The Quantum Leap
November 14, 2021

Quantum Superposition and Entanglement

In prior posts I emphasized the excitement and potential of Quantum Computing, without any reference to the underlying quantum mechanics, but would like to introduce you to some unique quantum properties in this post. While understanding the nature of Quantum Computing is complex and contains many new concepts, a basic understanding of "Superposition" and "Entanglement" is fundamental to grasp why this new computing methodology is so novel, powerful and exciting. I am going to try to describe these concepts in a way that does not require any math, although I will use some math references to highlight how these concepts manifest.

Superposition

As noted in the prior post, one of the fundamental differences between Quantum Computers and classical computers lies in the core components used to process information. We know that classical computers use a binary system, meaning each processing unit, or bit, is either a "1" or a "0" ("on" or "off") whereas Quantum Computers use **qubits** which can be either "1" or "0" (typically "spin up" or "spin down") or both at the same time, a state referred to as being in a ***superposition***. This is a bit more subtle than it sounds because in order to use qubits for computational purposes, they need to be measured and whenever you measure a qubit you will find it collapsing into either the 1 or 0 state. But *between* measurements, **a quantum system can be in a superposition of both at the same time**. While this seems counter-intuitive, and somewhat supernatural, it is well proven so please try and accept it at face value in order to get the gist of the other concepts covered in this post. For a deeper dive into superposition from a particle physics perspective (light is both a particle and a wave), you can investigate Wave–particle duality. [Fun Fact—Einstein did not receive the Nobel prize for his famous E=MC2 relativity equation but rather for his photoelectric effect work, which is fundamental to quantum mechanics, where he postulated the existence of photons, or "quanta" of light energy which underpins much of the power behind Quantum Computing].

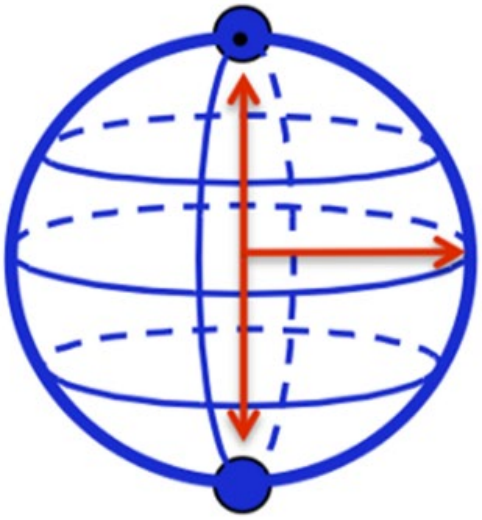
Without getting into the physics or explaining complex numbers, Superposition can be mathematically depicted as:

$$|\psi\rangle := \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}; \quad |\alpha|^2 + |\beta|^2 = 1.$$

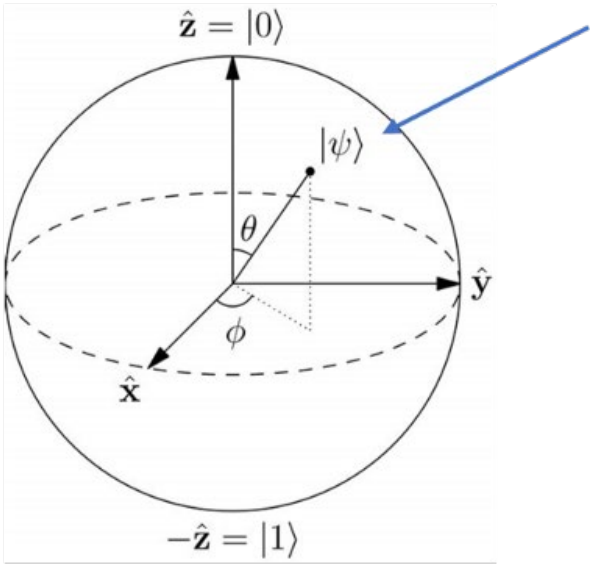
Please bear with me here, I have promised not to overwhelm you with complex math, I only want to highlight how to think about Superposition in a way that will help you appreciate its power for computing and to share the nomenclature that is generally used in the field. Don't focus on the Greek characters (psi, alpha and beta) or the linear algebra notation (the |Ket> notations and the parenthetical portion). Simply note that the equation above on the left, is the mathematical representation of a qubit and is simply stating that there is a probability that a given qubit (the Psi or trident symbol) when measured is "0" (the alpha symbol) and a probability that the qubit is a "1" (the beta symbol). The equation on the right, known as the

Born rule, is simply stating that the two probabilities add to 100%. Let me reframe that in a simpler manner. Before a qubit is measured, it is both a “1” and a “0” at the same time and the relative odds of it being one or the other are included in the qubit equation. In practice this means that using Quantum Computers to solve problems becomes a probabilistic analysis, and if the equations are run enough times, they will average out to the answer.

You may recall in a prior post that qubits are described as 3-dimensional, as shown below in blue and red. The line drawing version with the funny symbols, shows how this is used for calculations when put into a superposition (the math and symbols are helpful for those comfortable with them, but not essential for a general understanding):



Qubit



In this depiction, if the North pole is “0” and the South pole is “1” and if the qubit is tilted to the side, the degree of its tilt translates generally into these probabilities. In the image with the blue arrow pointing to psi, you will notice that the psi symbol looks like it is leaning between north and south, in this case closer to north. For example, this might be represented as “0.8 |0> + 0.6 |1>” meaning it is leaning closer to “0”. This generally means it would have a higher probability of being 0 when measured. [You will also note that if you square each term, you get 0.64 + 0.36 which equals 1, and therefore follows the Born rule, and roughly means that the odds of this qubit being a 0 are 64% and the odds of it being a 1 are 36%.]

The important part to take away is that since a qubit can represent an input with various weightings of 1 and 0, it contains much more information than a simple binary bit.

Entanglement

If the above explanation of superposition seems a bit unintuitive, I'm afraid that entanglement might seem even more bizarre [don't worry, you're not alone, even Einstein struggled with it], but I will do my best to explain it. I will ask you to accept that, like Superposition, this is an actual phenomenon which is well proven, even if you likely won't be able to picture it in your mind in a way that will be satisfying. And it is this feature of quantum mechanics that largely underpins the awesome power of Quantum Computers because it enables the information processing to scale by an **exponential factor** (more on that below).

Quantum entanglement is a physical phenomenon that occurs when a group of particles are created, interact, or share proximity in such a way that the particles are "connected," even if they are subsequently separated by large distances. Qubits are made of things such as electrons (which spin in one of two directions) or photons (which are polarized in one of two directions), and when they become "*entangled*", their spin or polarization becomes perfectly correlated. In fact, this concept is much older than Quantum Computers and was first described in 1935 by Einstein, along with Boris Podolsky and Nathan Rosen, and become known as the EPR (each of their initials) paradox, which Einstein famously referred to as "spooky action at a distance". What it means, simply, is that qubits can be made to entangle, which then enables them to correlate with each other. Quantum Computers use microwaves or lasers to nudge the qubits into a state/alignment where they can be correlated, or entangled.

Now let's walk through how this entanglement can manifest in an exponential increase in computing power. If we consider two classical bits, we know that they can be either 1 or 0, so together they can take on the following values:

0, 0

1, 0

0, 1

1,1

However, two entangled qubits can take all those values at once, because of the entanglement, so in this case 2 *qubits* can take the value of 4 *bits*. If we consider three classical bits, they can be any of the following combined entries:

0, 0, 0; 1, 0, 0

0, 1, 0; 1, 1, 0

0, 0, 1; 1, 0, 1

0, 1, 1; 1, 1, 1

So, in this case there are 8 combinations, but this can be fully described using 3 qubits (again because they are entangled). Mathematically, the number of bits required to match the computing power of qubits is as follows: **n qubits = 2^n bits** or an ***exponential*** relationship. For now, don't try and picture how entangled qubits do this, just know that they do. The purpose of this line of analysis is to give some numerical context as to why this entanglement makes Quantum Computers (phenomenally) more powerful than classical computers.

If we continue the logic above for increasing numbers of bits/qubits we get the following:

# of Qubits	Requited Bits to Match	Equivalent Classical Computer RAM [1]
1	2	2 bits
2	4	4 bits
3	8	1 byte
4	16	2 bytes
5	32	4 bytes
6	64	8 bytes
7	128	16 bytes
8	256	32 bytes
9	512	64 bytes
10	1024	128 bytes
11	2048	256 bytes
12	4096	512 bytes
13	8192	1 KB

[1] RAM = Rapid Access Memory. There are 8 bits in a byte

So, it only takes 13 qubits to have the equivalent classical computing power as a kilobyte (KB). Now let's see how that manifests in computer power/speed.

Let's assume we have a pretty powerful current classical computer processer, which might have a clock speed of 4 GHz, which means it can execute 4 BILLION cycles per second which sounds (and is) phenomenally fast. High end current gaming PCs generally operate at this speed and provide an excellent performance experience. Let's now use this baseline processing speed, and scale up the prior table, to see the profound impact of *exponential computing power* on processing time:

# of Qubits	Requited Bits to Match	Equivalent Classical Computer RAM	Equivalent Classical Computer Processing Time
10	1024	128 bytes	2.6 µs
20	1,048,576	131 KB	0.26 ms
30	1.1 billion	134 MB	0.27 seconds
40	1.1 trillion	137 Gigabytes	4.6 minutes
53	$9.0x10^{15}$	1 Terabyte	625 hours
63	$9.0x10^{18}$	1 Petabyte	73 years
100	$9.0x10^{30}$	1 Exabyte	10 trillion years
1,000	$9.0x10^{301}$	$1.3x10^{232}$ Exabytes	$8.5x10^{283}$ years

To give this some context, 100 qubits is the equivalent of an Exabyte of classical computing RAM which is a million trillion bytes (18 zeros). It would take a powerful classical computer nearly the lifetime of the universe to process that amount of data! The corollary is that quantum computers can perform certain complex calculations phenomenally faster than classical computers, and this concept of entanglement is a key to the performance superiority.

While this analysis assumes certain types of computer analysis/equations, the point is to show how Quantum Computers can process information at an **unprecedented speedup**.

The key takeaway from this post is that Quantum Computers, using qubits that can be both in superposition and entangled, allow these machines to process inputs much faster than is possible with classical computing architecture. Now all we need is a reliable working Quantum Computer with just 100 qubits, which would not only enable massive speedup for certain problems but would open the door to all sorts of new questions and analyses. Many experts predict this will be achieved within 5 years (IonQ has recently showcased a Quantum Computer with 32 entangled qubits, so real progress is being made). Some general categories of problems where this phenomenal speedup will have a profound impact include simulation, optimization and encryption. In the next post I will provide more insights into what types of problems can be solved with the exponential speedup that can be provided by Quantum Computers.

References:

https://towardsdatascience.com/the-need-promise-and-reality-of-quantum-computing-4264ce15c6c0

https://vincentlauzon.com/2018/03/21/quantum-computing-how-does-it-scale/

If you enjoyed this post, please visit my website and enter your email to receive future posts and updates: http://quantumleap.blog

Russ Fein is a venture investor with deep interests in Quantum Computing (QC). For more of his thoughts about QC please visit the link to the left. For more information about his firm, please visit Corporate Fuel. Russ can be reached at russ@quantumleap.blog.