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 and within industry. As quantum computing at its core involves linear algebra, there is no reason why such

[1] `https://github.com/glassnotes/Intro-QC-TRIUMF`
[2] `https://qiskit.org/textbook/ch-states/introduction.html`

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 $|\psi\rangle$ ($\left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right)$) 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 $|0\rangle$ ($\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$) and $|1\rangle$ ($\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$). 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. $|\alpha|^2$ gives the probability of measuring the qubit to be in state $|0\rangle$, and $|\beta|^2$ gives the probabilities of measuring

[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.

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:

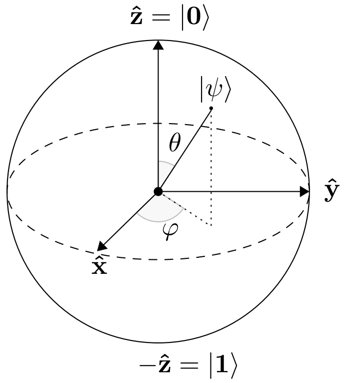
$$|\alpha|^2 + |\beta|^2 = 1$$

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]:


$\hat{\mathbf{z}} = |\mathbf{0}\rangle$
$|\psi\rangle$
θ
$\hat{\mathbf{y}}$
φ
$\hat{\mathbf{x}}$
$-\hat{\mathbf{z}} = |\mathbf{1}\rangle$

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. We might as well start with the simplest 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.

[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`

3.3 The Pauli 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 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.

3.4 The Phase (ST) Gates

3.5 The Hadamard Gate

4 Two Qubit Quantum Circuits

4.1 The Tensor Product - Qubits

4.2 The Tensor Product - Gates

4.3 Entanglement and CNOT Gates

4.4 Universality

To finish

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