A Brief Intro To Quantum Computing (Part 1)

Quantum physics to me was always this mystifying property which gave unreal capabilities to subatomic particles.

I mean come on, teleportation? Being in two places at once? Seems science fiction to me. Now if you aren't aware of quantum mechanics, basically electrons or any other subatomic particle have some wacky but neat super powers such as **superposition,** *(the power to be a wave and a particle, at the same time)* **quantum tunnelling,** *(the power to bypass any barriers i.e move through walls)* **entanglement** *(the power to be psychic, like having a twin where if one is affected then simultaneously so is the other).*

Neat, huh? Unfortunately us humans don't have these super powers so these forces never really affect us or matter in the classical physics world.

Or so I thought.

Introducing: Quantum Computing

Despite giving us the most spectacular wave of technological innovation in human history, there are certain computational problems that the digital revolution still can't seem to solve. Some of these problems could be holding back key scientific breakthroughs, and even the global economy. Although conventional computers have been doubling in power and processing speed nearly every two years for decades, they still don't seem to be getting any closer to solving these persistent problems. The reason being that today's digital, conventional computers are built on a classical, and very limited, model of computing. In the long run, to efficiently solve the world's most persistent computing problems, we're going to have to turn to an entirely new and more capable computing: the quantum computer.

Ultimately, the difference between a classical computer and a quantum computer is not like the difference between an old car and a new one. Rather, it's like the difference between a horse and a hawk: while one can run, the other can fly. Classical computers and quantum computers are indeed that different.

With quantum computing we can harness the superpowers of superposition and entanglement to solve complex problems that our classical computers cannot do. **Thus a quantum computer uses the quantum phenomena of subatomic particles to compute complex mathematical problems.**

Things that are different in the quantum system are also difficult to grasp at first glance, in order to relax we may need to see a cat video. What about Schrodinger's cat? Schrödinger's Cat

Some of us may don't like cats or find Schrodinger's cat to be annoying so let's have a look at the "The talk" - SMBC comic about QC.

Why should we be excited about quantum computers?

Quantum computers are in their early stage of development much like the classical computers back in the 50's. No doubt with the classical computers came revolutionary technology such as the internet so imagine the applications of quantum computers for the future. *Who back in the*

50's could predict such a thing as social media and the concept of being connected to millions of people through transmitting signals?

Future Applications of quantum computers:

- Better online security with development in quantum encryption
- Significantly improve AI technology
- Drug research and discovery
- More accurate weather predictions
- Optimizing traffic control

And many more ...

Classically a bit basically represents information at a fundamental level. It can take either of the two states, a **1** or a **0**, an **ON** or an **OFF**, **TRUE** or **FALSE**, two stable levels of current or voltage, and so on. Any physical entity that has two stable states can be used to store a ***bit*** of information. In traditional computers, we generally use a **transistor** for this, which basically acts like a switch that can be turned ON or OFF.

The fundamental unit of information of a **Quantum computer** is termed as the "**Qubit**".

The logic is simple, it's like a bit that can have infinite states instead of two.

But how? Enter **superposition**. At any instant of time, a Qubit represents the superposition of the two states, (say 0 and 1) in any proportion. And when you measure it, it collapses to one of its states.

Superposition

The concept of superposition is important because this is what qubits (quantum bits) about! So let's start developing a mathematical model for the spin. Don't get scared, it is pretty simple. The pace will be slower in this part so you can take time to adjust to the notation in quantum mechanics. It builds the foundation of something pretty fun. Also, the math is far more simple than reconciling the theory with intuition.

When we say the spin of a particle is in a superposition of states, it simply means it is in a linear combination of up spin and down spin. Here is the equation in the Dirac notation.

$$\overbrace{\alpha_0 \underbrace{|0\rangle}_{\text{up spin}} + \alpha_1 \underbrace{|1\rangle}_{\text{down spin}}}^{\text{linear combination}}$$

The coefficient α is called the amplitude.

$$\underbrace{\alpha_0}_{\text{amplitude}} |0\rangle + \alpha_1 |1\rangle$$

Here, the up spin and the down spin states are just the basis vectors. The concept is similar to the x, y basis vectors in the law of motion in Physics.

$$\vec{p} = \alpha_0 \vec{x} + \alpha_1 \vec{y}$$

$$\underbrace{|\Psi\rangle}_{\text{quantum state}} = \underbrace{\alpha_0|0\rangle + \alpha_1|1\rangle}_{\text{superposition}}$$

The Dirac notation $|\psi\rangle$ is just a short form for a matrix.

$$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{bmatrix}\alpha_0 \\ \alpha_1\end{bmatrix}$$

superposition

$|0\rangle$ and $|1\rangle$ are the two orthogonal basis vectors that are encoded as:

$$|0\rangle = \begin{bmatrix}1 \\ 0\end{bmatrix}, \quad |1\rangle = \begin{bmatrix}0 \\ 1\end{bmatrix}$$

0: not spin up

1: spin down

It also has a dual form written as:

$$\langle 0| = \begin{bmatrix}1 & 0\end{bmatrix}, \quad \langle 1| = \begin{bmatrix}0 & 1\end{bmatrix}$$

The math is simply matrix multiplication and linear algebra. We just shorten it with Dirac notation. Once you get familiar with it, we can take a lot of shortcuts to manipulate them easily. For example, the inner product of two orthogonal basis vectors $\langle 0|1\rangle$ is the multiplication of the 1 × 2 and 2 × 1 matrix. It is always zero. The inner product of any superposition is one, i.e. the total probability = 1.

$$\langle 0|1\rangle = 0, \quad \langle 1|1\rangle = \langle\Psi|\Psi\rangle = 1$$

Here are some more superposition states and the corresponding matrix.

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 \\ 1\end{bmatrix}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 \\ -1\end{bmatrix}$$

If you want more details on the notation again, Quantum Computing - Quantum Mechanics

Notation and Observables article (Part 0 of this series) provides you a summary for your later reference. But let's get into something important.

Between measurements, we can manipulate the superpositions. But when we measure the up spin, the superposition collapses to one of the possible states, i.e. either $|0\rangle$ or $|1\rangle$. This is the core principle of quantum dynamics, and how nature works. Let's say a particle is in:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

The chance that it collapses to a particular state equals the square of the corresponding amplitude. It turns out this method models the experimental results very well. In our example, the chance of measuring the particle in up spin is therefore 1/2.

square the coeff. to find the chance to be measured as up spin

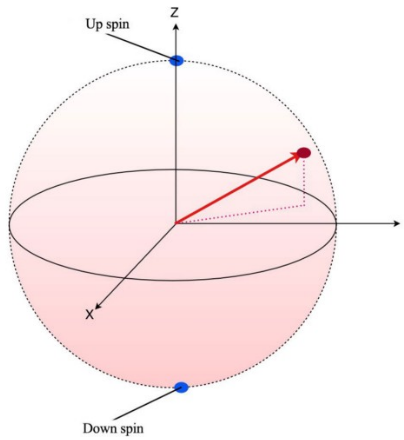
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

up spin

There is one obvious rule we need to follow. The probabilities of measuring all possible states add up to 1 ($\langle\psi|\psi\rangle=1$). To enforce this, we make

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

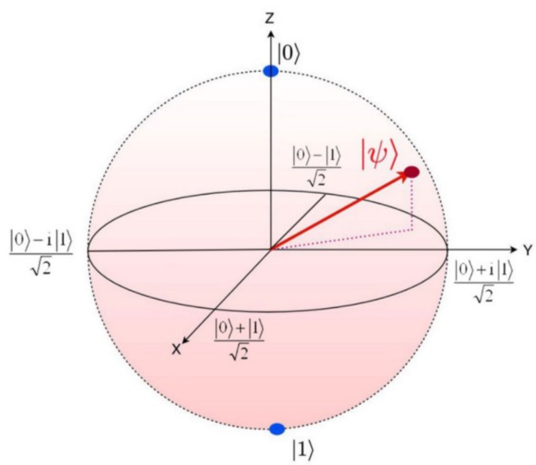
We can visualize the superposition as a point lying on the surface of a unit sphere. The up and down spin is just the north and south pole of the sphere respectively. So the red dot below is another example of a superposition state. When it is measured, nature forces it to take a side, either up or down.



But I am not 100% honest with you. To really have the superposition represented as the Bloch sphere above, the amplitude α can also be a complex number like:

$$\frac{1-i}{2\sqrt{2}}\left|0\right\rangle + \frac{1+i}{2\sqrt{2}}\left|1\right\rangle$$

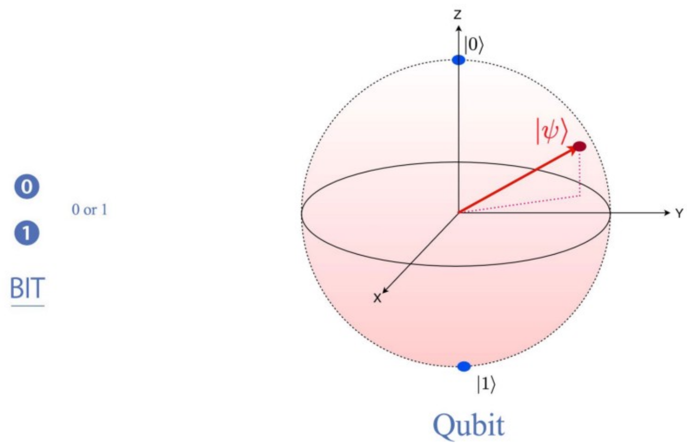
Here are the values of the superpositions in the six corners.



To calculate the probability, we compute the square of the norm, i.e. multiply the amplitude with its complex conjugate. (The complex conjugate of 3+4i is 3–4i)

$$\alpha^*_i \; \alpha_i$$

Let’s have a quick recap on “bits v.s. qubits”. A bit represents one of the two possible values, 0 or 1. A qubit represents points on the surface of the unit sphere. For round 1, a qubit wins over a bit on how many states that it can represent.



In addition, we can combine quantum states in forming a composite system. By the principle of quantum mechanics, a composite system is modeled by a tensor product.

$$|v\rangle \otimes |w\rangle \text{ or } |vw\rangle$$

Where

$$|a\rangle\ |b\rangle = \ |a\rangle \otimes |b\rangle = \begin{bmatrix} xu \\ xv \\ \vdots \\ yu \\ yv \\ \vdots \end{bmatrix}$$

For example, this is a composite system with 2 down spins and 1 up spin:

$$\begin{aligned} |101\rangle &= |1\rangle \otimes |0\rangle \otimes |1\rangle \\ &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}^{\mathrm{T}} \end{aligned}$$

Soon, we will see why this is so powerful — something that classical computing cannot deliver.

Here is another 3-qubits example:

$$\begin{aligned} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |1\rangle \otimes |1\rangle \quad &\equiv \quad \frac{1}{\sqrt{2}}\left(|011\rangle + |111\rangle\right) \\ &\equiv \quad \frac{1}{\sqrt{2}}\left(|3\rangle + |7\rangle\right). \end{aligned}$$

Here writing |011> as |3> is a shorthand notation where |011> is in binary and |3> is in decimal.

Below are the general equations describing a 2-qubit system. It consists of the spins of 2 particles.

$$|\Psi_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \quad |\Psi_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

$$\underbrace{|\Psi_0\rangle|\Psi_1\rangle}_{\text{2 qubits}} = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

So the new quantum state has 4 computational basis vectors, namely $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ with 4 complex coefficients.

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

For 3-qubits, we have 8.

$$|\psi_2\rangle = a_0\,|000\rangle + a_1\,|001\rangle + a_2\,|010\rangle + a_3\,|011\rangle + a_4\,|100\rangle + a_5\,|101\rangle + a_6\,|110\rangle + a_7\,|111\rangle$$

The system grows exponentially. 64-Qubits has

18,446,744,073,709,551,616 (20 digits)

basis vectors. With 64-qubits, we can encode and manipulate a lot of data using these billion-billion coefficients (dimensions). Qubits won round two.

Increasing the qubits linearly, we expand the information capacity exponentially.

But, there is a big catch! We can manipulate information in a very high dimensional space but we cannot read those coefficients directly. When all operations are completed, the only way to "read" the qubits is to measure it which returns one of the states only (not the coefficient).

no direct access

$$|\psi_2\rangle = a_0\,|000\rangle + a_1\,|001\rangle + a_2\,\underbrace{|010\rangle}_{\text{Get one of the states when measured}} + a_3\,|011\rangle + a_4\,|100\rangle + a_5\,|101\rangle + a_6\,|110\rangle + a_7\,|111\rangle$$

When qubits are measured, the capacity is no different from bits. It’s extremely tricky to design algorithms under this constraint. We have a turbocharged concept but the way to do things is awkward. We will come back to this later.

Now, we understand the Qubits, the equivalent of bits in the classical computer but far more powerful. In a classical computer, we have +, -, ×, ÷ operators to manipulate bits. Quantum computers have none of them. So how do we manipulate qubits? This will be answered in the next article.

References

https://www.mustythoughts.com/resources.html
Quantum Mechanics: The Theoretical Minimum - Susskind, Leonard, Friedman
Articles from Jonathan Hui
The Role of Interference and Entanglement in Quantum Computing - Jurgen Van Gael
Quantum Computation and Quantum Information - Nielsen and Chuang