Querying Qubits Creates Quantum Computers

Karl Smith
Physics Department, Wooster
(Dated: May 10, 2012)

Quantum computing is an emerging field in quantum physics where a computer is built to utilize bizarre properties of quantum mechanics so as to perform algorithms in a way fundamentally superior to classical computers. The quantum computer is conceived around the idea of the 'qubit', a quantum state that collapses into one of only two possible states when measured, corresponding to the classical term 'bit', which can exist in only two states. This paper describes two aspects of quantum computing that set it apart from classical computing: quantum parallelism, which utilizes superposition to test for global properties of functions in a way much faster than classical computers, and superdense coding, where one is able to send two bits of information by transmitting a single qubit.

PACS numbers: 03.67.Lx,03.65.Aa,03.65.-w,03.67.Ac,03.67.-a,03.65.Ud,42.50.Lc,42.50.-p

QUANTUM BITS: 'QUBITS'

Quantum computing utilizes quantum states and their properties and interactions in order to compute in a way fundamentally different from classical computing. However, quantum computing is only interested in a specific type of state: those that, when measured, are found to be in one of two possible states. That is, the quantum states that it uses are a superposition between two possible states which collapse into one or the other state. This two state model corresponds to the two state nature of classical bits.

Although it is possible and advantageous in some ways to create a quantum computer based on a quantum state of three possible states (a 'quatrit') or more, it poses no significant theoretical challenges in addition to those modeled on two-state systems [1].

It is relatively straightforward to generally define the qubit. It is a superposition of two quantum states, which will be called $|0\rangle$ and $|1\rangle$ (corresponding to classical zeros and ones). This means that any quantum qubit is of the form

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

where α and β are complex coefficients that define the superposition of the state. This can be represented as the vector

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{2}$$

If the state is normalized, we find that

$$|\alpha|^2 + |\beta|^2 = 1. \tag{3}$$

The probability that one will find that the system is in state $|0\rangle$ is $|\alpha|^2$, and the probability that it will be in state $|1\rangle$ is $|\beta|^2$ [1].

Bloch Sphere

A popular way to illustrate a qubit is with a Bloch Sphere, which is defined in spherical coordinates. The definition of the qubit in terms of α and β is four-dimensional (a real value for each coefficient and a complex value for each coefficient), so it is necessary to combine the imaginary values of the two coefficients; this is possible by factoring out "global phase", which is unnecessary.

In order to do that, we first need to separate out the real and complex values of α and β. Every complex number can be written as $C = re^{i\phi}$. So Eq. 1 becomes

$$|\psi\rangle = r_0 \mathrm{e}^{i\phi_0}|0\rangle + r_1 \mathrm{e}^{i\phi_1}|1\rangle. \tag{4}$$

We can then factor out the first imaginary term, which results in

$$|\psi\rangle = \mathrm{e}^{i\phi_0}\left(r_0|0\rangle + r_1 \mathrm{e}^{i(\phi_1-\phi_0)}|1\rangle\right). \tag{5}$$

It is now possible to eliminate this imaginary term since it does not change the probability when the system is measured. Measuring the system with some arbitrary measurement operator M_m, it is the case that $\langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\mathrm{e}^{-i\phi}M_m^\dagger M_m \mathrm{e}^{i\phi}|\psi\rangle$ [1]. This gives us

$$|\psi\rangle = r_0|0\rangle + r_1 \mathrm{e}^{i(\phi_1-\phi_0)}|1\rangle. \tag{6}$$

In order to get spherical coordinates from this, it is necessary to define r_0 and r_1 with an angle. It is possible to do this through the normalization constraint. We know from Eq. 3 that $|r_0|^2 + |r_1|^2 = 1$. If we compare this to the relationship $\cos x^2 + \sin x^2 = 1$, we can choose

$$r_0 = \cos\frac{\theta}{2} \tag{7}$$

and

$$r_1 = \sin\frac{\theta}{2}. \tag{8}$$

The choice to make the argument $\theta/2$ instead of simply θ was so that it runs from 0 to π instead of 0 to $\pi/2$ [2]. Defining it in this way makes the variables the same as they are standardly defined in spherical coordinates.

Our final result for the spherical definition of a qubit is

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{9}$$

Multiple Qubit Systems

The above formalism needs an expansion to be able to accommodate systems with more than one qubit and multiple-qubit gates. Describing a state of two qubits is represented as $|a\rangle|b\rangle = |ab\rangle$. In order to create the vector representing the state of this system, one needs to apply the "tensor product" of the two vectors. This means

$$|a\rangle \otimes |b\rangle = |ab\rangle = \begin{pmatrix} \alpha_a \\ \beta_a \end{pmatrix} \otimes \begin{pmatrix} \alpha_b \\ \beta_b \end{pmatrix} = \begin{pmatrix} \alpha_a\alpha_b \\ \alpha_a\beta_b \\ \beta_a\alpha_b \\ \beta_a\beta_b \end{pmatrix}. \tag{10}$$

Quantum Gates

Quantum gates can be represented with matrices. Quantum gates operating on qubits can be represented by writing the qubit in a state vector that is then multiplied by the quantum gate vector. There are single qubit gates that are 2×2 matrices which operate on only one qubit at a time. There are two-qubit gates that are 4×4 matrices which operate on two-qubit systems (represented by a tensor product of the two vectors representing the qubits, order of operation matters). There are gates that operate on more qubits than one or two, and these scale in a predictable manner. The basic quantum gates are shown in Table. I.

For example, if one were to apply an X (quantum 'NOT') gate, to some arbitrary state vector, the amplitude of the two states would be flipped. In this case

$$X\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}. \tag{11}$$

Here the X gate exchanges the probability amplitudes of the qubit's state, however other gates will change the qubit in more complicated ways.

TABLE I: Quantum Gates

Name	Matrix
Hadamard	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli-X (NOT)	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-iY	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
controlled-NOT	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

PHYSICAL QUANTUM COMPUTERS

Building physical quantum computers comprises a significant undertaking. A complete quantum computer requires a significant number of quantum systems that can be used to create enough quantum qubits. There must be a way of keeping the systems from decohering, or losing their quantum state due to uncontrolled measurement collapse. A classical computer must be used to control the quantum systems. Classical computers are also used to manage the quantum error correction programs (which are necessary since a small amount of decoherence is always expected). There also must be sufficient ways to interact the quantum qubits with 'gates'. Finally, it must be possible to measure the qubits in their correct basis.

It has been proven that any theoretical arrangement of one and two qubit quantum gates can be effectively created using only single qubit gates and the two-qubit gate "cnot" (albeit, sometimes this is extremely inefficient). This is similar to the classical "NAND" gate, with which any classical circuit can be created. This means that if it can be demonstrated that a physical system can reasonably manifest single qubit gates as well the cnot gate, then it is possible for a quantum computer to be built in using that physical system [1].

While it is possible to construct a physical quantum computer using such systems as a standard simple harmonic oscillator, it is extremely impractical since no more than one unitary transform may be applied to the system and certain types of algorithms would be unable to be run on it. Let us look at a few different type of physical quantum computers that are theoretically feasible.

Optical Quantum Computers

It is possible to create a superposition of a photon in an optical cavity. In this way, one can superpose a photon into two optical cavities and use these to transmit the qubit. This is called the 'dual-rail' representation. One can produce single photons by using an attenuated laser. Although it is near impossible to produce two photons simultaneously for the purposes of interacting with each other, it is possible to delay one of the photons until two are aligned. Photons evolves in time with the Hamiltonian $H = \hbar\omega a^\dagger a$. Applying this to a two-state quantum system (qubit) makes the system evolve from $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ to $|\psi(t)\rangle = c_0|0\rangle + c_1 e^{-iwt}|1\rangle$. This means that the 'dual-rail' quantum system $|\psi\rangle = a|01\rangle + b|10\rangle$ evolves only by a global phase factor e^{-iwt}, which is undetectable.

It is possible to perform any arbitrary single qubit gate using a combination of z-axis and y-axis rotations. Phase shifters can be used to perform arbitrary z-axis rotations and beamsplitters perform y-axis rotations, therefore it is possible to perform any arbitrary single qubit gate on an optical qubit. The cnot gate can be created from beamsplitters and Kerr media, a medium that has 'cross phase modulation'.

In this way, it is proven possible to construct a quantum computer using optical components: any arbitrary single qubit gate can be created and it is possible to create the cnot gate. This setup is very convenient and feasible for creating single photon qubits and performing single qubit gates. However, it is very difficult to create two qubit gates since the Kerr media is highly inefficient and scatters photons at a high rate. For this reason optical quantum computers have been generally considered unlikely candidates for physical quantum computers [1].

Optical Cavity Quantum Electrodynamics (QED)

Another method for creating a quantum computer involves trapping one atom in an optical trap with a high charge and only one or two optical modes. Firing photons into this trap will cause the photons and atom to interact reliably. Building a quantum computer using these can be accomplished in several ways. One is to use photons as the quantum bits and they interact with cavities to perform nonlinear interactions (quantum gates); the other is to use the cavities as the quantum bits and the photons serve to perform nonlinear interactions (quantum gates).

The Fabry-Perot cavity is a useful and frequently used type of optical trap cavity. This creates a large electric field in a narrow band of frequencies in the cavity, which is what allows the atom to exist in one of two modes. The atom's state is complicated, though a binary model suffices. The field evolves with the Hamiltonian $H = \hbar\omega a^\dagger a$.

The QED method is more promising than the optical method, since QED is able to create multi-qubit gates without the unreliable Kerr medium. Instead, QED can simulate the nonlinear interaction that the Kerr media would provide. This makes it a stronger candidate for being put to use in the future [1].

Ion Traps

Yet another method for creating a physical quantum computer involves using electron and nuclear spins as quantum bits. In order to use them, the atom is trapped in electromagnetic fields and cooled down so that the atom's kinetic energy does not interfere with the spin states.

Single-qubit gates are created by applying a magnetic field to the atom changes the Hamiltonian of the system and can be used to create rotation operations. A controlled-NOT gate is created using the Hadamard gate and interactions with phonons [1].

QUANTUM PARALLELISM

One of the clear advantages that quantum computing holds in contrast to its rival is that qubits can be in a superposition, whereas classical bits cannot. This has several advantages, among them quantum parallelism, which is the capability to evaluate the entire domain of a function in a single step, instead of one at a time. Since qubits collapse when they are measured, and so only yield one bit of information, one cannot have the computer output multiple evaluations of a function without evaluating extra qubits. However, one can determine some binary global property of the function (or alternatively, one can determine a global property or properties using binary queries).

Deutsch's Algorithm

Deutsch's algorithm is a novel example of quantum parallelism. It's goal is to determine whether or not a boolean function is *balanced* or *constant*. If a function is constant, then every input into the function results in an output of 1. If it is balanced, then the function will return 0 for half of its inputs and 1 for the other half (assuming some finite number of possible inputs). With a classical algorithm it is random how many times the function must be called before it can be classified as either of the two types; at most it will take $2N - 1$ tries where N is the number of possible inputs. However, Deutsch's algorithm can make this distinction by evaluating the function only once.

Begin with $|0\rangle$, apply a Hadamard gate to it, and one will get

$$H|0\rangle = |\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]. \tag{12}$$

If one then applies the unknown function to this state, the result will be

$$|\psi_2\rangle = f|\psi_1\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right] & \text{if} f(0) = f(1) \\ \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if} f(0) \neq f(1). \end{cases} \tag{13}$$

Apply another Hadamard gate to this first qubit to get

$$|\psi_3\rangle = H|\psi_2\rangle = \begin{cases} \pm|0\rangle & \text{if} f(0) = f(1) \\ \\ \pm|1\rangle & \text{if} f(0) \neq f(1). \end{cases} \tag{14}$$

As you can see, measurement of the qubit will reveal whether or not $f(0) = f(1)$. This is clearly a feature of the function that would typically require one to query the function twice, once to find $f(0)$, and another time to find $f(1)$. This quantum algorithm evaluates this with one query [1].

SUPERDENSE CODING

Superdense coding is the method by which one is able to transmit a greater amount of information using qubits compared with an equal number of bits. This is accomplished by entangling two or more qubits, which split between Bob and Alice (this entanglement could be done either by Bob or by a third party; Alice need not be involved). Alice then modifies her qubit(s) and sends them to Bob. By measuring the qubits, Bob is then able to tell how Alice modified her qubit(s).

Untangling Entaglement

A system of one qubit can have two possible states after measurement: $|0\rangle$ and $|1\rangle$. A system of two qubits then has four possible states: $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, where these correspond to the four different combinations of qubit possible states after measurement. A two-qubit system can be said to be in one of these four states. Entanglement may link the possible states for the two qubits. For example, if the state of the system is

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{15}$$

then measuring one qubit gives us the state of the other qubit.

In particular, Eq. 15 means that there is a fifty-fifty chance that both qubits will be found to be in their $|0\rangle$ or their $|1\rangle$ state; that is, if we were to measure one qubit, we now know what the state of the other one is. Eq. 15 is one of a series of states called 'Bell State'.

TABLE II: Two bits transmitted with one qubit.

Bits	Modification	Result
00	unmodified	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
01	$\left(\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}\right) Z =$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
10	$\left(\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}\right) X =$	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$
11	$\left(\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}\right) iY =$	$\frac{\|10\rangle-\|01\rangle}{\sqrt{2}}$

An Example: Sending Two Bits with One Qubit

Let us walk through an example where Alice sends Bob two bits of information sending only one qubit.

In advance, Alice and Bob agree to begin with the same state, as shown in Eq. 15. Alice can either send this qubit unmodified to Bob or she could pass it through one of three quantum gates, the X, iY, or Z gates [1]. The four possible quantum states are displayed in Table II.

These four end states are all called 'Bell States', and Bob can easily discover what Alice did to her qubit by passing the first qubit through a Hadamard gate and then measuring it.

The reason that this is possible is that these four states are orthonormal to each other. This means that four possible states (two bits) is the maximum amount of information one can communicate by sending only one qubit.

[1] Michael A. Nielsen & Isaac L. Chuang, *Quantum Computation and Quantum Information*, (2000).
[2] C. Leary, private communication (2012).
[3] Robert Raussendorf & Hans J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2000)
[4] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, (1987)