied together equal it?"[1]. The best classical algorithm to solve this problem takes approximately $O[e^{1.9(ln(n))^{1/3}ln(ln(n))^{2/3}}]$ time[2]. Quantum computing attracted little mainstream attention until the mathematician Peter Shor published a paper in 1994 detailing a *quantum* algorithm for factoring numbers in only *polynomial time*[4]. Shor's algorithm can factor a number in $O[(ln(n))^3]$. The speedup that this offers over classical algorithms is tremendous. A number that would take the fastest computers today millions of years to factor could be factored by a quantum computer using Shor's algorithm in only a few weeks!

6. THE HUNTING OF THE QUANTUM COMPUTER

Armed with the now-powerful theory of quantum information, researchers have been experimenting with many methods of physically implementing qubits and building quantum computers. John Preskill[2] lays out five basic requirements that a particular design must satisfy:

1. **Storage**: Qubits will have to be stored long enough for useful calculations to be performed.

2. **Isolation**: The qubits must be sufficiently isolated from the environment to avoid decoherence.

3. **Readout**: Preparation and measurement of qubits should be efficient and reliable.

4. **Gates**: A universal set of logical operations (gates) should be available for the manipulation of qubits.

5. **Precision**: All operations should be implemented with high precision to ensure reliability.

Several methods have been proposed that meet the requirements detailed above. Three methods which have yielded promising results are:

1. *Ion Trap*

2. *Cavity Quantum Electrodynamics (Cavity QED)*

3. *Nuclear Magnetic Resonance (NMR)*

6.1 Ion Trap

In this design, each qubit is carried by an ion trapped in a radio-frequency field. The state of each ion is a superposition of a ground state $|g\rangle$ and a stable long-lived excited state $|e\rangle$, which are interpreted as $|0\rangle$ and $|1\rangle$.

A laser is used to manipulate and read the qubits. The energy of the laser is tuned to the energy required to cause the transition from state $|0\rangle$ to state $|1\rangle$. A $|0\rangle$ ion, when illuminated, would constantly absorb and re-emit the laser light, while a $|1\rangle$ state would remain dark (since the energy of the laser is not enough to cause the transition from state $|1\rangle$ to a higher energy state). This is how the two states can be differentiated. Individual ions can be targeted easily because of the separation between them that is caused by their mutual electrostatic repulsion.

Logical operations are carried out on the qubits by varying the frequency of the laser. The operation of the first quantum logic gate was demonstrated by Monroe, Meekhof, et. al. in 1995 [10] using this design. They were able to create a quantum XOR gate (also known as the Controlled-NOT gate) using a total of five laser pulses. The frequency of laser pulses was of the order of 100 kHz[5]. Given this data, we can estimate the speed of such a computer in conventional terms: a simple NOT operation would take $\frac{1}{100 \cdot 10^3} \cdot 5 = 50\mu s$. This method is limited in speed by the frequency of the laser. It is physically impossible to increase the frequency of the laser significantly while still maintaining precision in the measurement of the state[2], so the Ion Trap technique does not offer much long term promise, especially considering that computers today perform calculations several orders of magnitude faster than this.

6.2 Cavity QED

This method is similar to the previous one in that a form of "trap" is employed to contain the qubits, and in that a laser is used to cause transitions in qubits. In this case, however, the trap is an *optical cavity*, which is essentially a cavity whose surfaces reflect waves of a certain frequency and thus trap those waves within it[6]. Another difference is that photons, rather than electrons, are the preferred modus operandi here. The two-level system that will be used to represent $|0\rangle$ and $|1\rangle$ is the polarization[3] of the photon, with "vertical" polarization representing $|0\rangle$ and "horizontal" polarization representing $|1\rangle$. A group at the California Institute of Technology headed by Jeff Kimble used this method to physically demonstrate a two-qubit operation[2] defined as:

$$|V\rangle_1 |V\rangle_2 \rightarrow |V\rangle_1 |V\rangle_2$$
$$|H\rangle_1 |H\rangle_2 \rightarrow |H\rangle_1 |H\rangle_2$$
$$|H\rangle_1 |V\rangle_2 \rightarrow |H\rangle_1 |V\rangle_2$$
$$|H\rangle_1 |H\rangle_2 \rightarrow e^{i\Delta} |H\rangle_1 |H\rangle_2$$

This operation changes the phase of the qubits if both are in state $|1\rangle$ (horizontal polarization[4]), and leaves the state unchanged otherwise.

6.3 NMR

This method is the newest, but shows the most promise. This design uses nuclear spin within a molecule as its qubit representation, and a magnetic field is used to establish two distinct nuclear states[7]. This design was considered difficult to implement because normal operating temperatures for the computer (viz. room temperature) are much higher than that required to cause a state transition from a $|0\rangle$ to a $|1\rangle$[2]. This results is a very turbulent system with a large amount of "noise." This problem was only overcome shortly before the turn of the century. Soon afterwards, in late 1999, a 5-qubit quantum computer was built which was capable of performing many logical operations, and was able to employ quantum parallelism in its computations[9]. More recently, in 2001, a 7-qubit quantum computer was constructed at IBM Almaden Research Center[8]. This is the most complex and most powerful quantum computer built to date. The computer can perform Shor's algorithm on 4-bit numbers, that is to say, numbers up to 15. A 7-qubit molecule is used to perform calculations (see Figure 1).

Each of the five Fluorine molecules and the two Carbon-13 molecules function as qubits. Programming and calculations are performed through the use of radiofrequency pulses, and qubits are "read" by magnetic resonance.

Although NMR techniques have shown the best results in practical quantum computers so far, it will be very difficult to use this method to build a quantum computer with more than 10 qubits, while worthwhile quantum computers would likely require thousands of qubits[7]. This limitation (on NMR) arises because increasing the number of qubits in this design can only be achieved by increasing the number of qubits in a single molecule. Unfortunately, this results in an exponential decrease in the Signal to Noise Ratio (SNR)

---

[3]Polarization refers to the plane of oscillation in an electromagnetic wave

[4]The actual design used "circular" polarizations, but for simplicity I am assuming planar polarization
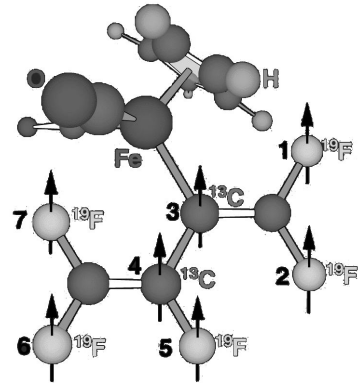

Figure 1: The world's most advanced quantum computer

that can be obtained. Although the SNR is already poor at seven qubits, it is possible at this level to "average out" the random noise to obtain useful results. This will not be possible when there are many more qubits, so other techniques will probably have to be developed before quantum computers can become mainstream.

7. FUTURE DIRECTIONS

In recent times, an alternate paradigm of "measurement-based" quantum computing has been proposed. In this model, logical operations are carried out through measurement rather than through the use of unitary gates. It has been shown that this model can, in spite of its non-unitary nature, be used to efficiently simulate any quantum circuit[12]. First proposed in 2001 by Raussendorf and Breigel[11], this *cluster state quantum computing* technique has received much attention in the past few years, and many have touted it as the biggest development in the field in the past decade. It is still unclear, however, that this model offers significant advantages over previous techniques. Perhaps, at least, there will be advantages and disadvantages that complement those of other techniques already in use today.

8. CONCLUSIONS

Quantum computers are a dream that researchers follow religiously every day. And every day there are new results that both strengthen and threaten the theory of quantum computation. Progress in science is a very strange thing: it is accomplished, more often than not, by researchers using all of the mental faculties available to them in an attempt to destroy new theories. If a theory withstands this incessant battering over time, it is taken more seriously by the scientific community at large and eventually becomes accepted as true. That quantum computation has withstood the power of the finest minds in the world beating down on it for more than twenty years is an impressive feat in itself. It is true that much of the hype surrounding quantum computers is simply exaggerated – just because quantum computers can solve *some* problems exponentially faster than their classical counterparts does not mean that they can solve *all* problems that much faster. In fact, for a great multitude of problems, no quantum algorithm has yet been discovered that is faster than known classical algorithms. Still, quantum computation is a very young field, and it certainly harbors tremen-

dous potential for the future. And that future may only be a few years away.

9. ACKNOWLEDGMENTS

10. REFERENCES

[1] M. A. Nielsen & I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2000.

[2] John P. Preskill, *Course Notes for California Institute of Technology Physics 219*,
http://www.theory.caltech.edu/ preskill

[3] Claude E. Shannon, *A Mathematical Theory of Communication"*, The Bell System Technical Journal, Vol. 27, pp. 379423, 623656, July, October, 1948.

[4] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* SIAM J.Sci.Statist.Comput. 26 (1997) 1484

[5] C. Monroe, D.M.Meekhof, et. al., *Demonstration of a Fundamental Quantum Logic Gate*, Physical Review Letters v.75, 25. 1995

[6] *Cavity Resonator*, encyclopedic article: Wikipedia, the Free Encyclopedia. 2005.
http://en.wikipedia.org/wiki/Cavityresonator

[7] R. W. Keyes, *After the Transistor, the Qubit?*, Computing in Science and Engineering. 2005

[8] IBM Research, *IBM's Test-Tube Quantum Computer Makes History*, Nature. Dec 19, 2001

[9] R. Marx, A. F. Fahmy, et. al. *Realization of a 5-bit NMR Quantum Computer Using a New Molecular Architecture.* Los Alamos National Laboratory Physics archives. http://lanl.arxiv.org

[10] C. Monroe, D.M. Meekhof, et. al., *Quantum Dynamics of Cold Trapped Ions With Application to Quantum Computation* Phys. Rev. Lett. 75, 4714, 1995

[11] R. Raussendorf and H. J. Breigel. *A one-way quantum computer.* Phys. Rev. Lett., 86(22):51885191, 2001.

[12] M. A. Nielsen. *Cluster-State Quantum Computation.* arXiv:quant-ph/0504097 v2, April 14 2005.

APPENDIX

A. LINEAR ALGEBRA SUPPLEMENT

In the linear algebra formalism of quantum mechanics, a qubit state is represented as follows:

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

Quantum mechanics places some constraints on the values that the co-efficients α and β may take. These values represent the *probability amplitudes* for the states they precede in the equation. The probability amplitude is simply that quantity which, when squared, gives the probability (technically, the probability density) of obtaining that state. Therefore:
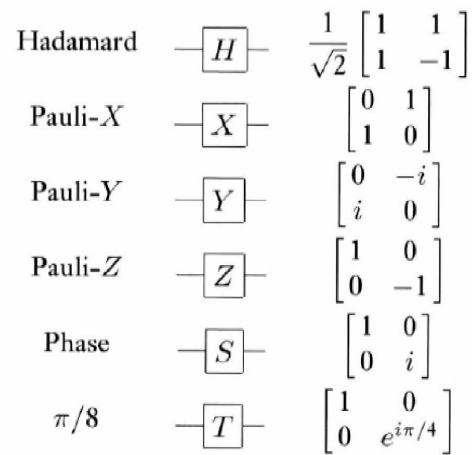
$$|\alpha|^2 + |\beta|^2 = 1$$
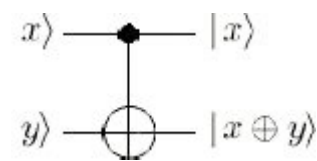

Figure 2: 1-Qubit gates

Figure 3: The CNOT gate

This requirement follows from the certainty requirement that the sum of the probabilities for all events must equal 1.

All quantum operators (also known as gates) must be *unitary* in order to ensure that all qubit states satisfy the above condition. A unitary matrix U is one that satisfies the following condition:

$$U^\dagger = U^{-1},$$

where the † symbol indicates the *hermitian conjugate*, the operation of taking the matrix transpose followed by complex conjugate; and $^{-1}$ indicates matrix inverse. This definition guarantees the following relation, which might also serve as an alternate definition of a unitary matrix:

$$U^\dagger U = I,$$

where I represents the identity matrix.

B. QUANTUM LOGIC GATES

Logical operations may be performed on one qubit, or on several qubits. All important 1-qubit gates are shown in Figure 2.

All multiple qubit operations can be achieved through the use of a "Toffoli gate" known as the Controlled-NOT gate (also known as CNOT gate or quantum XOR gate) in combination with other single-qubit operations[1]. The CNOT gate operates on two qubits. The second qubit is "flipped" if the first qubit, known as the control qubit, is $|1\rangle$. That is, the gate behaves like an X gate if the control qubit is 1, and otherwise does nothing. The CNOT gate is shown in Figure 3.

The $\oplus$ symbol in the diagram represents *modulo 2 addition* in this case. In general, for dimensions d greater than 2 (the dimension of a qubit is 2), it represents *modulo d addition*.