CSE 599d - Quantum Computing
One Qubit, Two Qubit

Dave Bacon
Department of Computer Science & Engineering, University of Washington

Now that we've gone through the requisite review of linear algebra and Dirac notation, we can begin to consider how quantum mechanics allows us to build computing devices. In this lecture we will discuss a single qubit, then two qubits, and then a single qubit quantum algorithm, known as Deutsch's algorithm.

I. ONE QUBIT

Suppose that we are dealing with a quantum machine with simply two configurations for each cell. Such a setup is called a qubit. The word "qubit" was first used in the scientific literature by Ben Schumacher. In fact the word was suggested, in jest, in a conversation between Ben Schumacher and William Wootters. The jest, I believe, was that qubit would be pronounced just like "cubit," which is an ancient length about equal to the length of a forearm, something like 18-22 inches (The Roman cubit was 17.4 inches; the Egyptian 20.64 inches.) Most people, I think, associate cubits with the Bible and if you ever get a chance to listen to Bill Cosby's comedy routine about Noah's ark, the word will hold a special place in your heart. I once missed a big opportunity when Ben Schumacher was visiting the Santa Fe Institute (SFI) in New Mexico where I was a postdoc. You see at SFI there was another fellow who had also invented a work that began with the letter "q" and was in the dictionary: Murray Gell-Mann who invented the word "quark." What opportunity did I miss? Well at the time my license plate read QUBITS and Murray's read QUARKS. So think about it, I had the opportunity to get a picture taken of two people who invented two "q"-words in the dictionary standing beside two cars with license plates both showing those words. I will never forgive myself for missing this opportunity.

Okay, back to the issue at hand. A qubit, like we said, is a two configuration system. Physicists like to call this a two-level system (TLS.) The quantum state of a two level system is given by

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

where $\alpha, \beta \in \mathbb{C}$ and since we require this to be a normalized state, we require that $|\alpha|^2 + |\beta|^2 = 1$. One thing which I haven't yet discussed is that for quantum states, a global phase for the state never has any observable consequences (and hence is irrelevant.) Thus the state $|\psi\rangle$ and $e^{i\gamma}|\psi\rangle$ will, no matter what happens later, both produce the same observable consequences (to see this note that the phase does not effect measurement properties and that a phase commutes with any unitary operator.) Thus it is useful to factor out this global phase. In particular it is useful to always choose the global phase such that the coefficient of the $|0\rangle$ ket is real an non-negative. Using this and the normalization constraint, it is useful to not use α and β, but instead to use $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$ where $0 \leq \theta \leq \pi$ and $0 \leq \phi < 2\pi$. When we do this, we see that we can map all of the single qubit states onto the surface of a sphere, i.e. we can interpret ϕ as the azimuthal angle and θ as the zenth angle in spherical polar coordinates. This sphere is called the Bloch sphere, and because we are physicists, even when we are talking about the surface of this sphere, which is really a ball, we still call this surface a sphere.

Now one thing that often confuses people when they first encounter the Bloch sphere is that single qubit states which are orthogonal are not orthogonal vectors on the Bloch sphere. Thus for instance, $|0\rangle$ and $|1\rangle$ are orthogonal, but are represented on the Bloch sphere as $\theta = 0$ and $\theta = \pi$, i.e. as points along the positive $\hat{z}$ axis and the negative $\hat{z}$ axis. Another point which often confuses people is that at the abstract level of qubits, the directions on the Bloch sphere have no "physical" meaning. This is because a qubit is any two level system, i.e. it could be the hyperfine levels of an ion. This, however, is not always true. Sometimes, the qubit we are talking about is actually what physicists call a spinor. In this case, the direction on the Bloch sphere do have something to do with directions in space. We'll have more to say about this in a bit.

Having defined a qubit, it is now useful to begin to discuss possible evolutions of this qubit. To discuss this, we need to introduce very quantum physicists favorite transforms, the Pauli operators. The Pauli operators are the four operators

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2}$$

where we have written out the three notations used most commonly for these operators (the identity operator has only two standard notations.) The Pauli operators are all hermitian, $\sigma_i^\dagger = \sigma_i$ and all square to identity $\sigma_i^2 = I$. From this first fact we know that the eigenvalues of these matrices are real and from the second fact we know that these eigenvalues must be either $+1$ or -1. In fact for all Pauli matrices the two eigenvalues for these matrices are $+1$ and -1. It is useful to know what these eigenvectors are for each of these matrices, so we list them below with a fairly standard notation:

Pauli operator	eigenvalue	eigenvector
$\sigma_x = X$	$+1$	$\|+\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
$\sigma_x = X$	-1	$\|-\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
$\sigma_y = Y$	$+1$	$\|+i\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$
$\sigma_y = Y$	-1	$\|-i\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$
$\sigma_z = Z$	$+1$	$\|0\rangle$
$\sigma_z = Z$	-1	$\|1\rangle$

It is nice to identify where these are on the Bloch sphere. Indeed we see that the ± 1 eigenvalue of the pauli matrix σ_α points along the $\pm\alpha$ axis. The Pauli operators satisfy the following commutation relations

$$[X, Y] = iZ,\ [Y, Z] = iX,\ \text{and}\ [Z, X] = iY \tag{3}$$

and the following anticommutation relations

$$\{X, Y\} = \{Y, Z\} = \{Z, X\} = 0. \tag{4}$$

Or in more sophisticated notation, $[\sigma_\alpha, \sigma_\beta] = \epsilon_{\alpha\beta\gamma}\sigma_\gamma$ (where $\alpha \in \{1, 2, 3\}$, ϵ is the Levi-Civita symbol, and there is an implicit sum over γ (Einstein's convention.) Similarly we could express the anticommutation as $\{\sigma_\alpha, \sigma_\beta\} = 2\delta_{i,j}$.

Having defined our good friends the Pauli operators, we can now discuss single qubit unitaries. To do this, we fist introduce the notation $\vec{n} \cdot \vec{\sigma} = n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3$, $n_i \in \mathbb{R}$, and note that $\vec{n} \cdot \vec{\sigma}$ is hermitian. Then we can consider the unitary operations defined by

$$U(\vec{n}) = \exp(i\vec{n} \cdot \vec{\sigma}) \tag{5}$$

Wait a second, what are we doing here, we are taking the exponential of a matrix (i.e. e^M.) What is this? Well we can just define it by its power series

$$\exp(M) = \sum_{k=0}^{\infty} \frac{M^k}{k!} \tag{6}$$

Using this definition, we can show that $\exp(iH)$ is unitary if H is hermitian. To see this, note that

$$\exp(iH)\exp(iH)^\dagger = \sum_{k=0}^{\infty} \frac{(iH)^k}{k!} \sum_{l=0}^{\infty} \frac{(iH)^l}{l!}^\dagger = \sum_{k,l=0}^{\infty} \frac{(iH)^k(-iH)^l}{k!l!} = \sum_{k=0}^{\infty}\sum_{l=0}^{k} \frac{(-1)^l(iH)^k}{(k-l)!l!} = \sum_{k=0}^{\infty}\sum_{l=0}^{k} (-1)^l \binom{k}{l} \frac{(iH)^k}{k!} = I \tag{7}$$

where in the second to last step we have used the fact that $\sum_{l=0}^{\infty}(-1)^l\binom{k}{l} = 0$ unless $k = 0$. Using this fact, since $\vec{n} \cdot \vec{\sigma}$ is hermitian, $U(\vec{n})$ is unitary. In fact, every single qubit unitary that has determinant 1 can be expressed in the form $U(\vec{n})$. This set of operators form a group which is called $SU(2)$ where the S stands for special and means that the determinant of the unitary is 1 and U stands for unitary, (meaning, of course, unitary!), and the two means two dimensional, as in these are two dimensional matrices. Actually if we want to be correct about things we usually say that the $\exp(\vec{n} \cdot \sigma n)$ is the "defining" representation of the group $SU(2)$. But we won't need to get into too much group theory right now, so we'll often use rather sloppy language here. Why do we restrict ourselves to the unit determinate unitaries? Since a global phase on a qubit doesn't matter and the determinant of a unitary matrix is just a phase $e^{i\alpha}$, this restriction does not lose us any generality.

OK, now there is a very nice expression for $U(\vec{n})$ which uses the fact that

$$(\vec{n} \cdot \vec{\sigma})^2 = (|\vec{n}|\hat{n} \cdot \vec{\sigma})^2 = |\vec{n}|^2(\hat{n} \cdot \vec{\sigma})^2 = |\vec{n}|^2 I \tag{8}$$

Using this expression and the power series for exp we can then show that

$$U(\vec{n}) = \cos(|\vec{n}|)I + i\sin(|\vec{n}|)\hat{n} \cdot \vec{\sigma} \tag{9}$$

Usually we use the notation $\frac{\theta}{2} = |\vec{n}|$, so we see that an element of $SU(2)$ can be parameterized by a unit vector $\hat{n}$ along with an angle $0 \leq \theta < 4\pi$, which we denote $U(\theta, \hat{n})$

Now you may immediately be suspicious about my choice of $\frac{\theta}{2} = |\vec{n}|$. Why this factor of 2 in the angle? Well first of all we can ask what $U(\theta, \hat{n})$ does to single qubit states on the Bloch sphere. For example, what happens to states when $\hat{n} = \hat{z}$? Then

$$U(\theta, \hat{z}) = \cos\left(\frac{\theta}{2}\right) I + i \sin\left(\frac{\theta}{2}\right) Z = \begin{bmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{bmatrix} \tag{10}$$

and

$$U(\theta, \hat{z}) \left(\cos\left(\frac{\theta'}{2}\right)|0\rangle + \sin\left(\frac{\theta'}{2}\right) e^{i\phi'}|1\rangle\right) = e^{\frac{i\theta}{2}} \left(\cos\left(\frac{\theta'+}{2}\right)|0\rangle + \sin\left(\frac{\theta'}{2}\right) e^{i(\phi'+\theta)}|1\rangle\right) \tag{11}$$

where we have explicitly factored out a global phase so that you can see that the terms inside of the equation has a real non-negative coefficient in front of the $|0\rangle$ ket. From the above expression one can see that the effect of $U(\theta, \hat{z})$ is to rotate elements of the Bloch sphere by angle θ about the $\hat{z}$ axis.

Now if one works through the full messy transformation of how $U(\theta, \hat{n})$ acts on the Bloch sphere, as you might guess from the example we just worked out, the effect of this transformation is to rotate the states on the Bloch sphere by an angle θ about the direction $\hat{n}$. Given this you may now even be more puzzled than before about why I let θ go from 0 to 4π. Well we've been talking about $U(\theta, \hat{n})$ as a rotation, but a rotation in the Bloch sphere space. Now since $U(\theta, \hat{n})$ is just a rotation of the Bloch sphere by angle θ about the $\hat{n}$ direction, it is natural to want to identify this with an actual physical rotation by angle θ about the $\hat{n}$ axis. But when we do this, something funny happens when you do this. Notice that when $\theta = 2\pi$, $U(2\pi, \hat{n}) = -I$. If we want to make this correspondence work, then we see that the rotation corresponding to a rotation by 2π will correspond to multiplication by a global phase of -1. So if we have a physical object where rotation in three dimensional space corresponds to our rotation of the Bloch sphere, we find that when we rotate the object by 2π, then the qubit acquires a global phase of -1. Now it might have been that nature wouldn't provide two level quantum systems where this correspondence works, but it appears that nature does. This object we call a spinor.

Now you might worry that, because a qubit is defined only up to a global phase (technically we should deal with rays in a Hilbert space, not the vectors) this global phase doesn't matter. But suppose you have the following situation. Take your spinor. Design a machine which rotates the spinor by 2π if the machine's memory cell is in one configuration, $|a\rangle$ and does nothing to the spinor if the machine's memory cell is in a different configuration,$|b\rangle$. Then if the machine's memory cell is in a superposition of the $|a\rangle$ and $|b\rangle$, then this superposition will acquire a phase of -1 between these two states. And relative phases between two states *are* observable! Thus you can design experiments where the fact that rotating a spinor by 2π does not return the qubit to its original state

One thing which is interesting to think about is whether we should be surprised by the fact that rotating a spinor by 2π does not return the objects quantum state to the same state. Well in one sense, we should be shocked by this, but in another sense we shouldn't be too surprised. There are two very cool tricks which demonstrate why we shouldn't be too surprised. The first is the Dirac belt trick. We can use a belt to represent a series of rotations in three dimensional space. That is we can think about one end of the belt as our original object and then the other end of the belt as the end result of the rotation. Since the belt is a continuous object it also represents all possible rotations between these two rotations. Now if you take a belt which is flat (representing a series of "no rotations") and give one end of it a twist by 2π the belt with have a twist in it that you can't get rid of by keeping the ends of the belt fixed and moving around the rest of the belt (representing the rotations between 0 and 2π.) But if you take a belt which is flat and rotate one end by 4π, then it *is* possible to keep the ends fixed in orientation and *to get rid of the two twists!* Now this is really cool! And it sort of demonstrates why we shouldn't be too surprised that rotating something by 2π does not return it to it's original state. Of course, we don't think spinors are actually "belts," so we haven't removed all the mystery: we've just made it a little more understandable.

The second trick which helps us understand the spinor is less known than the Dirac belt trick but is, I think, much more interesting. Suppose you have a sphere which you put in a box. Then attach strings from the surface of this sphere to the edges of the box in such a way that these strings aren't tangled (i.e. attach a point on a sphere to where the box intersects the ray from the origin on the sphere to the point on the sphere.) Now if you take this sphere and rotate it by 2π about some axis, then the strings will become all tangled. By moving the sphere up and down, back and forth, to and froe, but not rotating it, it is impossible to untangle the sphere. Now rotate the sphere by another 2π about the same axis for a total rotation by 4π. Now, *amazingly*, it is possible by simply moving the sphere around, and not rotating it, to completely untangle the strings. This again is a reason why we shouldn't be surprised by objects like spinors. Of course we don't think a spinor is just such an object as this box and sphere, but this does show us that if we define an object by its relationship to the external world, like our strings are doing, then the spinor is not so strange after all.

For those of you with a bit of knowledge of group theory, what is occurring here is that $SO(3)$, the group of special orthogonal transformations is double covered by $SU(2)$. What we are doing is we are using a representation of $SO(3)$ which is a representation "up to phase": $U(R_1)U(R_2) = e^{i\phi(R_1,R_2)}U(R_1 \circ R_2)$. You might recall that $SO(3)$ is not simply connected, that is if you think about the space of rotations, there are loops in this space which you cannot shrink to a point. To see this think about the space of rotations as a sphere of radius π: a rotation about an angle θ about a direction $\hat{n}$ is represented by a point at distance θ along direction $\hat{n}$. Then antipodal points on this sphere are the same rotation. However, if you draw a line from between these antipodal points, through the origin (remember this line represents a whole series of rotations), then you can see that it is impossible to contract this line to a point. Two paths are called homotopic if we can deform one to another. In $SO(3)$ we see that for every rotation there are two different classes of paths beginning at the origin and ending at a particular rotation. One can turn the set of all rotations along with their homotopy classes (those two different manners to construct the rotation) into a group. In our case when we do this the group we obtain is $SU(2)$. This method of taking a homotopy class and the transforms and constructing a larger group yields what is called the universal covering group. Thus what we have for spinors is effectively that $SU(2)$ is the double cover of $SO(3)$.

A. Quantum Wires, Circuit Elements, and Interference

At this point it is useful to begin to introduce the quantum circuit notation. The quantum circuit notation is a useful way to denote a set of actions that we apply to our quantum system. Here we'll just talk about one qubit, but in the next section we'll begin to denote more than one qubit. In the quantum circuit diagrams, time runs from left to right (unlike in physics where we often like to make time run from top to bottom). We denote a qubit by a single line, which is often called a quantum wire. A quantum wire really just represents a qubit which is not evolving, i.e. which is acted upon by I. If we initialize our qubit into a particular quantum state, then we usually write the appropriate ket on the left hand side of the appropriate quantum wire:

$$\alpha|0\rangle + \beta|1\rangle \ \text{———} \tag{12}$$

Now if we want to signify that a particular unitary evolution is to be enacted on our qubit, then we put a box with a symbol describing this unitary transform along the quantum wire. Thus for example the prescription, start in the state $|0\rangle$ and apply the transform $H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$ is denoted by

$$|0\rangle \ \text{—}\boxed{H}\text{—} \tag{13}$$

By the way, this operation, H, is called the Hadamard operation, and will be a good friend of ours for the next many lectures. Oftentimes, we will also denote the output of a quantum circuit as well. For example, the result of the above circuit is denoted by

$$|0\rangle \ \text{—}\boxed{H}\text{—} \ \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{14}$$

Finally we may want to denote a measurement in the computational basis on our qubit. This is denoted by a meter (or sometimes by an eyeball.) Thus, for instance we might have the circuit

$$|0\rangle \ \text{—}\boxed{H}\text{—}\boxed{\ } \tag{15}$$

At this point, one can already introduce some neat little circuits which are very strange from a classical perspective. First consider the following circuit

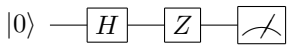
$$|0\rangle \ \text{—}\boxed{H}\text{—}\boxed{\ } \tag{16}$$

This circuit takes a system in a fixed configuration, $|0\rangle$, and the measurement after applying H, is 50% $|0\rangle$ and 50% $|1\rangle$. OK, this is not so strange: we've just produced a random bit. Certainly a classical machine can do this. Now consider applying the H twice:

$$|0\rangle \ \text{—}\boxed{H}\text{—}\boxed{H}\text{—}\boxed{\ } \tag{17}$$

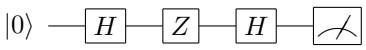
It is easy to check that $H^2 = I$, so that the state before the measurement meter is just $|0\rangle$. Thus applying H twice yields the configuration $|0\rangle$ with one hundred percent probability. Now this is a bit peculiar: applying the

same physical process to our qubit once randomized it, but applying it a second time turned it back into a totally determined configuration. A bit weird. But things get a little stranger. Now suppose that after applying H you apply the Pauli Z operator (remember the Pauli's are unitary):



(18)

Now the state right before the measurement meter is $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. So measuring the system results again in 50% $|0\rangle$ and 50% $|1\rangle$. But now apply a Hadamard before performing a measurement, i.e. the following circuit:



(19)

If you work through the math on this (and you should if you aren't already familiar with quantum circuits) then you will see that right before the meter the system has a description of $|1\rangle$ and so a measurement yields $|1\rangle$ with 100% probability. Now this is kind of peculiar: applying an operation which *didn't* have an observable consequence after applying the Hadamard, after applying a second Hadamard resulted in a totally different configuration. This demonstrates to use that it is just not the magnitude of the amplitudes in a quantum state that matter (i.e. if the qubit is $\alpha|0\rangle + \beta|1\rangle$, then it is not just $|\alpha|$ and $|\beta|$ which matter.) What we say is that the phases of the different configurations matter. And this is what is cool about quantum systems: because this phase, we see that the amplitudes can add in interesting ways that probabilities can't. In this particular example, we see that when we feed $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ into the Hadamard, the amplitudes to go to the $|0\rangle$ configuration constructively add up but the amplitudes to go to the $|1\rangle$ configuration destructively subtract and become zero. By changing the phase of the input to the Hadamard to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ we can reverse the pathways which are constructive and destructively adding up. This effect, where the amplitude can add in constructive or destructive manners is called interference. It is an expression, in general of the "wave nature" of quantum theory, i.e. just like waves on a pond when they cross each other can add or substract to each other the amplitudes in quantum theory can do a similar thing.

Now this last point brings us to an important and interesting question. If it is only interference which is going to make a quantum computer special then we might be in trouble. Why? Because we can imagine building a machine which uses classical waves, i.e. like the waves on a pond, to construct a computer. Why isn't a classical wave machine just like a quantum wave machine. This is a fun and interesting question that we will eventually go a long ways toward understanding in this course. Suffice it to say that you will find out that classical wave machines do not appear to be as powerful as quantum computers. But its a good question and we should keep it in the back of our minds as we continue on in this course.

II. TWO QUBITS

Having now introduced single qubits, we can start plugging onward and move up to a system with two two configuration systems, i.e. two qubits. The configurations of a two qubit system are the four configurations $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, and $|1\rangle \otimes |1\rangle$. Now it gets really tiresome writing these tensor products, so we often drop the $\otimes$, and express these in the slightly more compact notation $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, and $|1\rangle|1\rangle$. This can be confusing because the tensor product is implicit. Most often we drop the tensor product and combine the configurations together, and write $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. The general state of a two qubit system is given by the quantum state

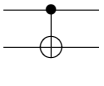
$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{20}$$

where $\alpha_{ij} \in \mathbb{C}$ and $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

What sort of operations can we perform on two qubits? Well any 4 dimensional unitary transform. It is important, however, at this point to begin to understand the issue of locality for our quantum system. In particular, when we have two qubits, we should think that we have two separate physical systems, each with a two level system. If we perform a unitary evolution (by turning on our lasers or such) on only one of these physical sysystems, then the unitary we are implementing is of the form $U \otimes I$, where U is a two dimensional unitary matrix and I is the two dimensional identity matrix representing that we have done *nothing* to the second physical system. Similarly if we act only on the second system, then the unitary we will enact is of the form $I \otimes U$. Finally, we can act with unitaries on both qubits at the same same but with a process that does not couple to two qubits and our unitaries will be of the form $U \otimes V$. It is only when we bring the two qubits together and allow them to interact quantum mechanically that we are able to enact unitaries which cannot be expressed in the form $U \otimes V$. An example of such a unitary, and

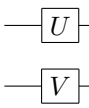
one which will be of some significance for us is the controlled-NOT operation,

$$C_X = \quad = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{21}$$



Here notice we've also begun to introduce the quantum circuit notation for two qubits. These two qubits are denoted by the two quantum wires. Since the controlled-NOT cannot be written as an action on either of these qubits along, we write it as a two qubit gate: a gate with two quantum wires input and two quantum wires output. This should be contrasted with an evolution like $U \otimes V$, which we denote in quantum circuit notation by

$$U \otimes V = \quad = \begin{bmatrix} U_{00}V_{00} & U_{00}V_{01} & U_{01}V_{00} & U_{01}V_{01} \\ U_{00}V_{10} & U_{00}V_{11} & U_{01}V_{10} & U_{01}V_{11} \\ U_{10}V_{00} & U_{10}V_{01} & U_{11}V_{00} & U_{11}V_{01} \\ U_{10}V_{10} & U_{10}V_{11} & U_{11}V_{10} & U_{11}V_{11} \end{bmatrix} \tag{22}$$



Within the class of two qubit states, an important distinction to make is between states that can be expressed as separate single qubit wave functions $|v\rangle \otimes |w\rangle$, where $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|w\rangle = \delta|0\rangle + \gamma|1\rangle$ and those that cannot be expressed like this. The first of these are called separable states and the latter are called entangled states. An example of an entangle state of two qubits is the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

How do we tell if a two qubit state is entangled? Well one way to do this is to just use the four equations that come from

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\delta|0\rangle + \gamma|1\rangle) = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{23}$$

and see whether these expressions have a solution (notice that because we can always multiply α and β by a factor and γ and δ by the one over this factor, there will always be multiple solutions, when they exist.) Another way which is nicer is to use the Schmidt decomposition. What is the Schmidt decomposition?

Well we begin by noting that whether or not a qubit is separable or not is not a function of the single qubit basis being used to describe each individual qubit. Thus it is natural to attempt to *mod out* local single qubit unitaries. In other words, we can ask what are the parameters of a two qubit state which are independent of the local single qubit basis. To address this consider the action of $U \otimes V$ on a two qubit state,

$$U \otimes V \sum_{i,j=0}^{1} \alpha_{i,j}|i\rangle \otimes |j\rangle \tag{24}$$

where we have been explicit in the tensor product here while in the future we will probably drop it. Write $U = \sum_{k,l=0}^{1} U_{k,l}|k\rangle\langle l|$ and $V = \sum_{k,l=0}^{1} V_{k,l}|k\rangle\langle l|$. Then

$$\begin{aligned} U \otimes V \sum_{i,j=0}^{1} \alpha_{i,j}|i\rangle \otimes |j\rangle &= \left(\sum_{k,l=0}^{1} U_{k,l}|k\rangle\langle l| \otimes \sum_{m,n=0}^{1} V_{m,n}|m\rangle\langle n| \right) \sum_{i,j=0}^{1} \alpha_{i,j}|i\rangle \otimes |j\rangle \\ &= \sum_{k,m=0}^{1} U_{k,l}\alpha_{k,m}V_{n,m}|k\rangle \otimes |m\rangle \end{aligned} \tag{25}$$

If we reexpress this as $\sum_{k,m=0}^{1} \alpha'_{k,m}|k\rangle \otimes |m\rangle$, then the new amplitudes in terms of the old, pre-$U \otimes V$ amplitudes are given by

$$\alpha'_{k,m} = \sum_{k,m=0}^{1} U_{k,l}\alpha_{k,m}V_{n,m} \tag{26}$$

Now the cool trick. If we think about $\alpha_{k,m}$ as a 2 by 2 matrix, then this expression is just

$$\alpha' = U\alpha V^T \tag{27}$$

where U and V^T are both unitary. Using the singular valued decomposition, it is thus possible to pick U and V^T such that α' is diagonal (and with positive entries.) Thus we have shown that it is always possible to pick a basis for each qubit, let's call then both $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$, such that our two qubit state can be expressed as

$$\sqrt{\lambda_0}|\tilde{0}\rangle \otimes |\tilde{0}\rangle + \sqrt{\lambda_1}|\tilde{1}\rangle \otimes |\tilde{1}\rangle \tag{28}$$

where λ_0 and λ_1 are positive numbers which sum to 1. Thus we see that there is one real number left over when we mod out the local single qubit unitaries. Further note that if $\lambda_0 = 1$, then this state is separable. Indeed it is easy to see that (except for the equivalent case of $\lambda_1 = 1$) this is the only case where we have a separable state. Thus one way to determine whether a state is entangled or not is to take the coefficients $\alpha_{i,j}$, treat them as a matrix and then perform a singular value decomposition on this matrix. If there is only one non-vanishing entry, then the state is separable. Otherwise it is entangled.

In a larger sense, however, performing the Schmidt decomposition is a nice way to put bipartite (two system) states in a form which is canonical up to the local unitary action $U \otimes V$. We've done it for two qubits, but one can also perform the Schmidt decomposition for larger bipartite systems. Indeed when we study entanglement we will find that the Schmidt coefficients (the λ_i) are extremely important to developing the theory of bipartite entangled systems. Another important remark to make here is that there is not generalization of the Schmidt decomposition to tri-partite or greater numbers of systems in general that has all of the properties that the Schmidt decomposition has. Its fun to think about why this is true, but it is also one of the frustrating reasons that the theory of multipartite entangled quantum systems is much less developed that that for bipartite entangled quantum systems.

A. Deutsch's Algorithm

Having introduced two qubits we can now examine the simplest example of a quantum algorithm. This is Deutsch's algorithm. Deutsch came up with this algorithm (or rather a slightly modified version of this algorithm) in 1985. Actually it might not be proper to call this an algorithm, as it only works on two qubits (it's generalization to more qubits is known as the Deutsch-Jozsa algortihm), but we will abuse language (because we can) and call it an algorithm.

Let's setup Deutsch's algorithm. In Deutsch's problem we are given a black box which computes a simple function. Let's just make this machine a classical machine right now. Now we will describe the black box. The black box takes as input two bits and produces as output two bits. So for example, we might feed in 00 and the black box may output 01. Each time we do this, we say that we are querying the black box. The goal now is to learn something about the possible function being computed by the black box by querying the box as few times as possible. In Deutsch's problem, the black box implements one of the four following functions

$$\begin{aligned} f_1(x,y) &= (x,y) \\ f_2(x,y) &= (x,\bar{y}) \\ f_3(x,y) &= (x, x \oplus y) \\ f_4(x,y) &= (x, x \oplus \bar{y}) \end{aligned} \tag{29}$$

Here x and y are bits, $\bar{y}$ denotes the negation of y, and $\oplus$ is the exclusive or operation (addition modulo 2: $0 \oplus 0 = 1 \oplus 1 = 0$ and $0 \oplus 1 = 1 \oplus 0 = 1$.) We denote the output of the black box by the two bits $(\cdot, \cdot)$. Now the goal of Deutsch's problem is to distinguish the first of these functions from the second of these two functions. In other words I give you a black box which implements one and only one of these functions and you want to determine whether the function implemented by the black box is in the set $S_1 = \{f_1, f_2\}$ or the set $S_2 = \{f_3, f_4\}$.

How many times do we need to query the black box (classically) to solve this problem? Well lets just try a possible query. Suppose we query the function with input $(0,0)$. Then the outputs we get are

$$\begin{aligned} f_1(0,0) &= (0,0) \\ f_2(0,0) &= (0,1) \\ f_3(0,0) &= (0,0) \\ f_4(0,0) &= (0,1) \end{aligned} \tag{30}$$

Thus we see that it is impossible to distinguish whether the black box is implementing a function from S_1 or S_2 by this single query. One can similarly go through the other three possible query inputs are see that no matter what we query, there is no way to use a single query to distinguish between whether we were given a function from S_1 or one from S_2. You can also quickly convince yourself that if you do two queries of the black box, then you can distinguish between S_1 and S_2

Now what we've just observed is that to solve Deutsch's problem, we needed to query the classical black box two times. The question Deutsch asked was what happens when you make this machine quantum and allow it to operate in a quantum mode. So the first thing we need to understand is how we make the black box quantum. First take a look at, say $f_2(x, y)$. This function sends (x, y) to $(x, \bar{y})$. We thus implement it by a two qubit unitary gate such that for the computational basis this is exactly the function computed. In other words we implement it as

$$U_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{31}$$

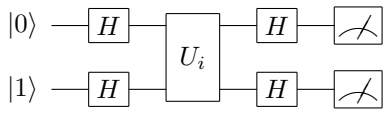
which you might recognize as $I \otimes X$. This matrix is unitary (it is a permutation matrix: a matrix where every row and every column is all zeros except a single entry with the value one. Permutation matrices are always unitary.) And we see that we can use it in a totally classical fashion to compute f_2: $U_2|x, y\rangle = |x, \bar{y}\rangle$. One can similarly define unitary matrices for each of the four functions in Deutsch's problem. To be specific, these unitary matrices are

$$U_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; U_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \; U_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \; U_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{32}$$

Now suppose that we are only allowed to input classical computational basis elements into the machines which compute these unitaries. Then by our above argument we will have to use the unitary twice (query it twice) in order to distinguish whether we were given a unitary from the set $\{U_1, U_2\}$ or from the set $\{U_3, U_4\}$.

But our machines are quantum, so our argument doesn't necessarily hold if use the more general properties of quantum theory. In particular, we can ask whether instead of querying using the computational basis states, using a general superposition and manipulation of the two qubits output from this device will allow us to solve Deutsch's problem with a single query? The answer, surprisingly is yes!

To see how this works, consider the following quantum circuit:



(33)

This circuit represents the following. We start in the quantum state $|0\rangle \otimes |1\rangle$. We then apply Hadamard operations to each qubit. Then we use the black box to implement the two qubit unitary U_i. Finally we again apply the Hadamard operations to each qubit and then we measure each qubit in the computational basis. Recall that the Hadamard matrix is

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \tag{34}$$

Thus the quantum state after the first Hadamards is given by

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \tag{35}$$

What happens next is a function of which unitary U_i is. In particular we find by explicit calculation that

$$\begin{aligned} |\psi_1\rangle = U_1|\phi\rangle &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \\ |\psi_2\rangle = U_2|\phi\rangle &= \frac{1}{2}(-|00\rangle + |01\rangle - |10\rangle + |11\rangle) \\ |\psi_3\rangle = U_3|\phi\rangle &= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \\ |\psi_4\rangle = U_4|\phi\rangle &= \frac{1}{2}(-|00\rangle + |01\rangle + |10\rangle - |11\rangle) \end{aligned} \tag{36}$$

Now we can act with $H \otimes H$ on these four states and see what happens. To be explicit note that

$$H \otimes H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{37}$$

Using this one can calculate that

$$\begin{aligned} |\chi_1\rangle &= (H \otimes H)U_1|\phi\rangle = |01\rangle \\ |\chi_2\rangle &= (H \otimes H)U_2|\phi\rangle = -|01\rangle \\ |\chi_3\rangle &= (H \otimes H)U_3|\phi\rangle = |11\rangle \\ |\chi_4\rangle &= (H \otimes H)U_4|\phi\rangle = -|11\rangle \end{aligned} \tag{38}$$

Thus when we perform the ultimate measurement in the case that the unitary was U_1 or U_2 we will observe configuration $|01\rangle$ with certainty and if the unitary was U_3 or U_4 we will observe the configuration $|11\rangle$ with certainty. Thus by looking at the first qubit we are able to solve Deutsch's problem: we can distinguish between the function being computed by the unitary being in the set S_1 verus the set S_2 by using the black box unitary only a single time!

So at this point you should begin to see some of the motivation to study machines which operate according to quantum theory. By using a machine which classically we need two queries to "learn" in a quantum manner, we can "learn" the function in only a single query! OK, so this is only a factor of two speedup, but it at least hints that something very strange is going on here.

In 1985 when Deutsch discovered this algorithm (actually he had a slightly modified version, but we will bend history), he wrote at the end of the paper describing the algorithm, the following prophetic sentence:

> *"Complexity theory has been mainly concerned with constraints upon the computation of functions: which functions can be computed, how fast, and with use of how much memory. With quantum computers, as with classical stochastic computers, one must also ask and with what probability? We have seen that the minimum computation time for certain tasks can be lower for Q than for T . Complexity theory for Q deserves further investigation."* –David Deutsch, (here Q=quantum computers, T=classical computers)

Something strange is going on here, and Deutsch sensed this. It would take another few years before this blossomed into a truly revolutionary result, but this humble little result is the beginning, and even today, when I look back at it, I get very excited and motivated to understand how quantum laws change the rules of computational complexity.

Acknowledgments

The diagrams in these notes were typeset using Q-circuit a latex utility written by graduate student extraordinaires Steve Flammia and Bryan Eastin.