

Quantum Computing Hierarchy

ECE725 Dr. Doug Barlage
Theodore Harris

Abstract

As Moore's law stagnates, the critical lengths of today's technology approach the nanoscale regime, and reach the physical limits of what is possible. Quantum computers (QC) are an option to the next logical step past conventional transistor-based logic. This paper will introduce the basic principles of quantum mechanics that QC's are based on. The fundamental differences between classical bits, and gates, and quantum bits and gates will be made apparent. Two of the most promising devices to be used in quantum computing, the SQUID, and spin-based quantum dot pair will be explained. The limitations that are holding QC's back will be discussed, and lastly the implications of the recent release of a commercial product will be addressed. Quantum computers offer an enticing glimpse into the kinds of computational problems that will be possible in the future.

Introduction

The principle characteristics that govern the behaviour of particles are used to an advantage in QC's. The properties utilized for operation are superposition and entanglement. The information observed from a QC will be shown to be a superposition. When entangled, quantum states are described relative to one another, though separated, e. g. one electron has spin up, while another is always spin down in reference. Each QC device discussed here uses both of these properties.

Classical computers start at the bit level. Logical gates operate on the bits, and computers are made up of these gates. So too do QC's follow this hierarchy. This paper will follow the quantum computing hierarchy to show the relation of qubits, to quantum gates, to the devices themselves, to solving actual problems. Each of these elements in

the hierarchy must be understood as a whole in order to understand QC's.

Q-bits (Qubits)

To describe the meaning of qubits, one could start by considering scaling a classical bit down to the smallest possible ideal value, which would be one electron. It is understood that classical bits are either 1 or 0. As devices scale down to the atomic regime, this could become a reality as Moore's law progresses. Some characteristic of the electron must be observable to denote either a 1 or 0. Examples of quantum quantities that could be measured to denote binary 1 or 0 are its presence (location) or spin (+1/2, -1/2). As is understood from quantum mechanics, on this scale, it is not possible to simply ascribe these states due to uncertainty, thus arises the idea of a statistical qubit. Qubits are statistics, like an experiment that has been repeated a large number of times.

Classical bits are 1 OR 0. Qubits are two state systems existing in superposition and can be 1 AND 0. A 3-bit system can store eight numbers; a 3-qubit system can store all eight numbers. It is this mix of allowed states that harnesses the quantum mechanical property of superposition. This is the feature that allows for inherently parallel processing, and where the true power of quantum computing comes from. Here a statistic for a qubit, X , is written as the sum of the probabilities that it is 1 and 0 in complex Hilbert space.

$$|X\rangle = w_0|x_0\rangle + w_1|x_1\rangle = (w_0, w_1)$$

It has been established how qubits differ from the classical bit. The next level up in building a useful computer is to develop the idea of quantum gates.

Quantum Gates

Quantum gates perform operations on quantum superpositions, i.e. qubits. All quantum computing gates are reversible when observed, unlike

conventional logic. Consider the logical OR, for example, is not a time-invertible computational process. If a logical function is

$$A + B = 1$$

representing A OR B is true, we can not deduce the values of the inputs (only that NOT A AND B is false from DeMorgan's theorem). Contrarily, knowing the result of quantum gates, the input(s) can easily be determined. A process is said to be physically reversible if it results in no increase in physical entropy; it is isentropic. There is also logical reversibility, for example, even in conventional logic, NOT gates are reversible. A universal gate is any gate to which operation can be reduced. The classical example of the simplest gate is the Hadamard gate, which is represented by the following block drawing.

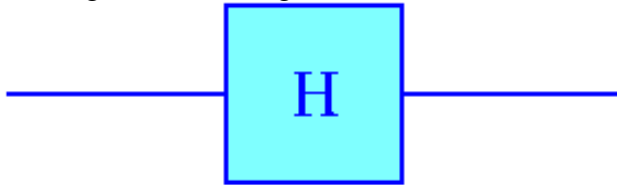


Figure 1. Hadamard Quantum Gate Representation [Wikipedia]

The gate operates on a single qubit by the rotation matrix.

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

It is easy to see how this logic is reversible. Since the rows of the matrix are orthogonal, it is a unitary matrix. Other examples are CNOT, and controlled and uncontrolled classes of gates.

The basic operation of quantum gates has been described so that the physics of the devices now has a purpose, and will be explored in the following sections.

Quantum Dot Pair QC

Two Q-dots fabricated physically close together in a substrate and operated by a DC H-field, as is indicated by the pink downward arrow below. The arrows on the electron denote spin up.

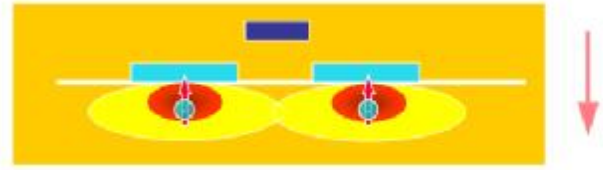


Figure 3. Quantum Dot Pair [K. W. Kim]

This structure can also be operated with a magnetic field applied in the other direction; the electrons will simply rotate the other way around to reach the desired state. The Hamiltonian for a single quantum dot pair is written as follows

$$H = m_B g B_1 S_1 + m_B g B_2 S_2 + J S_1 \cdot S_2$$

[Kim]

Here, μ is the Zeeman term. The Zeeman term is used due to degenerate energy levels of states splitting because of external fields. In this case, the aforementioned external field is the applied DC operational magnetic field. The Zeeman effect is the splitting of a spectral line into several components in the presence of a magnetic field, which is analogous to the Stark effect when an electric field is applied. S is the contact exchange coupling. The contact exchange coupling is the area of overlap between the electron wavefunctions that is needed for entanglement. The exchange coupling is given as

$$2J = \int_V u(\mathbf{r}_1 - \mathbf{r}_2) y_1(\mathbf{r}_1) y_1^*(\mathbf{r}_2) y_2^*(\mathbf{r}_1) y_2(\mathbf{r}_2) dV$$

[Kim].

This is derived using the Heitler-London approximation for excitons. Presumably, to engineer a current in a real-world device, this is necessarily done in three dimensions, including the intersection of the ellipsoid spheres.

In order to write to the qubit, the direction of the spin of the electron may be assigned. In order to change the direction of the spin of the electron to the other direction (1/2), an oscillating magnetic field must be applied parallel to the surface of the substrate, and orthogonal to the applied DC field. The change in the spin of the electron can be understood as a force acting on it by

$$F = qv \times B.$$

This alternating magnetic field must be applied only for a period of time coinciding with a half rotation. The frequency of the alternating magnetic field will be determined by

$$g * m_B B = \hbar \omega = \hbar n$$

where g is the gyration constant, particular to the mechanics of the system, including temperature. μ_B is the Zeeman term, and B is the magnetic field density.

There is the undesired affect of addressing neighbouring quantum dots due to the fact that the magnetic field is in the plane of the substrate, and will pass through each quantum dot on its way. This is overcome by changing the gyration constant, g , of each cell. The addressable precession frequency of the applied AC magnetic field then can be used to selectively address each qubit. Another possible method to address this problem is to have a gradient in the applied DC operating magnetic field, for example, by embedding a gradient of magnetic particles under the qubit array. Though not as feasible or precisely controlled, a gradient in temperature would also serve the same purpose.

For Si, this frequency is on the order of 30GHz. If the structure consists of unmatched dots, such as GaAs and AlGaAs, the gyration constant cannot be accurately predicted, and gate errors will result due to the improper frequency being applied.=

In order to propagate the logic through the quantum circuit and allow the wavefunctions to couple to each other, extra electro magnets can be added above the substrate to block off the communication between the wave functions. This is indicated in figure 3 by the blue box above and between the Q-dots.

Major drawbacks of these devices include the extremely low temperature they must be operated at, and the difficulties mentioned about addressing the proper qubit. The next design to be discussed, the SQUID, attempts to circumvent these flaws by a different approach altogether.

SQUID-based QC

Superconducting Quantum Interference Devices utilize Josephson junctions to couple wavefunctions. When two superconducting regions are isolated, the phases of the Cooper pairs in the two regions will be unrelated. As the separating distance decreases, though they are separated by a very thin insulating barrier, the wave functions will become weakly coupled, and the electron-pairs will be able to tunnel, and the waves functions become coupled [Bland] This is known as Josephson tunnelling, or Josephson current.

$$H = e_i (V_{xi}) S_z^i - \vec{E}_{ij} (\Phi_{xi}, \Phi_e, L) S_x^i$$

In the Hamiltonian, the first term including V_{xi} , is controllable by the gate voltage. The second term is the bit coupling across the junction. Φ_e is the applied magnetic operating flux. The subscripts denoting i 's and j 's describe an array of these devices. This is useful in addressing scalability, one of the major problems plaguing quantum devices today, as scaling up increases decoherence in the system. As mentioned above, the Hamiltonian is relating coupling of Cooper pairs, which in themselves deserve mentioning. Cooper pairs are particular to superconductors. They are a superposition of two electrons' wavefunctions, as they travel through a superconductor. They having opposing spins, entangled with one another, one will always have spin $+1/2$ and the other $-1/2$ relatively. The mass and charge is double that of an electron, and the velocity is at the center of the mass of the pair. [Bland] Since the mass is double, they are coherent over long distances, the affect being that they are not scattered. The problems involving these particles are referred to as Cooper pair in a box problems.

In order to do anything useful with the SQUIDs, the initial state must be known. The SQUID can be addressed by applying a magnetic field of a particular strength, as is derived from the above Hamiltonian. The magnetic flux to force the Hamiltonian to zero is given by the following strength,

$$\Phi_{xk} = \frac{1}{2} \Phi_0, V_{xk} = (2n+1)e / C_k \longrightarrow H = 0$$

[You]

The above will become more evident as the quantum phase shift is discussed. The basic structure of a SQUID is represented below.

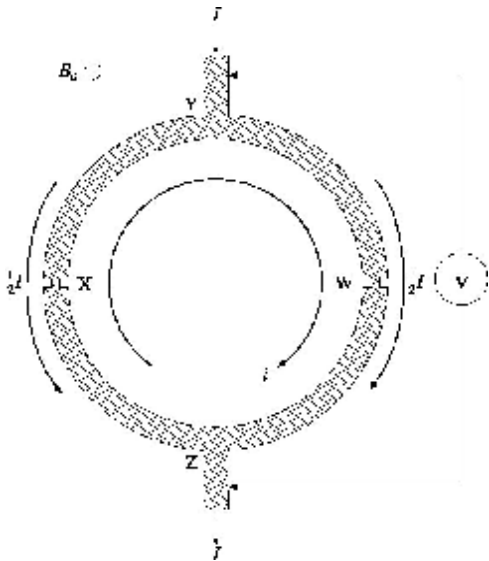


Figure 4. SQUID Diagram [Bland]

In fabrication, a layer of $1\mu\text{m}$ thick superconducting film, such as $\text{La}_{2-x}\text{Ba}_x\text{CuO}_y$, $\text{YBa}_2\text{Cu}_3\text{O}_y$, is deposited by electron beam vaporization. Ion implantation is used to destroy the superconductivity of the central ring. Finally, Au is deposited on top of the conducting ring to function as an ohmic contact, resulting in a $40\mu\text{m}$ loop. The interior Au ring would be removed by a photolithography process. The operating currents around the ring are on the order of $1\mu\text{A}$. It is necessary to shield SQUIDS from magnetic field noise in the environment by high permeability μ -metals composed of Ni, Fe, Mo, and Cu.

On one level, the SQUID is essentially a very accurate magnetic field sensor. The magnetic field measured is perpendicular to the substrate. The functionality of these devices is reliant on an application of Ampere's law of Maxwell's equations. Ampere's law,

$$\oint H \cdot dl = I_{enc}$$

relates the magnetic field, \mathbf{H} through a closed loop of material, given in point form as the curl of \mathbf{H} is the current density;

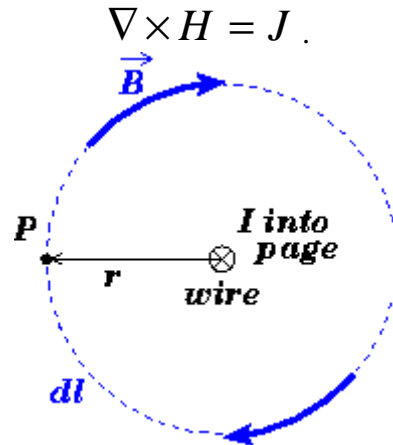


Figure 5. Ampere's Law [Gladney]

The induced current attempts to flow in a path according to the right-hand rule, in order to create its own opposing magnetic field. The SQUID, however, has two sections of thinner material incorporated into its design. These thinner sections are known as weak links and are denoted by X and W in Figure 4. The low current density in the weak links introduces a phase change in the induced current. This also limits the amount of current so that the flux is not cancelled. The quantum condition arises from the fact that the geometry is a ring, thus the phase change around the ring must be $2n\pi$. The change in H field magnitude causes a change in current density, and thus a phase around the ring. By measuring the phase change, a magnetic field can be determined very precisely. The phase change $\Delta\phi$ is a function of magnetic field density, related by

$$\Delta f(B) = 2p \frac{\Phi_a}{\Phi_0},$$

where the Φ_a/Φ_0 term is the ratio of applied and resultant magnetic fluxes through the ring. The constraints applied to the ring are that the wave function and phase shift must be continuous in order to propagate without experiencing destructive interference. There by, the phase shift is prefixed by a quantity of 2π . A further result of this is the resultant magnetic flux will be quantized. Quantum amounts of flux are known as fluxons.

This understanding is analogous to the DeBroglie wavelength constraint of an atom.

The SQUIDs surveyed are operating at a range of temperatures over 4.8K-68K, which are easily attainable. The boiling point of liquid nitrogen is 77K, so liquid He still must be used at a temperature of 1.6K, and a boiling point of 3K.

This is similar to an artificial metamaterial unit cell, however the induced current would go so far as to create a magnetic field that not only subtracts from the applied field, but causes the vector magnitude to go in the other direction.

Now that the properties of QC's are understood, how these properties address mathematical problems will be discussed.

Applications of Quantum Computers

Quantum computers are most suited to solve problems of the set NP-complete. The following conditions may be used to define these sorts of problems, which are mathematically known as "hard problems":

1. The problem is solved by repeatedly guessing answers and checking them.
2. There are a finite number of possible answers to check.
3. Every possible answer takes the same amount of time to check.
4. There are no clues as to which answers might be better.

Examples of these kinds of problems are password cracking, protein folding, and systems of particles. The later type mentioned are highly statistical problems with applications to fields such as physical chemistry, materials science, and quantum mechanics. A QC, after all, is essentially a quantum experiment in a box, so it is naturally adept at such problems.

In complex mathematics, problems are solved in P, polynomial time, the amount of time an algorithm is solved in the worst case size input.

It is desirable to determine which problems can be solved by a Turing machine, and are thereby computable. Some problems are not, such as halting problem, which was proved unsolvable by Turing. A relevant question in computing is how fast a problem can be solved on a Turing machine. Take a class, TIME(n) which consists of all problems that can be solved in time that is linear in input size, and generally a class, TIME(n^c) for input sizes that are polynomial. There exists the complexity class P, which is the union of all of those. P is class of problems that can be solved in time when the input is polynomial in size. In complex theory vocabulary, polynomial time makes problems "easy", contrary to exponential time which is "hard".

NP is the class of problems for which finding a solution may be very difficult, but once it is determined, then it can easily be checked, in polynomial time (known as easy). Consider the factoring problem, which is hard. Given the factors, they can easily be checked by multiplying them together. In quantum mechanics, Shor's algorithm can be used to factor in polynomial time. This algorithm is not in polynomial time on a classical computer. A problem in complexity theory is formally described by a "language". The set of all primes could belong to a language, and a machine could be built which tests whether or not a given input is in the language. The inputs can be small (1) or very large ($2^{100} + 1$), and of course the machine will take longer on the large input than it will on the small input. This running time classifies the difficulty of the problem. Consider a machine that can do primality testing in time n^2 , this means that on a given n-bit long number, it takes some constant * n^2 steps. The factoring language can be described by a set $L = \{(n, p, q): n = pq\}$.

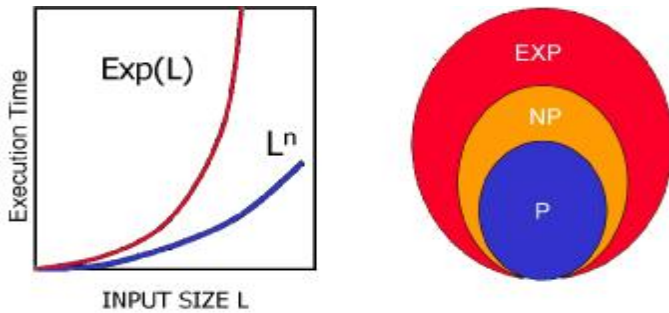


Figure 2. Complexity of Problems, Computation Time [quantiki]

P is the class of problems that can be solved in polynomial time, whereas NP is the class of problems whose solutions can be verified in polynomial time. Clearly P is a subset of NP, since if it is possible to solve a problem, it follows that it is possible to check it.

P and NP sets of problems have been described, now NP-completeness will be discussed. P is a subset of NP, but it is unknown whether or not they are equal. This is because some other algorithm could be discovered that is easy.

The unknown relation whether $P = NP$ or is NP strictly larger. This has not been proven in any matter, and there is a \$1 million reward. NP-complete problems are the "hardest" problems in NP, so if the "hardest" ones can be solved in polynomial time, then everything must be solvable in NP in polynomial time and thus $P = NP$. That said, most people believe P is not equal to NP. [Varia]

Quantum algorithms are largely unexplored, so it is conceivable that some problems have a polynomial time algorithm in the quantum mechanics model, and this would be huge proof that quantum computers are better than classical ones. Already Shor's algorithm has been an example of this; he showed factoring is exponentially faster on a quantum computer.

Shor's algorithm is what originally brought interest to quantum computers in 1994 as useful machines. It is a quantum algorithm which can find the prime factors of large numbers. Today's encryption is secure because factoring is traditionally a computational problem with a huge CPU overhead. As will become apparent, QC's make short work of this problem in polynomial

time, allowing them to factor exponentially faster than supercomputers. Below is an overview of a section of Shor's algorithm (which totals 11 steps).

$$x^r \equiv 1 \% n$$

$$(x^{r/2})^2 = x^r = 1 \% n$$

$$(x^{r/2})^2 - 1 = 0 \% n$$

if ($r == \text{even}$)

$$(x^{r/2} - 1)(x^{r/2} + 1) = 0 \% n$$

Listing 1. Shor's algorithm [adapted from Hayward]

In the above pseudocode, r 's are superposition of states, % denotes modulus division, and there is a Fourier transform is involved. [Hayward] By examination, it can be seen how factors can be resolved, and also how the problem becomes exponentially difficult as it progresses toward the solution. It is well worth noting that all encryption measures in use today, including banking, will become insecure with these developments. Quantum cryptography is a possible solution, but this does not work as simply a stronger encryption. This relies on the quantum property that quantum information is destroyed when observed.

In a system that is inherently parallel, increasing exponentially as more qubits are added to the computer, it can be effective for solving any type of problem, possibly even those for which a very clear algorithm exists. This idea could be very important to artificial intelligence, such that an algorithm to do some chore does not have to be explicitly written, but can be solved nonetheless.

This section will conclude by questioning whether Turing's formalism of computation still holds true, or must be modified for QC's. Turing demonstrated that any computer may be modelled by another and the results will be identical. QC's were shown to be exponentially faster than a Turing machine by Deutsch and Jozsa. QC's are a fantastic way to solve difficult problems that normally require supercomputers, but they are still far from useful. In the next section, the current drawbacks are discussed.

Technological Difficulties

The problems implementing QC's are formidable. Since QC's are so sensitive to magnetic fields (and they must be to detect such small currents), noise levels must be very low. To shield a SQUID from high frequency magnetic fields, mu-metals are employed.

Decoherence can be thought of as dispersion of light in a fiber optic, when it is desirable to keep it confined. On the quantum level, loss of a signal becomes increasingly important, because the signal is physically very small. Qubits must only interact with one another and not affect the environment, thus spreading and being lost.

Another peculiar manifestation of quantum mechanics is that quantum information is destroyed when it is observed, and it cannot be known until it is observed. This is quite different from electronics, where a bit can be read, then some time later, be read again. This property is used as an advantage in quantum cryptography.

A fourth issue is the extremely cold temperatures needed for every device in question. If someday, materials scientists can develop good high temperature superconductors, perhaps SQUIDs can be used much more readily. For the spin-based quantum dot devices discussed, the following must be true:

$$gm_b B \gg K_b T. \text{ [Kim]}$$

This is a difficult constraint, as this is a sub-Kelvin temperature. A goal operating temperature for these devices is that of liquid He is 1.6K.

There are more problems with coherence in solidstate semiconductor quantum devices, but they are still the most promising. These difficulties are labelled technological here because, by definition technology is the tools and methods used to accomplish a task, which improve with time. As technology advances, QC's will become useable. Even with all of these problems, one company thus far has succeeded in releasing a QC product.

Commercial Ventures

The first QC was announced Feb 2007 as commercially available by the Canadian spin-off D-

Wave. It is a breakthrough to finally have a commercial chip that can be bought by anyone that is truly a QC; however the product thus far is more of a proof of concept. As a proof of concept, it may not be particularly useful, and has many disregarding the innovation as hype. Aronson says, "D-Wave's current machine is said to have sixteen qubits. [They hope to reach 1024 qubits by the end of 2008.] Even assuming it worked perfectly, with no decoherence or error, a sixteen-qubit quantum computer would be about as useful for industrial optimization problems as a roast-beef sandwich." At a demonstration by D-Wave, the Orion chip has been shown to solve the following problems:

1. Searching for protein matches. Proteins from a database were fed to the chip for matching, as a maximum independent set problem.
2. Given constraints on which people can not be seated together and who want to sit together at a wedding, find the optimal arrangement.
3. Solving a Sudoku puzzle (presumably without an algorithm).

By this demonstration, QC's were shown to be useful, real products with a market.

Conclusion

The basic principles behind the functionality of quantum computers have been introduced and discussed. The low level foundations of the qubit and quantum gate were discussed. Complex theory, including non-deterministic polynomial problems, has been introduced as is necessary to understand the applications of quantum computers. The ramifications of the superior ability of QC's to break codes will result in a new way to secure data. Two of the leading candidates for functional quantum devices have been explained, the SQUID and spin-based quantum dot pair.

Quantum computers are primitive in development, thus their technical problems have only begun to have been addressed. The problems implementing QC's are greater than those faced by classical computers, and include scalability, decoherence, gate errors, and low operating temperatures. Inevitably these problems will be

diminished as diligent research continues in the field.

Just as was true for conventional computers, as quantum computing develops, new algorithms will be invented and thus new uses for QC's will find fruition. That which seems like science fiction today, will become science fact tomorrow. Just as computers were once only in movies and have since moved into our lives, so too will QC's come into our world.

Sources

1. Quantum Interference devices made from superconducting oxide films, R. H. Koch, C. P. Umabach, P. Chauhari, and R. B. Laibowitz, IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598, 1987
2. A Mössbauer Spectroscopy and Magnetometry Study of Magnetic Multilayers and Oxides, John Bland, Oliver Lodge Laboratory, 2002
3. Quantum Computing Concept and Realization, K. W. Kim, A. A. Kiselev, M. Lashkin, W. C. Holton, V. Misra, North Carolina State University
4. Scott Aaronson, University of Waterloo, <http://scottaaronson.com/blog/?p=198>
5. Image credit: UPenn Physics web page, Larry Gladney
<http://www.physics.upenn.edu/courses/gladney/phys151/lectures/>
6. Wikipedia articles on various topics
7. Frenkel excitons beyond the Heitler-London approximation, Agranovich, V. M.; Basko, D. M, Journal of Chemical Physics, Volume 112, Issue 18, pp. 8156-8162 (2000)
8. K. W. Kim, Private communication
9. M. Varia, Private communication
10. Quantum Computing and Shor's Algorithm, Matthew Hayward, University of Illinois, 2002
11. Scalable Quantum Computing with Josephson Charge Qubits J. Q. You, J. S. Tsai, J. J. and Franco Nori, Frontier Research System, The Institute of Physical and Chemical Research (RIKEN), Wako-shi 351-0198, Japan NEC Fundamental Research Laboratories, Tsukuba, Ibaraki 305-8051, Japan, Center for Theoretical Physics, Physics Department, Center for the Study of Complex Systems, The University of Michigan, Ann Arbor, Michigan 48109-1120