Simulation of Quantum Computation on Intel-Based Architectures

Yan Pritzker
ypritzker@openqubit.org
http://www.openqubit.org

Revision A

...trying to find a computer simulation of physics, seems to me to be an excellent program to follow out...and I'm not happy with all the analyses that go with just the classical theory, because NATURE ISN'T CLASSICAL, dammit, and if you want to make a simulation of nature, you'd better MAKE IT QUANTUM MECHANICAL, and by golly it's a wonderful problem because it doesn't look so easy.

-Richard P. Feynman (1981) (International Journal of Theoretical Physics, Vol. 21, p. 486)

Contents

About the OpenQubit Project

This project began as a hobby but quickly got out of hand. The idea for this project came to me after I had read several books on quantum physics several months ago. I was always interested in the subject, and my honors chemistry class sophomore year gave me some foundation to understand it. Several of the books mentioned quantum computers and simulation thereof. I was disappointed to find out that quantum computers wouldn't be realized physically for several decades, but the prospect of simulation of such computers was very exciting.

I didn't have the mathematical or physical background to even begin to understand quantum computing, so I decided to find help in the Linux community. Linux is a free operating system which has been historically used by mostly programmers.

I founded the OpenQubit organization on December 9, 1999 when I posted an article to a large news site on the Internet (slashdot.org, which gets more than a million hits a month), stating my intentions to create a quantum computer simulation. I was immediately flooded with requests for more information. I organized a mailing list which in the first day gained eighteen members, and within a week was well over 100. Currently, there are 183 subscribers to the list.

The list became a place for physicists, computer scientists, hobbyists, and laymen to discuss a multitude of topics. After talking with some of the physicists, I began to understand quantum mechanics and quantum computing much more. I started writing some basic code for the simulator, and within several days released it to the mailing list. Several other programmers on the list helped me with some other code. Everyone worked on a piece of the simulator. The computer scientists (myself and about five others) would write some code, post it to the list, and then the quantum physicists would tell us where we were wrong and where the code didn't make sense. On February 9, 1999 we finally had a working, stable simulator. It could run Shor's factoring algorithm, which was one of my original goals for the project. Two days later, we released the code to the Linux community through another news site (freshmeat.net).

Currently, the OpenQubit software is in its third revision (series 0.3.x). An article about quantum computing, which will mention OpenQubit, will be published in PC World in May of 1999. The OpenQubit web page is located at *http://www.openqubit.org* (Denmark mirror at *http://dk.openqubit.org*) and the latest source code can be downloaded from *http://www.openqubit.org/code/devel*.

Although the goal of this paper is to introduce the concepts of quantum computing, a firm understanding of the basic concepts of quantum theory is necessary in order to comprehend the nature of quantum computers. A kind of summary of quantum theory is packed into the first ten or so pages in the first section of this paper.

1 Introduction to Quantum Mechanics

Anyone who is not shocked by quantum theory has not understood it.
-Niels Bohr

Quantum theory is, without question, the one greatest achievement of 20th century physics. It is far more significant, direct, and practical than perhaps its rival in greatness, the theory of relativity. Yet it makes some very strange predictions. So strange, in fact, that even Albert Einstein found them incomprehensible and refused to accept the implications of quantum theory, spending a large part of his life trying to find a way around it. Einstein, like many physicists of the time thought quantum theory to be nothing more than a mathematical trick which happened to explain the workings of atomic and subatomic particles, but had no real physical significance (Gribbin, 1984).

In the world of quantum mechanics, nothing is real until an observation is made, and one cannot make statements about things while one is not observing them. Events are governed by probabilities;

a radioactive atom, for example, might decay or it might not. One cannot say what will and will not happen, but can only talk about probabilities of these events occurring. Even Schroedinger, one of the founders of quantum theory, was upset at its implications. He tried to show the absurdity of quantum theory by setting up a thought experiment which would tie together the microscopic world of quantum mechanics with the macroscopic world (Gribbin, 1984).

In this experiment, a radioactive atom which had exactly a fifty percent chance of decaying or not was placed in a room with a radioactivity detector (a Geiger counter) which when set off would break a vial of poison, releasing it into the room which contained a live cat. Quantum theory says that while the atom is not observed, it has neither decayed nor not decayed, and thus the detector has neither been set off nor not set off. Consequently, the cat neither lives nor dies. If one accepts quantum theory and all of its implications, then the cat in the room is neither dead nor alive until someone looks into the room and observes it. Thus, nothing is real until it is observed. This may be a bold claim to make, but this theory nonetheless accurately explains scientific observations. The next several sections will introduce the reader to the concepts of quantum mechanics, and why scientists today believe that quantum theory is a valid explanation for everyday events (Gribbin, 1984).

1.1 The Wave-Particle Duality of Matter

Newton thought that light was made of particles, and he had good reason to believe so. Rays of light were observed to travel in straight lines, as particles do. Light also bounces off of a mirror much like a ball from a wall. However, a contemporary of Newton, Dutch physicist Christiaan Huygens developed the idea that light was not made of particles, but was rather a wave, moving through a substance he called the "lumeniferous ether." This wave theory explained refraction and reflection just as well as the particle theory did. However, certain observed effects could only be explained by the particle theory, so the wave theory was forgotten and discarded. By the early nineteenth century, however, the status of the two theories had become almost completely reversed (Gribbin, 1984; Guillemin, 1968).

1.1.1 Young's Double-Slit Experiment

In 1801, British Physicist Thomas Young designed an experiment that would test whether or not light propagates in the same manner as a wave of, say, water does. Let us examine the nature of water waves in order to understand his experiment better. Suppose one drops two stones into a pond. The stones produce tiny waves, or ripples, in the water. When they are dropped close together, the ripples of one stone interact with those from the other. Because of the oscillating nature of a wave, it happens sometimes that two crests meet and create a bigger crest (or two troughs to create one trough equal in amplitude to the sum of the two). Other times, a crest from one wave meets the trough of the other. In this case, the amplitudes of the waves cancel leaving no wave in their place. This effect of adding and canceling amplitudes is known as *interference* (Gribbin 1984; Guillemin, 1968).

Young decided to test the wave nature of light by setting up an experiment much like the dropping of the stones in the water. He placed a wall with two tiny slits in front of a detector screen. At this wall, he directed a light beam. Because of the effects of diffraction, light on the other side of the wall would spread from each slit in semicircles. Young found that the pattern observed on the detector screen when light was passed through the slits was an interference pattern much like that of the rocks in the water, which appeared on the detector screen as a series of light and dark bands. Thus, Young proposed that light must be a wave since a clear interference effect was observed between the light coming from the two slits (Gribbin, 1984).

There was a remaining question however, if light was a wave, what was the medium through which it propagated? For example, water waves use water as a medium, and radio waves propagate through air. The wave theory seemed to be at last completed when James Clerk Maxwell established the existence of waves as fluctuating electromagnetic fields. This answered the question of what exactly is "waving" in a beam of light. It was the electromagnetic fluctuation that gave light its wave-like characteristics (Gribbin, 1984).

1.1.2 The Discovery of the Electron

In the late 1800s, studies were being done on the discharge of electricity through rarefied gases. During these studies, it was discovered that when very high voltage was put through gases, a beam of something appeared to travel from one end of the gas chamber to another. These beams were named *cathode rays* because they appeared to originate at the cathode, the negative electrode in the gas chamber. At the time, no one really knew what these rays were, but merely that they existed. Some scientists thought that the rays may be a form of light. However, when magnetic fields were brought near the spot the beam made on one end of the chamber, it was deflected. This suggested that cathode rays could be charged particles. The direction of their deflection was consistent with a negative charge. Cathode rays soon became recognized as beams of particles which today are called *electrons* (Guillemin, 1968).

1.1.3 Blackbody Radiation

In the early 1900s, many scientists were attempting to explain *blackbody radiation* which is basically the phenomenon of hot objects glowing with different colors. At this time, the best scientific view of the world required that material objects must be described in terms of particles, but electromagnetic radiation, including light, must be described in terms of waves. Scientists sought to unify the wave and particle theories by looking at how radiation interacts with matter. But instead of unifying, classical physics broke down almost completely (Gribbin, 1984).

A hot object radiates electromagnetic energy, and the frequency of the radiation emitted increases with temperature. Thus, a warm piece of iron emits infrared radiation, invisible to the eye, which gradually increases towards the frequency of red light (at which point we call the object red-hot) and then towards blue and ultraviolet. The electron had only been recently discovered, but it was quite easy to see how a charged part of the atom such as the electron could vibrate and produce a stream of electromagnetic waves. At higher temperatures, it would oscillate more rapidly and thus produce higher frequency waves. The only problem with this theory, a combination of the best of classical theories–statistical mechanics and electromagnetism–was that it predicted a very different form of radiation than was actually observed coming from hot objects (Gribbin, 1984; Guillemin, 1968).

The classical theory predicted that the radiation given off by hot objects would approach infinity as the temperature of the object increased and drop off at zero at extremely low frequencies (low temperatures). This was not the case however; instead of the radiation becoming more and more ultraviolet at high frequencies, it dropped to zero after a certain cutoff point. Thus the predictions of the theory were incorrect and this dilemma is sometimes called the "ultraviolet catastrophe" (Gribbin, 1984).

The theory was not a complete failure, however, as it could explain things at low frequencies. At least the classical theory was half right. The reason for radiation dropping off to zero at high frequencies was somewhat of a mystery. This puzzle attracted many physicists including Max Planck, a conservative scientist whose primary interest was thermodynamics. In 1900 he made a mathematical discovery through desperation, luck, insight, and a slight misunderstanding of the mathematical tools he was using. Planck's formula explained the curve of blackbody radiation, but no one could

explain the physical assumptions that went with the formula. In other words, the solution to the problem was known, but nobody knew why it was the solution. After some more work, Planck found the reason behind the "ultraviolet catastrophe" in what became known as *Planck's quantum hypothesis* (Gribbin, 1984).

Planck said that energy inside the atom could only be emitted in lumps of a certain size, called quanta, which could be described quite nicely by the equation $E = h\nu$ where h is what we now call Planck's constant and ν is the frequency. Planck explained that for very high frequencies, the energy needed to emit one of these energy packets was very large, and thus only a few of these quanta were emitted. This, of course, explains why at high frequencies there was not a lot of ultraviolet radiation given off, but rather the radiation level dropped to zero (Gribbin, 1984).

1.1.4 The Photoelectric Effect

In 1899, Phillip Lenard showed that electrons can be produced by light shining onto a metal surface in a vacuum. This was called the *photoelectric effect.* Lenard looked at the way the intensity of the light affected the way electrons were stripped from the metal. He hypothesized that if he used a brighter light, more energy would shine on the surface of the metal, and thus electrons should be knocked off the metal more rapidly and fly with a greater velocity. However, he found that as long as the wavelength of the light remained unchanged, the electrons flew off with the same velocity. Only the number of electrons ejected increased (Gribbin, 1984; Guillemin, 1968).

Einstein realized that there was a simple way to explain this, provided that Planck's equations were taken as physically meaningful. Einstein simply applied the equation $E = h\nu$ to electromagnetic radiation. He said that light was *not* a wave, contradicting scientific thought for hundreds of years. He said that light comes in packets of energy (quanta) just as Planck proposed the oscillations inside the atom do. Every time this quanta of energy hits an electron, it gives it the same amount of energy and therefore the same velocity. Increasing the brightness of the light means simply increasing the amount of light quanta emitted and thus increasing the ejected electron count. These light quanta are known today as *photons.* This was the work for which Einstein received his Nobel Prize in 1921 (Guillemin, 1968).

1.1.5 The Wave-Particle

So, there seemed to be two conflicting theories. Young's experiments seemed to show that light was a wave, and yet Einstein found that light was made of particles, or quanta. For some time, many scientists struggled with this problem but no one could explain how it could be possible that light was sometimes a wave and sometimes a particle. Physicists finally gave up and came to the conclusion that this *wave-particle duality* simply exists and it must be accepted (Gribbin, 1984).

Niels Bohr proposed the famous *principle of complementarity* which states that one cannot observe both the wave and particle nature of an object at the same time. If one is performing an experiment to test the wave nature of light, he or she will verify it to be a wave. If, on the other hand, one is testing for particle properties, those are the only properties he or she shall observe (Gribbin, 1984).

Louis deBroglie later generalized that all matter has both wave and particle properties and came up with mathematical ways of describing the wavelength of any object. Even macroscopic objects such as tables and chairs have a wave nature; their wavelength is just so tiny that we do not observe them "waving." However, with microscopic objects such as electrons and other small particles, the wave nature is quite visible (Gribbin, 1984).

Although some scientists seemed bothered by the idea that light should behave sometimes like a particle and sometimes like a wave, there really is nothing to worry about. Nature seems to have no problem with light being both a particle and a wave. It is only because of the way we visualize

things that we are confused when we are told that light is both particle and wave in one. There is no reason for light, electrons, or anything in nature to be like anything that we can visualize, or any model that we can invent. So we must simply accept this existence. In fact, *electrons do not really exist, but they could exist, and it is this potential for existence that we call "an electron"* (Gribbin, 1984).

1.1.6 The Double-Slit Experiment, with Electrons

Now, as a conclusion to the wave-particle duality principle we shall examine what happens when we perform Young's double slit experiment with electrons. This experiment really demonstrates quantum theory in its full glory, and Feynman noted that if one comes to terms with the mysteries of this experiment, then every other situation in quantum mechanics can be explained by referring back to this simple, yet interesting experiment (Feynman, 1965).

Recall Young's double-slit experiment discussed in (1.1.1). First let us imagine what happens when we fire bullets, as suggested by Mr. Feynman, at a double-slit setup. Bullets, are of course particles and thus can travel through either one hole or the other. We will place a wall on the other side of the slits, and a detector box on this wall that will count how many bullets land inside it. Thus, if we count the total bullets that passed through the hole and the bullets inside the box, we can calculate the probability that a bullet will land in the detector box (Feynman, 1965).

When we cover one of the holes, we can determine the probability P_1 that the bullet will go through the uncovered hole and hit the detector. Doing the same with the other hole, we discover a probability P_2 for the bullet to hit the detector by going through the second hole. If we now open up both holes, we find that the probability of finding a bullet in the detector is simply the sum of the individual probabilities:

$$P_{12} = P_1 + P_2 \tag{1}$$

Now we will set up a similar experiment with electrons instead of bullets. An electron gun will be the source of electrons. In front of the detection screen we place an electron detector that will make a "click" on a loudspeaker, for example, when an electron arrives. We will also place a detector box as in the bullet experiment to count the probability of an electron landing in there (Feynman, 1965).

When we run this experiment we notice two things. First, we always hear a click when an electron arrives. We always hear a full click, and no half-clicks, for example. We conclude that whatever arrives at the detection screen comes in lumps, or quanta so it must be indivisible, consistent with the particle theory (Feynman, 1965).

Now we close one hole, obtain the probability of the electron striking the detector box and do the same with the other hole. When we open both holes we notice that something strange has happened. The overall probability P_{12} is *not* the sum of the individual probabilities! This effect comes from interference. If we treat the electron as a wave instead of a particle, then we can no longer talk about the probability of the electron arriving at the detector. Instead, we can talk about the amplitude of the probability wave. In quantum mechanics, this probability wave is called the "wavefunction" of a particle. Standard convention is to label the amplitude of the wave as ψ ("psi") or ϕ ("phi"). To obtain the probability of the electron arriving at the detector, we must square the wavefunction. Thus, $P_1 = |\phi_1|^2$ and $P_2 = |\phi_2|^2$. Now, the sum of the probabilities is the sum of the squares of the amplitudes:

$$P_{12} = |\phi_1 + \phi_2|^2 = \phi_1^2 + \phi_2^2 + 2\phi_1\phi_2 \tag{2}$$

There is a third term introduced, $2\phi_1\phi_2$ which is the term that causes the interference. One can see that if one of the waves is negative (at a trough), the probability sum will be decreased, and if

two troughs or two crests meet, then the probability will increase at that point. How could it be, though, that the electron "clicked," on the detector, registering as a particle, yet still managed to interfere with itself like a wave? (Feynman, 1965).

The answer to this is simple, yet strange, and that is the world of quantum mechanics that we must accept. The electron *sometimes appears as a particle, and sometimes appears as a wave.* When we hear it click, we are measuring the particle nature of the electron. When we observe the interference pattern, we see that the electron traveled as a probability wave through both holes. This apparent state of being in both holes at once is called a "superposition of states" (Feynman, 1965; Gribbin, 1984).

Perhaps there is a way to "trick" the experiment. What if we place some sort of detector at the holes so that we can actually observe which hole the electron goes through. We may place a light source at the holes so that we may "see" the electrons coming through. We find, much to our surprise, that the electron now acts just as an ordinary particle, and does not form an interference pattern. It acts like a bullet instead, and the resulting probability distribution on the detection screen is the simple sum of the individual probabilities. What we have done by observing the electron is collapse its wavefunction, restricting its probability wave to a certain subspace. In this case, we have determined the hole that it went through, and thereby turned the wave into a particle because there are no more choices to be made. The reason for this quantum trickery is called the *indeterminacy* or *uncertainty* principle (Feynman, 1965; Gribbin, 1984).

1.2 Uncertainty

Quantum theory places a limitation on the accuracy of measurement. Werner Heisenberg originally stated that if we know an object's momentum Δp, we cannot know its position, x more accurately than $\Delta x = h/\Delta p$, where h is a constant called Planck's constant and equals approximately $6.63 * 10^{-34} J \cdot s$. The units (Joule-seconds) seem strange but they are known as "actions" and are not everyday features of classical physics. An action has an interesting property–it is absolutely constant and has the same size for any observer (this property is shared by the speed of light). The significance of actions became apparent only after Einstein's theory of relativity because it turns out that actions are conserved in space-time. Heisenberg's uncertainty principle talks about the uncertainty of any action measurement (such as that of momentum and position, or energy and time) (Gribbin, 1984).

Basically, Heisenberg said that if we know an object's position with infinite accuracy, we have absolutely no idea about its momentum (i.e. how fast it is moving). Similarly, if we are very sure of its momentum, we have no idea where it is. The physical reason behind this theory is this: in order to "observe" something we need photons to bounce off of this object and enter our eye. For example, I only see a book on my table because millions of photons are bouncing off of it. On the macroscopic level, this seems to have no implications. However, on the atomic level, a photon striking an electron will knock it off course. Thus, if one wishes to measure the position of an electron, the photon we send at it will strike it and modify its momentum (Gribbin, 1984).

Heisenberg's uncertainty principle, in a sense, protects quantum mechanics. Heisenberg realized that if it were possible to measure position and momentum at the same time, quantum mechanics would collapse. We would be able to, literally, find out which hole the electron went through and still observe an interference pattern. Thus he proposed that it was impossible. Then, many physicists tried to imagine creative ways to defeat the uncertainty principle, but no one could do it (Gribbin, 1984).

Imagine for example that we allow the wall through which the electrons pass in the double-slit experiment to move. When an electron comes in, it will deflect from a certain part of one of the hole and thus the wall will get a kick and move in the opposite direction of the deflection. Thus, by not touching the electrons at all and merely by observing the wall we can apparently figure out where they hit (Feynman, 1965).

However, to do this we will need to know accurately the momentum of the wall. The uncertainty principle says that if we measure the momentum of the wall with great accuracy, we will lose accuracy in its position. Thus, an electron flying through will knock the plate off to one side and we will be able to tell either where it is or how fast it is moving, but not both. And we need both to accurately judge where the electron went through (Feynman, 1965).

As a final example, let us see why atoms do not collapse. Although many of us take atoms for granted, the idea of atoms is completely illogical. If a negative charge is orbiting a positive one, it would spiral into the nucleus and the atom would collapse. Atoms are completely impossible from the classical point of view. However, if an electron were to fall into the nucleus, we would then know its position with infinite accuracy, and we would know its momentum at the same time, and this, is quantum-mechanically impossible (Feynman, 1965).

1.3 Philosophical Implications

1.3.1 The Copenhagen Interpretation

The view of quantum mechanics presented above, utilizing wavefunctions and observers collapsing them is known as the Copenhagen Interpretation, named after the home city of Niels Bohr. The Copenhagen Interpretation says that unlike, in the classical world, nothing exists in a determined state until we observe it. In fact, the observer interacts with the system being observed to such an extent that the system cannot be thought of having an independent existence. We cannot say what a particle does, or even if it exists while we are not looking at it. When we perform an experiment we get a set of readings or properties which suggest to us that a certain type of particle exists. Almost every time we repeat this experiment, we get similar readings. But as John Gribbin put it, "the interpretation in terms of particles is all in the mind, and may be no more than a consistent delusion." If we cannot say what a particle does when we are not looking at it, then it is even reasonable to say that the electron did not *exist* before the late 1800s when it it was discovered (Gribbin, 1984).

In quantum physics, one cannot describe the position of a particle in space-time precisely, so in this sense even the theory of relativity is regarded as a "classical" theory. Newton thought that if we could ever measure all the properties of all the particles in the universe, we could determine the future state of the universe because they would follow classical laws.[1] In quantum physics, we cannot perform such a measurement in principle because by measuring position we disturb momentum, and by measuring energy we lose precision in the time the measurement took place. Thus, quantum theory says that the future of the universe is undetermined, a thought that was deeply unsettling for Albert Einstein whose view on the subject was: "I cannot believe that God would choose to play dice with the universe"(Gribbin, 1984).

1.3.2 Many Worlds

However strange the Copenhagen Interpretation is, it seems to be the most widely accepted interpretation, for the second interpretation of quantum physics is perhaps even more unsettling. This second view involves parallel universes existing alongside ours, and although that may sound unusual it is in fact less strange than the Copenhagen Interpretation if looked at closely (Gribbin, 1984).

One of the features of the Copenhagen Interpretation that doesn't make much sense is the concept of the collapse of the wavefunction by the observer. What happens when an observer enters the room where Schroedinger's cat is residing? The wavefunction of the cat is collapsed, but now this observer becomes part of the wavefunction. If he chooses not to tell anyone about what he saw, to the outside world the room with the cat remains in a superposition of states. If he calls up his friend and tells

[1] i.e. objects in motion would remain in motion unless affected by an external force, etc.

him the news, now they are both part of the wavefunction. And this spreads and spreads until, say, the entire universe knows about the cat. But who shall collapse the wavefunction of the universe? By definition, the universe contains everything, so there cannot be an outside observer. Indeed, the Copenhagen Interpretation seems to imply that there is scientific reason to believe in a God! (Gribbin, 1984).

The many worlds theory gets rid of wavefunctions and the need for an observer. There is no such thing as a dead-alive cat paradox because the cat is both dead and alive. It is simply alive in one universe and dead in another. The many worlds theory proposed by Hugh Everett in the 1950s says that wavefunctions do not collapse. All of the possibilities in a quantum state are real all at once, and each exists in its own part of "superspace" (and supertime). When we make a measurement at the quantum level, we are forced by the process of observation to select one of the alternative universes which then becomes real for us (Gribbin, 1984).

Let us visit Schrodinger's cat one more time. The conventional Copenhagen Interpretation tells us that both possibilities of the cat being alive and dead are equally unreal, and only one of them becomes a reality when we collapse the wavefunction of the cat inside the box. Everett's many worlds theory says that both possibilities are equally *real* and that both exist in their own worlds. There is both a live cat and a dead cat, a decayed atom and an atom that never decayed; but they are located in different worlds. Faced with the decision of whether or not the atom should decay, the whole universe split into two versions of itself, identical completely except for the fact that in one the atom decayed and in the other it did not. It sounds like science fiction, but it is really only the consequence of taking the equations of quantum mechanics literally (Gribbin, 1984; Guillemin, 1968).

1.4 Dirac Notation

Without going too deep into the mathematical reasons behind it, Paul Dirac proposed a simple system of notation for describing quantum systems called *bra-ket* (read "bracket") notation. An initial state in a quantum system is represented in bra-ket notation by the symbol $|somestate\rangle$ which is called a *bra* and a final state is represented by the symbol $\langle somefinalstate|$ which is called a *ket.* When these two are put together we get a braket, which represents the phrase "the amplitude that" (Feynman, 1965).

So, if we wanted to describe, in the double-slit experiment with electrons, the amplitude that an electron would arrive at detector x after leaving its initial position s we could write it as.

$$\langle \text{Particle arrives at } x \,|\text{Particle leaves } \, s\rangle$$

It is often convenient to simply abbreviate this to single letter notation such as $\langle x|\ s\rangle$. When we talk about describing a quantum system, we are talking about describing the wavefunction of the system which is the sum of all of the amplitudes for every outcome in the system. Quantum states can be treated as vectors. A completed bracket denotes a dot product so it is is just a number. Because of the nature of waves, this number must be complex[2] (Feynman, 1965).

Let us describe Young's double-slit experiment with electrons using this notation. If we wish to describe a specific route the electron takes, for example from the initial position to hole one to the detector, we can write it as the product of the amplitude to get from the initial position, s to the first hole and from the first hole to the detector at position x:

$$\langle x|\ s\rangle_{\text{via hole 1}} = \langle x|\ 1\rangle\,\langle 1|\ s\rangle$$

In general, we can describe the complete amplitude of going from s to x by using the sum of all the individual routes, conveniently represented with summation notation:

[2]The real part describes the amplitude of the wave, while the imaginary part describes the phase.

$$\langle x|\ s\rangle = \sum_{i=1,2} \langle x|\ i\rangle \langle i|\ s\rangle \tag{3}$$

The vectors represented by i are referred to as base states (base vectors). A base state is one from which all future behavior of the state is determined. i.e. we can say that the base states in our system are the state of the electron arriving at hole one and the state of the electron arriving at hole two. It does not matter where the electron started because whether it arrives at the detector only depends on which hole it went through. Base states must always be *orthogonal*, i.e. their dot product must be zero. This means that we cannot jump from one base state to another (Feynman, 1965).

As shown above, we can represent the wave function of any system by listing the amplitudes from going from any initial state to each of the base states. So, to generalize from (Eq. 3):

$$\langle \chi|\ \phi\rangle = \sum_{i} \langle \chi|\ i\rangle \langle i|\ \phi\rangle \tag{4}$$

Notice, that since this equation uses only closed brackets, it is dealing entirely with complex numbers and no vectors. This is the equivalent of re-writing the all-too-familiar vector equation for force:

$$F = ma$$

into real number form by taking the dot product of both sides by an arbitrary vector C:

$$C \cdot F = C \cdot (ma)$$

but since this is true for any vector C there is hardly a use for writing the C. Going back to our wavefunction equation, we see that both sides are multiplied by the vector representing the final state $\langle \chi|$. So we can simply discard that term from (Eq. 4) to result in the equation:

$$|\phi\rangle = \sum_{i} |i\rangle \langle i|\ \phi\rangle$$

Also, observe that there is a complete bracket, which is the amplitude that ϕ is in the base state i which is also referred to as the coefficient for the base state i. This coefficient can be written simply as a_i. Thus, our final general formula for describing a quantum system is:

$$|\phi\rangle = \sum_{i} a_i\, |i\rangle \tag{5}$$

Remember, that the probability of an outcome is the square of the magnitude of the amplitude so the probability of outcome i is $|a_i|^2$. So, to represent Young's double-slit experiment, once more, with the electron having equal probability of arriving at either hole 0 or 1, denoted by the states $|0\rangle$ and $|1\rangle$, respectively:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

And that concludes our excursion into quantum physics (Feynman, 1965).

2 Quantum Computers

Quantum Computation is a very new field in science. It relates as much to quantum physics as it does to computer science. The concept of quantum computers is currently at a very theoretical stage, as working quantum computers may not be realized for another couple of decades. However, there have been several very promising proposals on their implementation, namely the *linear ion trap* and *NMR* (*N*uclear *M*agnetic *R*esonance) architectures, which will be discussed later. Today, quantum computing is approached largely from the standpoint of simulation, which allows for the development of programs for a quantum architecture on *classical* hardware.

Quantum computers will be radically different from the computers of today. Classical computers, as the computers of today are referred to in the quantum computing field, interpret the movement of thousands of electrons, or lack thereof, as ones and zeros or *bits*. A quantum computer, on the other hand, may function using only several quantum objects such as atoms, ions, or photons, interpreting their states, or polarizations as ones, zeros, and superpositions of ones and zeros(i.e. it is neither one or zero until observed; or, if one follows the many-worlds theory, it is *both* one and zero until observed). Either way, each quantum bit, or *qubit* can exist in a superposition of states with different probabilities of seeing a one or a zero when one observes the qubit (Steane, 1997).

A quantum computer, operates in a memory and efficiency space exponential to its resources. In other words, while a standard computer with three bits can store the numbers 0 through 7, a quantum computer can store all of these numbers in a coherent superposition. The power of such computers comes from the idea of *quantum parallelism.* Classically, we can decrease the time of computation of a certain process by increasing number of processors working in parallel. However, in order to achieve exponential parallelism, we need to add an exponential amount of processors. In a quantum computer, parallelism increases exponentially with the size of the system. Thus, a linear increase in physical space causes an exponential increase in computation power (Steane, 1997).

2.1 Inside the Quantum Computer

If one wishes to keep a superposition of states, one must not observe the state he/she is working with. Thus, it is impossible, for example, to set up a superposition of the numbers one through five, and add it to a superposition of the numbers six through ten, and expect as a result a superposition of the results of each individual addition. This is not possible because by observing the outcome, we will only get *one* of those values. It would seem that this fact removes all superiority from quantum computers, but there is a way around this limitation. Sometimes, we do not need to know the "sum" in order to solve a problem; there may be some other thing that we can observe and use it indirectly to solve the problem at hand. This is the technique employed by Shor's polynomial-time factoring algorithm which shall be discussed shortly. Another technique is to transform the state in order to "amplify" the likelihood of certain outcomes of interest. This technique is used by Grover in his database searching algorithm (Steane, 1997).

2.1.1 The Qubit

The basic unit in a quantum computer is the *qubit,* or *qu*antum *bit*, analogous to the bit of classical computers. The qubit can be represented by any two state system such as the ground and excited state of an ion, the spin of an electron, or the polarization of a photon. For the purposes of quantum computing, the base vectors (states) $|0\rangle$ and $|1\rangle$ in a two dimensional vector space are used to encode the classical bit values 0 and 1, respectively. However, this is where all analogies to classical systems cease, for quantum bits may exist in superpositions of states such that

$$\psi = a\,|0\rangle + b\,|1\rangle \quad \text{where } |a|^2 + |b|^2 = 1$$

If such a superposition is measured, one will get $|0\rangle$ with probability $|a|^2$ and $|1\rangle$ with probability $|b|^2$. Thus, a qubit can be in an infinite number of superpositions, as long as the probabilities of the states add to one (Steane, 1997).

Although a qubit can be in an infinite number of states, it can still only encode a zero or a one. The limit is because one must still measure it to obtain a value. Thus, if one needs to store a number larger than a zero or one, he/she must use several qubits. In a classical physical system of n particles whose states can be described by a vector in two dimensional space–basically, a system with only two outcomes such as one or zero–forms a vector space of $2n$ dimensions. In other words, if there are two classical bits, they can each alone represent only the state zero or one. But when they are put together, they can represent the numbers 00 to 11, which in decimal are zero to three. Thus, two particles can represent four states (Steane, 1997; Rieffel and Polak, 1998).

In a quantum mechanical system, though, the vector space grows *exponentially* with the size of the system. Thus, a three qubit system has an eight dimensional vector space. This system can store all of the numbers zero through seven in a coherent superposition. To understand this better, think of a macroscopic objects that suddenly breaks into pieces. It is possible to describe this object by describing each of its pieces. In a quantum system, this is not true. It is possible to have states that are not describable by their individual particles, which are called *entangled states* which have no classical counterpart whatsoever and which contribute to the exponential space (Rieffel and Polak, 1998).

2.1.2 Measurement

The process of measurement of one or more of the particles in a quantum system results in the vector space of the system being reduced to a subspace which is restricted to the measured value. For example, suppose that there is a two qubit system such that

$$\psi = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

This is a coherent superposition of all of the numbers zero through three. If one measures the first (rightmost) qubit of this system, the system will reduce to one of the following superpositions:

$$\psi = a\,|00\rangle + b\,|10\rangle \text{ or } \psi = a\,|01\rangle + b\,|11\rangle$$

The vector space is reduced because the measurement has restricted the value of the first qubit to either zero or one. Thus the system has gone from being a superposition of four states, to a superposition of only two states. Another measurement will result in the complete collapse of the wavefunction into one value in the set $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ (Rieffel and Polak, 1998).

Measurement can be used to show the entanglement between particles. For example, the first state in this section was entangled because measuring one part of it affected another (i.e. measuring the first qubit to be zero caused the probability of measuring zero in the second qubit to increase from 1/4 to 1/2. On the other hand, neither of the two states resulting from the measurement is entangled because measuring a one or zero in the first qubit of these states does not affect the probability of obtaining a one or zero in the second qubit (Rieffel and Polak, 1998).

2.1.3 Quantum Gates

It is possible to transform quantum states without measuring them. The mathematics of such transformations is complex and will not be discussed, but the ideas will be. Any transformation on a quantum state must be unitary. One can think of a unitary transformation as simply the rotation of the complex vector space. Another requirement is that quantum transformations must be reversible which is due to laws of thermodynamics (classical systems dissipate heat when performing

computations, but a quantum system must maintain its superposition and thus cannot lose any heat, and operations must therefore necessarily be reversible). This is not important to understand in order to accept (Barenco et al., 1995).

Adriano Barenco, et al. showed that all quantum transformations can be built from a basic set of gates which consisted of one bit gates (such as negation and qubit rotation) and the two bit exclusive-or gate (also known as the controlled-not, or CNot).[3] The one bit gates suggested by Barenco, et. al. are the qubit rotation (R_y), the phase rotation (R_z), and the phase shift (Ph). These operations are particularly nice because they are easily implemented using a laser, for example. Using these fundamental operations it is possible to perform any imaginable quantum transformation. It was also noted that any unitary transformation may be represented by a matrix (Barenco et al., 1995).

2.2 Quantum Computing Pros/Cons

2.2.1 Usefulness

Building a quantum computer will be a great technical challenge; are the advantages of building such a computer great enough to face this challenge? One of the primary goals of a quantum computer will be to act as a factoring engine, using Shor's polynomial-time factoring algorithm to quickly factor large numbers. Currently, the best known algorithm for factoring numbers runs in exponential time (i.e. the time to factor increases exponentially with the size of the input) (Preskill, 1996).

Shor's algorithm reduces this time to polynomial time.[4] This means that large numbers that took years to factor before may be factorable in hours or even minutes. The factoring of large numbers is used as a base for todays most secure encryption algorithms including the infamous Triple DES and RSA. A quantum computer will make cracking codes as easy as multiplying numbers. A quantum computer can also be used to create a cryptographical system which is completely uncrackable by any methods but has certain limitations (Preskill, 1996).

Another application, proposed by Grover is a database search algorithm for unsorted data which runs in a time proportional to the square root of the input size. Conventional approaches require a number of comparisons equal to the number of items in the database. This type of algorithm does not have an exponential speedup over the classical search, but it is a large speedup nonetheless. There has not been much more proposed for the use of quantum computers, but as they become more and more developed, new algorithms are bound to show up (Preskill, 1996).

2.2.2 Feasibility

Because a superposition of states may only exist while it is not being observed, a quantum computer must be completely isolated from its environment. If it does interact with its environment, the quantum state is said to *decohere*, or lose its meaning and information. Because of this, it has proven very difficult to build a true quantum computer physically. Optimistic scientists speculate, however, that such a computer may be built within several decades, when technology is sufficient (Preskill, 1996).

Entangled states are especially vulnerable to decoherence since an error in one of the qubits can affect the whole state. In order for a quantum computer to function, it must employ very effective error-correcting techniques. These error-correction techniques must be effective enough that not even one qubit fails during the course of a computation. A problem with error-correcting is that it requires enormous *overhead* (extra resources) both in terms of the number of qubits involved and

[3]The exclusive or is defined as follows: For bits a and b, if a is set, then b is flipped; otherwise b is not changed. The exclusive-or leaves the state of bit a intact, and thus this is a reversible operation because one can always deduce the inital state from the final state.

[4]Specifically, the time to factor increases only as the cube of the input size.

the number of quantum gates needed. This increase in resources, by itself causes more errors to appear. Thus, error-correction will, at best, be very difficult to implement (Preskill, 1996).

2.2.3 Quantum Hardware

There are currently two very promising architectures for physical quantum computers, known as *linear ion trap* and NMR, respectively. Both have shown results that are impressive, but both have their intrinsic limitations. Quantum hardware of the future, will probably not be similar to these proposed architectures (Preskill, 1996).

Simply put, the linear ion trap uses trapped calcium ions (positively charged atoms) and manipulates them by sending photons (in the form of a laser pulse) at them. The frequency and duration of the laser pulse determines how the ion will be affected. Through careful use of the laser, it is possible to perform a controlled-not operation, which has been shown to be universal for quantum computers. The speed of such a computer, however, is limited by the frequency of the laser, which at high frequencies causes instabilities and errors (Preskill, 1996).

NMR, or Nuclear Magnetic Resonance, quantum computer uses the fact that nuclei in a molecule act as tiny magnets when placed in an electromagnetic field and detects their spin (aligned or antialigned to the field) as a logical one or zero. Because this signal from an individual molecule is very small, NMR has to use a group of molecules which are presumed to be in a similar state, and uses "majority rules" to decide which way the atoms are spinning. The problem with NMR is that it is difficult to make sure that all the molecules start in the same state, but two separate solutions to this problem were published in 1997, giving a great push to NMR architecture development (Preskill, 1996).

2.3 Quantum vs. Classical Algorithms

2.3.1 Efficiency

An algorithm is called "efficient" if it runs in polynomial time or faster. What does this mean? Let us examine the task of finding the factors of a number. Consider the following problem:

$$?\times? = 29083$$

Using paper and pencil this problem will take approximately one hour to solve. However, to solve the reverse problem:

$$127 \times 229 = ?$$

Takes less than a minute. This is because an efficient algorithm for multiplication is known, but there is no such algorithm for factoring. In order to classify problems by efficiency, they can be analyzed by the way the time to perform increases with the size of the input. For example, adding another digit to the factoring problem will increase the work to several hours, while another digit added to each of the factors in the multiplication problem will only increase the work by less than a minute. Multiplication is a polynomial-time algorithm; factorization runs in exponential time (Shor, 1996).

2.3.2 Shor's and Grover's Algorithms

Shor's algorithm, published in 1994, solves the problem of factorization by using a method which runs in polynomial time. There is one catch, however: this polynomial speedup can only be achieved on a quantum computer. Shor reduces the problem of finding the factors of a number to finding the period of a certain function. This is an "indirect" approach which measures a property of a function

in order to solve another problem. The mathematical details of this algorithm are beyond the scope of this paper, but in brief Shor uses the exponential parallelism of quantum systems to compute the period of a certain function. Classically, this period computation would take an exponential number of steps by itself, and thus the algorithm would run in exponential time. A quantum computer allows for this computation to take place in polynomial time. This period is then obtained with fairly high probability (if it is not, the algorithm is simply repeated). This period can then be used to factor the number at hand. Thus, Shor's algorithm is exponentially faster than any known factoring algorithm for classical computers (Shor, 1996).

Grover's algorithm, presented in 1996, applies to searching an unsorted database. It provides only a polynomial speedup, but this speedup is very important nonetheless. Grover sets up a superposition of all of the entries in the database and then makes several rotations and special operations so that the output is the item that is being looked for with a probability of at least 0.5 (Steane, 1997).

3 Quantum Computer Simulation

Although quantum computers, at this point in time, are not technologically feasible, this minor setback does not prevent the development of quantum algorithms, i.e. programs that will run on a quantum computer once it is built. In order to develop such algorithms, a quantum computer simulator[5] is necessary.

The OpenQubit core development team, consisting of the author and several colleagues around the world has developed such a simulator. It is currently in the stages of its infancy, but there is a working prototype of Shor's algorithm, and very recently proposals for the implementation of Grover's database search algorithms have been submitted. At this time, the stable version of OpenQubit is 0.2.0 and this is the version that was used in the efficiency tests. There is also a test version in development (0.3.x, a.k.a. NewSpin) which has a better model, and so this will be the version that is discussed.

3.1 OpenQubit Model Overview

OpenQubit uses an object-oriented model[6] to describe the workings of the quantum computer. The main class in the QState class which describes the quantum state of the machine. For an n qubit machine, it stores 2^n amplitudes as complex numbers in order to describe all the possible outcomes of the state. This class provides memory management facilities for the class QRegister, which is a substate, addressing several or all the qubits in the QState. The basic set of operators (R_y, R_z, Ph, CNot) is provided through a set of classes. Because the act of applying an operator is the same for any gate class[7], this application process has been abstracted away into a separate class, and all the gates *inherit*[8] from this class. A detailed description of the software follows. It consists of documentation generated from source code and a diagram representing the class structure.

[5] A simulator or emulator is a program which runs on top of classical hardware and provides a working environment like that of a quantum computer. Thus, the user may then develop a program as if the computer he was using was of a quantum nature.

[6] Briefly, object oriented programing (OOP) centers heavily on the modeling of physical entities. Traditional programming methods concentrate on algorithms and procedures, but OOP concentrates on describing objects and their interactions. Each object is described by a set of properties and a set of methods (functions that it can perform). The basic unit of object oriented programming is the *class*. For example, a person might be modelled by a class containing properties to describe the person's hair color, etc, and methods such as walk, talk, and eat.

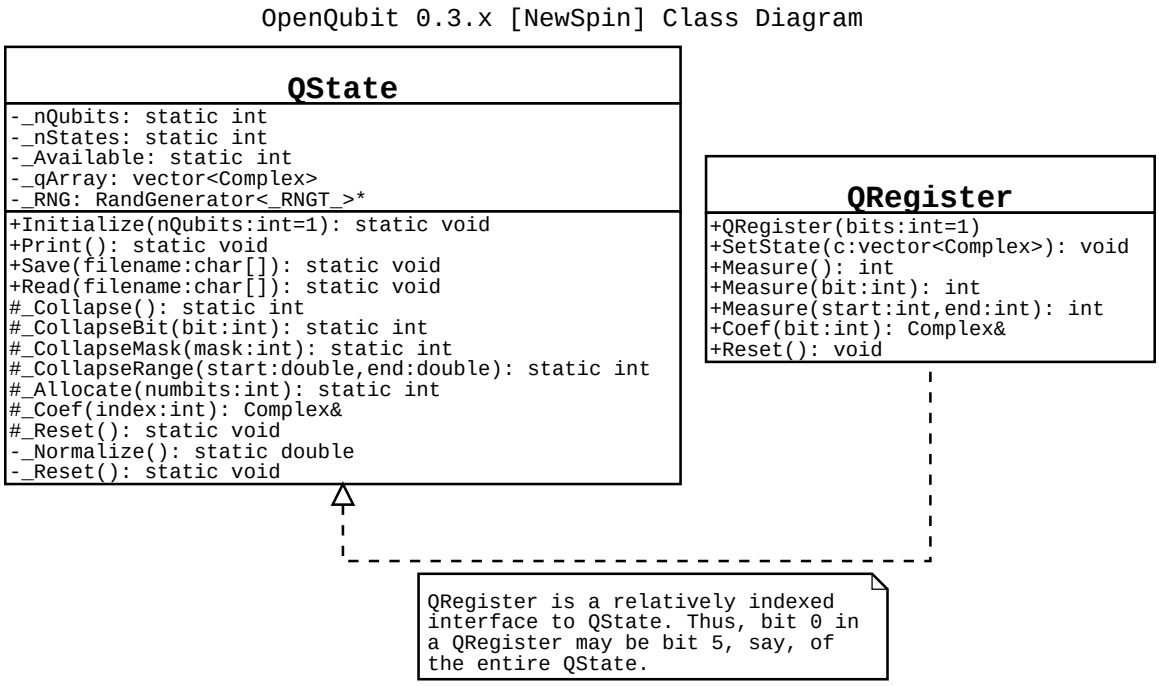
[7] In order to apply the gate, just multiply the quantum state by the matrix which represents the gate.

[8] An OOP term. If a class inherits from another class, then it will gain all the properties and methods of that class as its own, and more can be added as seen fit by the designer.

The OpenQubit software was developed by the OpenQubit core development team consisting of Yan Pritzker, Ralf Podeszwa, Peter Belkner, Chris Dawson, Igor Kofman, Jonathan Blow, and Joe Nelson. It was developed for the Linux operating system. OpenQubit is an organization which I founded on December 9, 1998 as an attempt to bring together physicists, computer scientists, and laymen together in order to create a quantum simulation API (Application Programmer Interface). At the time, I had little experience with quantum physics, and approached the matter from largely a computer science standpoint.

The OpenQubit software library is released under the GPL2 (GNU Public License Version 2) which, in brief, requires the software to always include source code and to always be distributed free of charge. A copy of this license can be obtained at *http://www.gnu.org/copyleft/gpl.html*. OpenQubit is a work in progress, so certain parts of documentation or diagram may be inaccurate by the time this paper is read.

3.1.1 OpenQubit Main Class Diagram



3.1.2 Sample Output

Provided here is the output from a sample run of Shor's factoring algorithm using OpenQubit.

```
OpenQubit version 0.2.0, Copyright (C) 1999 OpenQubit.org
Shor's algorithm for factoring numbers
Enter number to factorize: 15
Enter a number from 1..14: 4
Preparing equal superposition in the first register
Modular exponentiation
Fourier transformation of the first register
Measured state is:
1.000000 |000100000001>
The result is 128
```

```
Fourier domain is 256
Extracting the period using continued fraction expansion...
Period guess is: 2
Period guess is probably correct
Factors found! 15 = 5 * 3
```

4 OpenQubit Documentation

The documen+tation following this paper was generated using the PERCEPS documentation generator from OpenQubit source code. The full source code to OpenQubit is available at *http://www.openqubit.org.*

References

[1] Barenco, Adriano et. al. (1995, December 18). *Elementary gates for quantum computation.* xxx.lanl.gov e-Print Archive.

[2] Feynman, R., Leighton, R. B., Sands, M. (1965). *The Feynman lectures on physics.* London: Addison-Wesley.

[3] Gribbin, John (1984). *In search of Schroedinger's cat.* New York: Bantam Books.

[4] Guillemin, Victor (1968). *The story of quantum mechanics.* New York: Charles Scribner's Sons.

[5] Preskill, John (1996, December 17). *Quantum computing: pro and con.* xxx.lanl.gov e-Print Archive.

[6] Steane, Andrew (1997, September 24). *Quantum computing.* xxx.lanl.gov e-Print Archive.