PC351: Quantum Computing

by Scott King

Winter Term 2017

1 Introduction

- *Quantum information science* is the study of how laws of quantum mechanics can be used to perform processing tasks
- They will be able to solve or make efficient tasks such as optimizaation, NP-complete problems

1.1 Classical computation

In classical computing, a bit is a binary digit, represented as 0 or 1; and it is in only one state at any given time. In quantum computing, we need to represent that bits with vectors for their possible states. If we were to describe a *qubit* on a regular axis, it would be represented as:

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

and on a basis rotated 45°:

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

We use something known as *gates* to perform operations on the state vectors. The identity gate (I) works as such:

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} &\Rightarrow I|0\rangle \Rightarrow |0\rangle \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} &\Rightarrow I|1\rangle \Rightarrow |1\rangle \end{aligned}$$

There is also the bit flip (not) gate:

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

Most of the time we do no know the exact state of a qubit, so we represent them with probabilities:

$$\begin{aligned} |v\rangle &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \alpha\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \alpha|0\rangle + \beta|1\rangle \end{aligned}$$

And the probability that the qubit is 0 or 1 is $\alpha+\beta=1$.

Operators can be more general operations between any vector between the x and y axes.

Example 1. Hadamard gate, H:

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

The gates can also be applied using all Dirac notation, which is a standard notation for describing quantum states. Here the action of a Hadamard gate being applied:

$$\begin{aligned}
H(\alpha|0\rangle + \beta|1\rangle) &= \alpha H|0\rangle + \beta H|1\rangle \\
&= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \alpha|1\rangle + \beta|0\rangle - \beta|1\rangle) \\
&= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle \\
&= \frac{1}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle
\end{aligned}$$

since $\alpha+\beta=1$.

The idea to find these probabilities is to find the measurement matrix such that:

$$\begin{aligned}
\begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \\
&= M_0|v\rangle \\
M_1|v\rangle &= \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}
\end{aligned}$$

1.2 Quantum Bits

A *quantum bit*, mostly referenced to as, a **qubit** can be represented with the general form:

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

where $\alpha, \beta \in \mathbb{C}$. Remember that $|\alpha|^2 + |\beta|^2 = 1$; where $P(0) = |\alpha|^2$ and $P(1) = |\beta|^2$.

2 Quantum Model

Let's talk about how we define a qubit state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. We have to remember that α and β are complex numbers; so in the quantum case, we say that they are probability amplitudes. This isn't so bad, we can observe them!

The inability to directly observe the state is called a superposition. This sort of details that we are in a state that is a combination of both. (Ex. a qubit is as a state of 0,1 at the same time). We would say there is a superposition at $|0\rangle$ and $|1\rangle$.

There exists a *normalization condition* that says: $P(0)+P(1)=1$ and also $|\alpha|^2+|\beta|^2=1$.

Example 2. $|\psi\rangle=(1+i)|0\rangle+2|1\rangle$

$$\begin{aligned}
\alpha &= 1+i \\
|\alpha|^2 &= \alpha^* \alpha \\
&= (1-i)(1+i) \\
&= 1-i^2 \\
&= 2 \\
\beta &= 2 \\
|\beta|^2 &= \beta^* \beta \\
&= (2)(2) \\
&= 4
\end{aligned}$$

Based on the above, we can see that this state is not valid, as it does not pass the normalization condition: $|\alpha|^2+|\beta|^2=6\neq 1$.

Our condition is now $N=|\alpha|^2+|\beta|^2=6$. Let's define a new, normalized state:

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{N}}|\psi\rangle \\
&= \frac{1}{\sqrt{6}}[(1+i)|0\rangle+2|1\rangle]
\end{aligned}$$

We now have $\alpha=\frac{1+i}{\sqrt{6}}$ and $\beta=\frac{2}{\sqrt{6}}$ and the associated $|\alpha|^2=\frac{2}{6}$ and $|\beta|^2=\frac{4}{6}$. We have now just forced $|\alpha|^2+|\beta|^2=1$.

2.1 Complex numbers

First, let's define $|\alpha|=$ the magnitude and $i\,\theta=$ the phase. We can say that:

$$\begin{aligned}
\alpha &= \alpha_R+\alpha_{\mathrm{Im}} \\
&= |\alpha|e^{i\theta}
\end{aligned}$$

Note: $e^{i\theta}=\cos(\theta)+i\sin(\theta)$; $|\alpha|\cos(\theta)=\alpha_R$; $|\alpha|\sin(\theta)=\alpha_{\mathrm{Im}}$

We have:

$$\begin{aligned}
|\psi\rangle &= \alpha|0\rangle+\beta|1\rangle \\
&= |\alpha|e^{i\theta_\alpha}|0\rangle+|\beta|e^{i\theta_\beta}|1\rangle \\
&= e^{i\theta_\alpha}[|\alpha||0\rangle+|\beta|e^{i(\theta_\beta-\theta_\alpha)}|1\rangle]
\end{aligned}$$

We can then define: $e^{i(\theta_\beta-\theta_\alpha)}=e^{i\varphi}$. $|a|=\cos\left(\frac{\theta}{2}\right)$ and $|\beta|=\sin\left(\frac{\theta}{2}\right)$ and thus we have the identity:

$$|\alpha|^2+|\beta^2| = \cos^2\left(\frac{\theta}{2}\right)+\sin^2\left(\frac{\theta}{2}\right)=1$$

$$|\psi\rangle = e^{i\theta_\alpha}\left[\cos\left(\frac{\theta}{2}\right)|0\rangle+\sin\left(\frac{\theta}{2}\right)e^{i\varphi}|1\rangle\right]$$

at this point, we can drop the overall phase factor $e^{i\theta_\alpha}$.

$$\begin{aligned}
P(0) &= \alpha^* \alpha \\
&= \left(e^{-i\theta_\alpha}\cos\left(\frac{\theta}{2}\right)\right)\left(e^{i\theta_\alpha}\cos\left(\frac{\theta}{2}\right)\right) \\
&= \cos^2\left(\frac{\theta}{2}\right) \\
P(1) &= \beta^* \beta \\
&= \left(e^{-i\theta_\alpha}\sin\left(\frac{\theta}{2}\right)e^{-i\varphi}\right)\left(e^{i\theta_\alpha}\sin\left(\frac{\theta}{2}\right)e^{i\varphi}\right) \\
&= \sin^2\left(\frac{\theta}{2}\right)
\end{aligned}$$

The standard qubit state is $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\varphi}|1\rangle$. We say that this is the standard form of a qubit on the Bloch sphere.

All qubits can be represented as a vector of length 1. The surface of the Bloch sphere of all qubits is the space in which all gates will act.

Simple qubit gates (operators) are rotations that do not change the length of the vector. They for the set of *unitary* operators (matrices). They are defined as $U^\dagger U = 1 = I$.

2.2 Important unitary gates

$$\begin{aligned}
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} &\rightarrow \text{bit flip gate} \\
Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} &\rightarrow i\,X\,Z \\
Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} &\rightarrow \text{phase flip gate} \\
I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\rightarrow \text{identity gate} \\
X^2, Y^2, Z^2 &= I
\end{aligned}$$

$\dagger$ is called "dagger", and it works as such: $U^\dagger = (U^*)^T$.

Example 3. $M = \begin{pmatrix} 0 & i \\ 1 & 1 \end{pmatrix}$; $M^* = \begin{pmatrix} 0 & -i \\ 1 & 1 \end{pmatrix}$

$$\begin{aligned}
(M^*)^T &= \begin{pmatrix} 0 & 1 \\ -i & 1 \end{pmatrix} = M^\dagger \\
M^\dagger M &= \begin{pmatrix} 0 & 1 \\ -i & 1 \end{pmatrix}\begin{pmatrix} 0 & i \\ 1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \neq I
\end{aligned}$$

Let's show a general U, such that:

$$U = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}$$

where $U^\dagger U = I$.

$$U = e^{i\delta}\left[\cos\left(\frac{\gamma}{2}\right)1 + i\sin\left(\frac{\gamma}{2}\right)(n_x X + n_y Y + n_z Z)\right]$$

This can be written $\forall$ gates of U.