A Brief Introduction to Quantum Circuits

Rio Weil, Student # 47189394

This document was typeset on February 16, 2021

Contents

1 Introduction

This document is meant to serve as a bare-bones introduction to the math of gate-model quantum computing. This is no means a comprehensive review on the topic, but is meant to provide some background information that might be useful for understanding the project. This set of notes assumes some prior knowledge of linear algebra as well as some basic knowledge of complex variables. This set of notes is based off of information from a TRIUMF Lecture series about introductory quantum computing given by Dr. Olivia Di Matteo[1] as well a information from sections 1.1-2.2 of the Qiskit Quantum computing textbook[2]. For further (more comprehensive) reading on Quantum Computation, both the Qiskit textbook, as well as *Quantum Computation and Quantum Information* by Nielsen and Chuang are good sources.

2 What is a Qubit, anyway?

2.1 Motivation

Shor's factoring algorithm for prime factorization and possibilities for other faster-than-classical quantum algorithms have lead to a recent surge in quantum computing research and development, both in academia

[1] `https://github.com/glassnotes/Intro-QC-TRIUMF`

[2] `https://qiskit.org/textbook/ch-states/introduction.html`

and within industry. As quantum computing at its core involves linear algebra, there is no reason why such systems cannot be simulated on classical computers[3]. Though much more complete and powerful software (such as the qiskit library for Python) exist for this purpose, it was a fun task to try to implement rudimentary one/two qubit systems in Java as part of the CPSC 210 project. For this purpose, let's start by discussing how a qubit differs from the familiar classical bit and how we can think about it mathematically.

2.2 From a Classical Bit to a Qubit

One may be already familiar with the classical bit, where the state is represented by a single binary value; 0 or 1. Physically, this corresponds to voltage above some threshold in computer hardware. A quantum bit, or qubit, is represented differently, requiring two *complex* numbers to describe a single qubit state. The reader may already be familiar with the pop-sci description that "A qubit can be both a 0 and a 1 at the same time!". This description is actually fairly close to the truth. If we let $|0\rangle, |1\rangle$ represent the pure 0 and 1 states of the qubit (alternatively, we can call these *eigenstates*), then the general state $|\psi\rangle$ of a qubit can be written as:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

Where $\alpha, \beta \in \mathbb{C}$. In other words, a qubit in general is a linear superposition of the pure 0/1 states. We can also rewrite this in a more familiar vector form, by thinking of qubit states as vectors over $\mathbb{C}^2$. If we identify:

$$|0\rangle \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Then we can identify the qubit state $|\psi\rangle$ as:

$$|\psi\rangle \mapsto \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

However, there is one slight oversimplifcation that we have yet to address; α, β in general cannot be arbitrary complex scalars, for reasons that tie very closely to quantum measurement, as we will see in a moment.

2.3 Quantum Measurement and Probabilities

One way that the quantum world differs significantly from the classical world is in the nature of measurement. Unlike a classical measurement, where measurement leaves the state of the object unchanged (e.g. if we were to measure the position of a soccer ball, we don't change the position of the baseball in the process, unless we mistakenly kick it in the process), quantum measurement is a dynamical process. Measurement in a certain basis will cause the quantum state to collapse to a pure state/eigenstate of the basis, irreversably changing the quantum state. To make this more concrete, let's return to our example of the single qubit. A measurement of the general qubit in state $|\psi\rangle$ ($\binom{\alpha}{\beta}$) in the 0/1 basis (which will be the only basis discussed in this document, as well as the only measurement basis included in the project) will collapse the state of the qubit into one of the pure states $|0\rangle$ ($\binom{1}{0}$) and $|1\rangle$ ($\binom{0}{1}$). A natural question then becomes; how do we know which state we will measure the qubit to be in? The answer is that we can't; we can only predict the **probabilities** of measurement. Measurement is inherently a probabilistic process. How do we get these probabilities? If we recall how we expressed our general quantum state:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

We can see that α quantifies how much of $|0\rangle$ goes into $|\psi\rangle$, and β quantifies how much of $|1\rangle$ goes into $|\psi\rangle$. To get the probabilities of measurement, we can take the modulus squared of these amplitudes; i.e. $|\alpha|^2$

[3] A question may arise for why we want to build quantum computers at all if this is the case; as we wei will see later, the issue is that an n quantum bit is represented by a 2^n length column vector and acted on by $2^n \times 2^n$ matrices, which quickly becomes unfeasible to compute.

gives the probability of measuring the qubit to be in state $|0\rangle$, and $|\beta|^2$ gives the probabilities of measuring the qubit to be in state $|1\rangle$. As a brief review, the modulus of a complex number $z = a + ib$ is given by $|z| = \sqrt{a^2 + b^2}$. It is important to define the probabilities with these modulus as probabilities are real numbers (not complex!). Because the probability of measuring either $|0\rangle$ or $|1\rangle$ has to add up to one, a restriction that we place on α, β is therefore:

$$|\alpha|^2 + |\beta|^2 = 1$$

We note that if $\alpha = 1$ and $\beta = 0$, we have that $|\psi\rangle = |0\rangle$, and that the probability of measuring the state to be in $|0\rangle$ is 100%, and the probability of measuring the state to be in $|1\rangle$ is 0%; this is a good consistency check that our definition makes sense! With these basics established, we can move onto one-qubit quantum circuits and how we can manipulate qubits using gates. We might predict that since we can identify qubits with vectors, we can identify operations on qubits as matrices; and this prediction will turn out to be correct!

3 One Qubit Quantum Circuits

3.1 The Bloch Sphere

Before we get into a discussion of how we operate on gates, it may be helpful to introduce a visualization for what these gates are doing; for this purpose, we introduce an object called the Bloch sphere[4], which is a unit sphere in complex space. We can regard all single-qubit states as vectors that lie on the Bloch sphere. We can picture it as follows[5]:

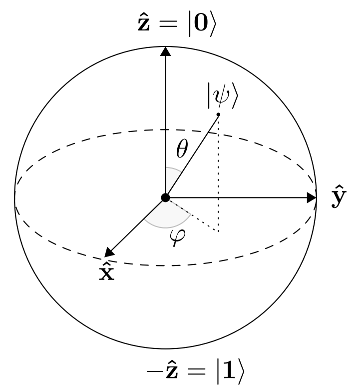

Figure 1: Visualization of a single qubit using the Bloch sphere. Qubit states correspond to vectors that lie on the sphere.

The north/south poles of the sphere correspond to the pure $|0\rangle$ and $|1\rangle$ states of the qubit. The $\pm\hat{\mathbf{x}}$ axes correspond to $|0\rangle \pm |1\rangle$ states, and the $\pm\hat{\mathbf{y}}$ axis correspond to $|0\rangle \pm i\,|1\rangle$ and $|0\rangle - i\,|1\rangle$ states. This visualization will come in useful very shortly when we begin to talk about gates; we will find that many of these gates just correspond to rotations of the qubit state vector around different axes of this sphere!

3.2 The Identity "Gate"

In an analog to classical gates which act on classical bits (e.g. a NOT gate that turns a 0 bit into 1, and a 1 bit into a 0), we can think of operations on qubits in a similar way. Now, since we have vectors for our qubits instead of the single numbers that were the classical bits, we will see that our gates will be represented by matrices instead of classical gates that just take in boolean values. We might as well start with the simplest

[4]Readers familiar with complex analysis may recognize this as the Riemannian sphere
[5]Figure taken from `https://tex.stackexchange.com/questions/345420/how-to-draw-a-bloch-sphere`

possible operation of all, namely that of doing nothing. This would of course correspond to the 2x2 identity matrix:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

This isn't a particularly interesting example, but we will see it has some uses when we discuss 2 qubit systems a little while later.

3.3 The Pauli (XYZ) Gates

Three gates (that actually do things) that are good to start out with are the Pauli-X, Pauli-Y, and Pauli-Z gates[6]. In matrix form, these are given as follows:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The Pauli-X gate is known as the bit flip operation. So see why it gets this name, lets see what it does to the pure states $|0\rangle$ and $|1\rangle$:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

We can see that it indeed "bit flips" the $|0\rangle$ to the $|1\rangle$ state and vise versa. This is the quantum analog of the classical NOT gate. The Z gate is often called the phase flip operation. Let's see what it does to our pure states:

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

We can see that it leaves the $|0\rangle$ state unchanged, and flips the phase of the $|1\rangle$ state. Finally, for the Y gate we have:

$$Y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i|1\rangle$$

$$Y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i|0\rangle$$

In the Bloch sphere picture, the Pauli-X gate corresponds to a rotation of π radians of $|\psi\rangle$ around the x axis of the Bloch sphere, the Pauli-Y gate to a rotation about the y axis, and the Pauli-Z gate to a rotation about the z axis. We mentioned before that $\pm\hat{\mathbf{z}}$ on the Bloch sphere corresponds to $|0\rangle$ and $|1\rangle$, that $\pm\hat{\mathbf{x}}$ corresponds to $|0\rangle \pm |1\rangle$, and that $\pm\hat{\mathbf{y}}$ corresponds to $|0\rangle \pm i|1\rangle$. This lines up with the eigenvectors of the Pauli X, Y and Z matrices, as we might have expected!

3.4 Products of Gates

To apply more than one gate to a single qubit, we can just apply multiple matrices to our vector. For example, applying X and then Z to $|0\rangle$ we have:

$$ZX|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

[6] Readers familiar with quantum mechanics will represent these as the Pauli spin matrices

3.5 The Phase (ST) Gates

Two more important single qubit gates are known as the S and T gates:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \end{pmatrix}$$

These gates change the relative phase between $|0\rangle$ and $|1\rangle$. Though they do not affect the amplitudes of the state, they can affect the measurement outcomes. We note that S is often called $\sqrt{Z}$ as $S^2 = Z$. Additionally, T is often called $\sqrt{S}$ as $T^2 = S$:

$$S^2 = SS = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

$$T^2 = TT = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = S$$

In the Bloch sphere picture, S corresponds to a rotation of $\frac{\pi}{2}$ radians around the z axis, and T corresponds to a rotation of $\frac{\pi}{4}$ around the z axis. A brif note; though it is not implemented in this project, we do note that it is possible to generalize these Pauli/phase gates to arbitrary rotations around the Bloch sphere. However, the ones discussed in this document are the standard examples, and hence were the only ones that were used in the implementation of the project. We also note that a generalization is not required in order for universal quantum computation (this is discussed later on in this document, towards the end).

3.6 The Hadamard Gate

We end the discussion on one qubit quantum circuits with a very important gate known as the Hadamard gate (in fact, this might possibly be the most important single qubit gate of all!). In matrix form, it is given as:

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

The Hadamard gate has the property that it will take a pure state and put it into a superposition of pure states:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$$

We note that if we were to measure either $|+\rangle$ or $|-\rangle$, there would be a 50/50 chance of measuring $|0\rangle$ or $|1\rangle$. We now move onto a discussion of multi-qubit systems (specifically, two).

4 Two Qubit Quantum Circuits

4.1 The Tensor Product - Qubits

Since we had a 2-element column vector to represent our single qubit, readers may anticipate (correctly) that 2 qubits would be represented by a 4-element column vector. Since Hilbert Space (A vector space where quantum states live in) compose under an algebraic operation known as a tensor product, qubit states and quantum gates compose in the same way. Let's quickly just see how a tensor product works algebraically. Given two matrices:

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \quad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

Their tensor product is given by:

$$A \otimes B = \begin{pmatrix} a_1 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & a_2 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \\ a_3 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & a_4 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1b_1 & a_1b_2 & a_2b_1 & a_2b_2 \\ a_1b_3 & a_1b_4 & a_2b_3 & a_2b_4 \\ a_3b_1 & a_3b_2 & a_4b_1 & a_4b_2 \\ a_3b_3 & a_3b_4 & a_4b_3 & a_4b_4 \end{pmatrix}$$

Now, let's apply this two qubits. For a system of two qubits, we now have a total of 4 pure states/eigenstates; A state where the first qubit is 0 and the second is 0, a state where the first qubit is 0 and the second is 1, a state where the first qubit is 1 and the second is 0, and finally a state where both qubits are 1. We can see how each of these states can be obtained through composition under the tensor product:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Hence, the general state of a two qubit system can be represented by:

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$

Where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, and the modulus squared of the coefficient gives the probability of measuring that state. For normalization of probabilities, we again require that:

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

4.2 The Tensor Product - Gates

For a two qubit system, we can use a lot of the machinery that we established for the one qubit case. We can simply take the gate that we want to apply to the first qubit and compose it with the tensor product to the gate we want to apply to the second qubit. For example, say we had an initial state $|00\rangle$ (that is, both of the qubits are in a pure zero state), and we want to apply the Hadamard gate to the first qubit and do nothing to the second qubit. Mathematically, this operation would involve the matrix:

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \\ \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & -\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}}\end{pmatrix}$$

Applying this to our state we would have:

$$H \otimes I = \begin{pmatrix}\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = |+\rangle \otimes |0\rangle$$

Where the result is (as we would expect) the tensor product of the + state with the pure zero state. We can do this process for any of the 7 gates as discussed in the above section!

4.3 Entanglement and CNOT Gates

In addition to the single qubit gates as discussed above, there is one final gate to discuss; this gate, known as the CNOT gate, is a gate that acts on two qubits:

$$C = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

This might not look like a particularly special gate, but it is **extremely** important gate for multi-qubit quantum computation. In particular, it is responsible for entangling two qubits. Quantum entanglement refers to a scenario where a system is stronger-than-classically correlated. To make this notion more concrete, Let's apply the CNOT gate to the $|+\rangle \otimes |0\rangle$ state that we obtained above. To start, clearly both the first qubit and the second qubit are in a sense indepedent, and they both have their own state (as we can write is as a tensor product of the first qubit with the second). However, let us now apply the CNOT gate:

$$C\left(|+\rangle \otimes |0\rangle\right) = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Something quite cool has happened here; by applying the CNOT Gate, we can no longer write our system in the form $|\psi_1\rangle \otimes |\psi_2\rangle$; that is to say, the individual qubits no longer have their own state. *We cannot describe the qubits individually, and can only describe the combined state.* We can also see that the measurement outcomes are perfectly correlated between the two qubits. If I were to measure 0 for one of the qubits, I would have to measure 0 for the other as well! In principle, we could entangle as many qubits as we would like (if we had an arbitrary n-qubit system) but the two qubit system is sufficient to convey the idea.

4.4 Universality - What gates do you need?

To finish off the discussion, it might be worthwhile to consider "what set of gates is actually necessary to do quantum computation?" For a classical system of any number of bits, we only need two gates (e.g. AND and NOT) to carry out any arbitrary operation. One might expect that quantum bits being more complex[7] that

[7] unintentional pun

we would require a large number of gates; perhaps all of the ones discussed in this document, or even more. It turns out that this is not the case. For a 1 qubit system, we can carry out any operation to arbitrary precision through only using the two gates of T (phase) gate and the H (Hadamard) gate. For a multi-qubit system, we can carry out any operation to arbitrary percision through only using the T, H, and CNOT gates (as well as the identity "gate", but this just corresponds to doing nothing so it doesn't really count). Although the scope of this project is small (you really can't do much with two qubits), it does contain all of the necessary machinery to fully control the system!

5 Conclusion

I hope that this short set of notes helps to provide some of the mathematical background for understanding the code behind the project (at its core, it really is just implementing everything described in these notes to Java). Although a more detailed discussion about quantum algorithms and computation is beyond the scope of this document, I hope that this may have piqued enough interest to inspire further pursuit into the topic. Thank you so much for reading!