1 Introduction to Quantum Computing

Classical computers, i.e. the computers that we all know and love, run on *bits* or 1's and 0's. This is the fundamental unit of information in classical computers. In quantum computers, information is built upon an analagous concept, the *quantum bit* or *qubit*. We will discuss the defining properties of qubits, some of which may seem very different from those of bits.

1.1 Information Storage

In classical computing, each bit can be in one of two states–1 or 0. We denote *quantum states* by $|0\rangle$ and $|1\rangle$, pronounced "*ket zero*" and "*ket one*," respectively. This follows traditional *Dirac notation*[1]. Unlike classical bits, qubits can be in a *superposition* between these two states. We describe a quantum state as follows: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. This describes a probability distribution over the quantum states $|0\rangle$ and $|1\rangle$ with *amplitudes* α and β. We can also think of $|\psi\rangle$ as a vector in a two-dimensional complex vector space. The states $|0\rangle$ and $|1\rangle$ form an orthonomal basis in this complex vector space and are called the *computational basis states*.

So how can we know which state a bit or qubit is in? In classical computing, we can simply read the bit to determine whether it's a 0 or a 1. Qubits are a little trickier. We cannot read $|\psi\rangle$ to determine its exact state, that is α and β. As soon as we measure $|\psi\rangle$, the superposition will collapse to either $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. In other words, $|\psi\rangle$ is like a weighted coin that we can flip once to get either heads or tails, but we have no way to directly measure the bias in the coin. Unlike a coin, as soon as $|\psi\rangle$ has been measured to reveal some quantum state, $|\psi\rangle$ will permanently collapse to that state, i.e. $|\psi\rangle = 1|0\rangle + 0|1\rangle$ or $|\psi\rangle = 0|0\rangle + 1|1\rangle$. Every time we measure it thereafter, we will observe the same state that we measured the first time. In the coin analogy, it's like we have a weighted coin that we can flip once to reveal heads or tails, and every subsequent flip always yields the initial state that we flipped to.

You may be wondering why this is useful. It seems impossible that our fundamental unit of information in this model of computation is unknowable, immeasurable. The beauty of quantum computation lies in the *manipulation* of these immeasurable qubits such that by the time we measure them at the end, the result will inform us of the state they started in. More on that later.

[1] See reference on notation

1.2 Special States $|+\rangle$ and $|-\rangle$

As we already glossed over, $|0\rangle = 1|0\rangle + 0|1\rangle$ and $|1\rangle = 0|0\rangle + 1|1\rangle$. We sometimes represent these states as column vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Thus, we can represent a transformation on qubits by a 2-by-2 matrix where the first column is the image of $|0\rangle$ and the second column is the image of $|1\rangle$ under the transformation. For example, the quantum NOT gate can be realized as a matrix:

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

This takes a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and transforms it into $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$. Alternatively, by matrix multiplication we see that

$$X|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

So, any transformation on a single qubit can be represented by a 2-by-2 matrix. What about the transformation that, when given $|0\rangle$ or $|1\rangle$, outputs an *equal superposition* of $|0\rangle$ and $|1\rangle$? We might represent that as follows:

$$\widehat{H} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

There are a few problems with this transformation. First, applying this transformation $\widehat{H}|0\rangle = 1|0\rangle + 1|1\rangle$, which means that $|\alpha|^2 + |\beta|^2 = 1^2 + 1^2 \neq 1$. So, we must *normalize* the matrix, to get

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

Now, applying the transformation to our basis vectors, we get $\widehat{H}|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $\widehat{H}|1\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. There is still a problem with this transformation. All quantum transformations must be *reversible*, but we have mapped the two basis vectors to the same state, so the transformation is not reversible. To fix this, we will simply negate one of the ones:

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

This is called the *Hadamard transform* or *Hadamard gate*. It acts on the basis vectors as follows: $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Both of these states are in an equal superposition between $|0\rangle$ and $|1\rangle$. These states come up rather often, so they have been given the special shorthand notations $|+\rangle$ and $|-\rangle$, respectively.

The requirements that quantum transformations be reversible and normalized are encapsulated by the property that the matrix representation for any transformation be *unitary*. That is, $U^\dagger U = I$ where $U^\dagger$ is the transpose of the complex conjugate of U and I is the 2-by-2 identity matrix. Within those requirements, we can construct any transformation we like. What about transforming multiple qubits?

1.3 Multiple Qubits

To represent multiple qubits, we expand our two quantum states to many using tensor products [2]. For example, in a two qubit system, we have the following basis states:

$$|0\rangle \otimes |0\rangle,\ |0\rangle \otimes |1\rangle,\ |1\rangle \otimes |0\rangle,\ \text{and}\ |1\rangle \otimes |1\rangle.$$

These four states can equivalently be written as:

$$|00\rangle,\ |01\rangle,\ |10\rangle,\ \text{and}\ |11\rangle.$$

Thus, any two-qubit state can be represented as a linear combination of these basis states, namely $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. In general, an n-qubit state can be represented as

$$|\psi\rangle = \sum_{i \in \mathbb{Z}_2^n} \alpha_i |i\rangle,$$

where i is the binary representation of the numbers $0, \ldots, n-1$. The probability of observing a state $|i\rangle$ upon measuring $|\psi\rangle$ is $|\alpha_i|^2$.

We may measure qubits individually as well. For example, measuring just the first qubit gives us 0 with probability

$$\sum_{i \in \mathbb{Z}_2^{n-1}} |\alpha_{0i}|^2,$$

leaving the post-measurement state

$$|\psi'\rangle = \frac{\sum_{i \in \mathbb{Z}_2^{n-1}} \alpha_{0i}|\alpha_{0i}\rangle}{\sqrt{\sum_{i \in \mathbb{Z}_2^{n-1}} |\alpha_{0i}|^2}}.$$

[2] See appendix on tensor products

Something that follows from the above equation but which is not self-evident is the concept of *entangled states*. Consider the following state:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Suppose we measured the first qubit. We will observe $|0\rangle$ with probability $1/2$, and the resulting post-measurement state is: $|\beta'_{00}\rangle = |00\rangle$ (by the equation above). How can this be? We only measured the first qubit, and yet, we now have information about both qubits. This is precisely because the state is entangled. Another example of an entangled state is:

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

These two states, $|\beta_{00}\rangle$ and $|\beta_{01}\rangle$, are the first two *Bell states* or *EPR pairs*. Quantum entanglement is a powerful computational tool and will be used in many quantum algorithms in the rest of the text.

Now that we have the means to represent an n-qubit state, the state transformations can be represented by 2^n-by-2^n matrices. In particular, the n-qubit Hadamard transform is $H^{\otimes n} = H \otimes H \otimes \ldots \otimes H$, i.e. n tensor products.

1.4 Summary

In summary, below are the main constraints that our quantum computations must abide by:

- After measuring a state, it collapses irreversibly to one of the basis states.
- Aside from measuring, all transformations on the qubits must be reversible and normalized, i.e. the matrix representation must be unitary.