Contents

1 Lecture 1 **2**

1.1 Motivating Quantum Computing 2

1.2 Measurement 2

2 Lecture 2 **4**

2.1 Axioms of Quantum Mechanics 4

2.2 Bell Inequalities 5

1 Lecture 1

1.1 Motivating Quantum Computing

The classical unit of computation is a **bit**. How small can we shrink bits? Let's conduct a thought experiment. Let's suppose we could shrink them down to the size of a Hydrogen atom. The "state" of $|0\rangle$ being the ground state and $|1\rangle$ first excited state. However, electrons in general exist in superposition states! These states look like:

$$\{\alpha |0\rangle + \beta |1\rangle : \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$$

But it gets weirder. According to quantum theory, when conducting a measurement on such a state, we end up getting:

$$M = \begin{cases} 0 & \text{wp } |\alpha|^2 \\ 1 & \text{wp } |\beta|^2 \end{cases}$$

Furthermore, the act of measurement "collapses" the wavefunction to a state $|0\rangle$ or $|1\rangle$. Subsequent measurements will give that pure state deterministically.

Now, suppose we have a system of two such Hydrogen. There are now 4 basis states:

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

Effective computation now comes from extrapolating to n such **qubits**. Now such a state would look like $\sum_{x \in \{0,1\}} \alpha_x |x\rangle$.

This is pretty profound. Classical computers were designed to use nature (through silicon) in order to work for humans. But with all this effective work that nature is doing behind the scenes, it seems that quantum computing is really the more powerful framework we should've asked for.

1.2 Measurement

Now suppose we do a "partial" measurement, e.g. only measuring the first bit. What will we get? It seems reasonable that the probability should be the sum of the probabilities of getting a 0 in the first qubit, e.g. we get a 0 w.p. $|\alpha_{00}|^2 + |\alpha_{01}|^2$. The state collapses, but it must be renormalized so the coefficients can still be probabilities! So the new state is actually

$$\frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Now suppose we are given a qubit in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{e^{i\theta}}{\sqrt{2}} |1\rangle$$

How can we figure out θ (phase estimation)? Well if we measure this, we will get either 0 or 1 with probability $1/2$ each. This will tell us nothing about θ. It turns out this is only a special case of measurement.

To understand what general measurement is, we first go back to our state representation. What we really mean by a superposition is a linear combination of two vectors. We fix some basis $|0\rangle$ and $|1\rangle$, and a normalized state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ is a unit vector in a 2-dimensional complex vector space. Now we can think about a measurement in the following way:

Definition 1.1
A **measurement** of some state $|\phi\rangle$ in some basis $\mathcal{U}$ is a projection onto one of the basis vectors $|u\rangle$. The value of the measurement is: u with probability of the scalar projection squared, $\left|\frac{\langle u|\psi\rangle}{\langle \psi|\psi\rangle}\right|^2$.

So for example, let's stick to our 2-space and pick a new orthonormal basis $\{|u\rangle, |u^\perp\rangle\}$ and our state $|\psi\rangle$. Suppose $|\psi\rangle$ makes an angle of θ with the $|0\rangle$ axis and makes an angle of μ with the $|u\rangle$ axis. By a simple diagram, it's clear from ψ's projections that measurement in the standard basis yields 0 with probability $\cos^2\theta$ and in our new basis it yields u with probability $\cos^2\mu$.

Note 1.1
There is a bit of a subtlety here. We assumed that the amplitudes we are working with are real, but in general they can be complex. It turns out, all of quantum computing can be formalized with only real amplitudes, but it gets more messy when interfacing with physics. For now, we will assume real amplitudes only, but most results generalize to complex amplitudes.

Another common example of a basis is:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Measuring our original phase estimation in this new basis is exactly what we need! We just need to write it in the new basis to figure out the amplitudes:

$$\begin{aligned}
\frac{1}{\sqrt{2}}|0\rangle + e^{i\theta}\frac{1}{\sqrt{2}}|1\rangle &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\right) + e^{i\theta}\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle\right) && (1)\\
&= \frac{1}{2}(1+e^{i\theta})|+\rangle + \frac{1}{2}(1-e^{i\theta})|-\rangle && (2)\\
&= \frac{1}{2}(1+\cos\theta + i\sin\theta)|+\rangle + \dots && (3)\\
& && (4)
\end{aligned}$$

so we get $|+\rangle$ from the measurement with probability

$$\frac{1}{2}|1+\cos\theta + i\sin\theta|^2 = \cos^2(\theta/2)$$

Now we can repeat the measurement (with other processed inputs) to get statistics and thus a good estimate on θ.

2 Lecture 2

2.1 Axioms of Quantum Mechanics

We list some axioms of Quantum Mechanics. Consider an electron with k energy levels, $|0\rangle, |1\rangle, \ldots, |k-1\rangle$.

Note 2.1 (Superposition Principle)
If there are k distinguishable (eigenstates) of a system, then the state of a system can be written as:

$$|\psi\rangle = \sum_{j=0}^{k-1} \alpha_j |j\rangle$$

where $\alpha_j \in \mathbb{C}$ and $\sum_j |\alpha_j|^2 = 1$.

This forms a Hilbert space, i.e. a Complex inner product space (but we will often think of all amplitudes as real). The $\{|j\rangle\}_{j=0}^{k-1}$ forms a basis for this state space. We can think of

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{k-1} \end{pmatrix}, |0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots$$

For inner products, we use Dirac's Bra-Ket notation. As we have already seen, the "kets" are regular vectors and the "bras" $\langle\psi| = |\psi\rangle^\dagger$ are elements of the dual vector space (which can be thought of as conjugate transposes). This means:

$$\langle\psi| = |\psi\rangle^\dagger = \sum_j \left(\alpha_j |j\rangle\right)^\dagger = \sum_j \alpha_j^* \langle j|$$

where $(\cdot)^*$ is the complex conjugate.

Now define $|\phi\rangle = \sum_j \beta_j |j\rangle$. We can take inner products by using the following notation:

$$\langle\psi, \phi\rangle = \langle\psi|\phi\rangle = \left(\sum_i \alpha_i^* \langle i|\right)\left(\sum_j \beta_j |j\rangle\right) = \sum_{i,j} \alpha_i^* \beta_j \langle i|j\rangle = \sum_j \alpha_i^* \beta_j$$

Because $\langle i|j\rangle = 1$ if and only if $i = j$ (they form an orthonormal basis).

We generally use $k = 2$, call the Hilbert space generated $\mathcal{H}$. We typically think about chaining together (tensor-producting) this Hilbert space with itself n times. This is called a n-**qubit** state. A general state can then be written as:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

with $\alpha_x \in \mathbb{C}$ and $\sum_x |\alpha_x|^2 = 1$.

Note 2.2 (Measurement Principle)
Pick an orthonormal basis $\mathcal{U} = |u_0\rangle, |u_1\rangle, \ldots, |u_{k-1}\rangle$. The outcome of a measurement is j with probability $\left|\langle u_j|\psi\rangle\right|^2$. In this process, the state is also perturbed and turned into the state $|u_j\rangle$

Look at last lecture for examples of measuring in different bases, with real amplitudes one can think about qubit states geometrically. The basis $\{|+\rangle, |-\rangle\}$ serves us well.

2.2 Bell Inequalities

Let us look more closely at combining two qubits, each with states $\alpha_0 |0\rangle + \alpha_1 |1\rangle$, $\beta_0 |0\rangle + \beta_1 |1\rangle$. We (tensor) product them together, producing a state:

$$|\psi\rangle = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_0 |01\rangle + \alpha_0\beta_0 |10\rangle + \alpha_0\beta_0 |11\rangle$$

but most states are not a product of two states.

The Bell basis states are a common example of states which are **entangled**, e.g. cannot be written as "product states."

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}} |00\rangle \pm \frac{1}{\sqrt{2}} |11\rangle, \left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}} |01\rangle \pm \frac{1}{\sqrt{2}} |10\rangle$$

These four states form an orthonormal basis for two qubits.

Suppose your system was in the state Φ^+ and we did a partial measurement on the qubit Then with probability $1/2$ we collapse to $|00\rangle$ and with probability $1/2$ we collapse to $|11\rangle$. Note that we could achieve this in a classical sense too, with correlated ("glued") coin flips.

Furthermore, the Bell states are rotationally invariant.

Theorem 2.1
In any basis, we can write the Bell States as:

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle = \frac{1}{\sqrt{2}} |vv\rangle + \frac{1}{\sqrt{2}} \left|v^{\perp}v^{\perp}\right\rangle$$

Let's prove this. Suppose $v = \alpha |0\rangle + \beta |1\rangle$. Then without loss of generality, we can write $v^{\perp} = -\beta^* |0\rangle + \alpha^* |1\rangle$. This means that:

$$\begin{aligned} |vv\rangle + \left|v^{\perp}v^{\perp}\right\rangle &= (\alpha |0\rangle + \beta |1\rangle)(\alpha |0\rangle + \beta |1\rangle) + (-\beta^* |0\rangle + \alpha^* |1\rangle)(-\beta^* |0\rangle + \alpha^* |1\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned}$$

where some algebra is elided. Note that we could achieve this in a classical sense too, with correlated coin flips that are rotated.

To go beyond classical computation, we consider two qubit measurements. The first player measures in the standard basis and the second player measures in a new basis, $\{|v\rangle, |v^{\perp}\rangle\}$, rotated at an angle θ from the standard basis. The probability that these two measurements are inequal is $\sin^2\theta$ (for example, if the first measurement is 0, then the state $|00\rangle$, so the component of $|v\rangle$ in the $|0\rangle$ direction is $\cos\theta$).

However, classically, the probability that one observes a different outcome is proportional to θ.

So John Bell's experiment is as follows. Alice is given a uniformly random bit x and Bob is given a uniformly random bit y. They must each report back a bit a and b respectively. Alice and Bob "win" the game if $xy = a + b \pmod 2$.

They can play the game in two ways: either classically or quantumly. Classically, they cannot communicate (apart from maybe the "glued" coin). In the quantum setup, Alice and Bob share a Bell state. If Alice chooses a bit 0, they measure their qubit in the standard basis, otherwise they measure it in a basis rotated by $\pi/4$. If Bob chooses a bit 1, they measure their qubit in a basis rotated by $\pi/8$, otherwise they measure in a basis rotated by $-\pi/8$. Call their measured bits a and b respectively.

We then mention the following two facts:

1. No classical strategy can win with probability $> 75\%$. A randomized strategy can do no better than a deterministic strategy since the opponent's strategy is known. The best deterministic strategy is to report $a = 0$ and $b = 0$ (or $a = 1$ and $b = 1$), because $xy = 0$ with probability 75% (if at least one of the bits is 0); trying to force the answer to be 1 will give you a lower probability of success. You can do no better. The glued coin doesn't help you either; the best it could do is give you a shared source of randomness.

2. In each of the 4 cases, the probability winning in a quantum setup is $\cos^2 \pi/8 \approx 85\%$. For example, take the case when x and y are both 0. Then they need to both measure a 1 or both measure a 0. The probability Alice measures a 0 is $1/2$ and then collapses the state to a $|00\rangle$. The probability that Bob then sees a 0 is $\cos^2 \frac{\pi}{8}$ because of the rotation, giving us $\frac{1}{2} \cos^2 \frac{\pi}{8}$. Likewise, the probability Alice measures a 1 is $1/2$ and then collapses the state to a $|11\rangle$. The probability that Bob then sees a 1 is $\cos^2 \frac{\pi}{8}$, so overall the probability is $2 \cdot \frac{1}{2} \cdot \cos^2 \frac{\pi}{8} = \cos^2 \frac{\pi}{8}$. The other cases are similar.

which clearly shows the quantum setup gives us something not present in the classical one.