The Quantum Leap
January 24, 2022

A Quantum Computing Glossary

Hopefully many of you have been following this blog since it began and are familiar with the terms highlighted below. For some of you, a refresher for reference may be helpful. For others, this may all be very overwhelming and confusing. I've curated this list to provide a broad set of definitions that should help frame the Quantum Computing (QC) potential, and for ease of reference as you come across terms where a definitional reminder would be helpful. In the first post in this series, I introduced QC with the following word-cloud graphic:

While not every word in this cloud bears defining in this post, I hope many of these definitions help you in your efforts to understand and appreciate QC, and I have grouped them into silos to add context (although some may naturally apply to more than one silo). This is not intended to be a complete list, and it's likely that more definitions will need to be added over time, but this should provide a good grounding in the general nomenclature and principles.

Quantum Concepts

- Dirac Notation: Symbolic representation of quantum states via linear algebra, also called *bra-ket* notation. The *bra* portion represents a row vector and the *ket* portion represents a column vector. While a general understanding of QC does not necessarily require familiarity with linear algebra or these notations, it is fundamental to a deeper working knowledge.
- Collapse: The phenomenon that occurs upon measurement of a quantum system where the system reverts to a single observable state. Said another way, after a qubit is put into a superposition, upon measurement it collapses to either a 1 or a 0.

- Quantum Supremacy: Demonstrating that a programmable quantum device can solve any problem that no classical computing device can solve in a feasible amount of time, irrespective of the usefulness of the problem. Based on this definition, the threshold was passed in October 2019.
- Quantum Advantage: Refers to the demonstrated and measured success in processing a real-world problem faster on a Quantum Computer than on a classical computer. While it is generally accepted that we have achieved quantum supremacy, it is anticipated that quantum advantage is still some years away.
- Quantum Tunneling: Quantum Tunnelling is the quantum mechanical effect in which particles have a probability of crossing a barrier or transitioning through an energy state normally forbidden by classical physics, due to the wave-like aspect of particles.
- Bloch Sphere: a geometrical representation of the state space of a qubit, named after the physicist Felix Bloch. The Bloch Sphere provides the following interpretation: the poles represent classical bits, and we use the notation $|0\rangle$ and $|1\rangle$. However, while these are the only possible states for the classical bit representation, quantum bits cover the whole sphere. Thus, there is much more information involved in the quantum bits, and the Bloch sphere depicts this.
- Entanglement: 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.
- Superposition: 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.
- Schrodinger's Cat: A quantum mechanics construct or thought experiment that illustrates the paradox of superposition wherein the cat may be considered both alive and dead (until the box is opened and its status is then known for certain). This "both alive and dead" concept often confuses early students of quantum mechanics.
- Heisenberg Uncertainty: (also known as Heisenberg's uncertainty principle) is any of a variety of mathematical inequalities asserting a fundamental limit to the accuracy with which the position and momentum of a particle can be known based on its starting parameters. Generally, the more precise the position location is, the less precise the momentum can be described, and vice versa. This also confuses early students of quantum mechanics who are used to typical physics where speed and position are usually well known by observation.

Hardware/Physical Components

- Auxiliary Qubit: Unfortunately, there is no such thing as quantum-RAM so it is difficult for QC's to store information for extended periods of time. An "Auxiliary Qubit" serves as a temporary memory for a quantum computer and is allocated and de-allocated as needed (also referred to as an ancilla).
- Cryogenics: Operating at extremely cold temperatures, generally meant to be less than -153 Celsius, or in the case of QC, -180 Celsius. Cryogenics are of particular interest for QC

when applied to silicon-based semiconductors because at this temperature, such semiconductors operate with superconductivity (i.e., the electrons flow with no loss to resistance).

- Dilution Refrigerator: Used in superconducting qubits and often with quantum dots, whereby a series of physical levels (typically 7) are sequentially chilled to the lowest level, where the qubits operate.
- High Performing Computer (HPC): Sometimes also referred to as a "supercomputer" is generally meant to represent any ultra-high performing classical computer. Powerful gaming PCs operate at 3 GHz (i.e., 3 billion calculations per second) while HPC's operate at quadrillions of calculations per second. Despite this blazing speed, there are many problems that HPC's cannot perform in a reasonable about of time, but theoretically can be done with a QC in a very short amount of time.
- Quantum Annealer: Annealing is used to harden iron, where the temperature is raised so the molecular speed increases and strong bonds are formed. The iron is then slowly cooled which reinforces these new bonds, a process called "annealing" in metallurgy. Quantum annealing works in a similar way, where the temperature is replaced by energy and the lowest energy state, the global minimum, is found via annealing. Quantum annealing is a quantum computing method used to find the optimal solution of problems involving many solutions, by taking advantage of properties specific to quantum physics. Since there are no "Gates", the mechanics of annealing are less daunting than full blown QC, although the outputs are less refined and precise than they would be under a full gate-based QC.
- Quantum Dot: Quantum dots are effectively "artificial atoms." They are nanocrystals of semiconductor wherein an electron-hole pair can be trapped. The nanometer size is comparable to the wavelength of light and so, just like in an atom, the electron can occupy discrete energy levels. The dots can be confined in a photonic crystal cavity, where they can be probed with laser light.
- Quantum Sensor: Quantum sensing has a broad variety of use cases including enhanced imaging, radar and for navigation where GPS is unavailable. Probes with highly precise measurements of time, acceleration, and changes in magnetic, electric or gravitational fields can provide precise tracking of movement. In this case, if a starting point is known, the exact future position is also known, without the need for external GPS signals, and without the ability for an adversary to jam or interfere with the signals, so this is of particular interest to the military. Another application of quantum sensing involves ghost imaging and quantum illumination. Ghost imaging uses quantum properties to detect distant objects using very weak illumination beams that are difficult for the target to detect, and which can penetrate smoke and clouds. Quantum illumination is similar and can be used in quantum radar.
- Qubit: Also known as a quantum bit, a qubit is the basic building block of a quantum computer. In addition to the conventional—binary—states of 0 or 1, it can also assume a superposition of the two values. There are several different ways that qubits can be created with no clear candidate emerging as the definitive method.

Computing Operations

- Fault Tolerance: technical noise in electronics, lasers, and other components of quantum computers lead to small imperfections in every single computing operation. These small errors ultimately lead to erroneous computation results. Such errors can be countered by encoding one logical qubit redundantly into multiple physical qubits. The required number of redundant

physical qubits depends on the amount of technical noise in the system. For superconducting qubits, experts expect that about 1,000 physical qubits are required to encode one logical qubit. For trapped ions, due to their lower noise levels, only a few dozens of physical qubits are required. Systems in which these errors are corrected are fault tolerant.

- Gate: A basic operation on quantum bits and the quantum analogue to a conventional logic gate. Unlike conventional logic gates, quantum gates are reversible. Quantum algorithms are constructed from sequences of quantum gates.
- Hadamard Gate: The Hadamard operation acts on a single qubit and puts it in an even superposition (i.e., turns and spins the qubit so the poles face left and right instead of up and down). It is a universal gate operation which establishes superposition.
- Measurement: the act of observing a quantum state. This observation will yield classical information, but the measurement process will change the quantum state. For instance, if the state is in superposition, this measurement will 'collapse' it into a classical state of 1 or 0. Before a measurement is done, there is no way of knowing what the outcome will be.
- NISQ: Noisy intermediate-scale quantum, coined by John Preskill in 2017, meant to depict the current state of QC whereby qubits suffer from noise and rapid decoherence. It generally means the establishment of 50-100 logical qubits (the "intermediate-scale" portion of the definition, which would require 100,000 – 1,000,000 physical qubits with the balance of the qubits dedicated to noise reduction).
- Noise: In QC, noise is anything which impacts a qubit in an undesirable way, namely electromagnetic charges, gravity or temperature fluctuations, mechanical vibrations, voltage changes, scattered photons, etc. Because of the precise nature of qubits, such noise is nearly impossible to prevent and requires substantial error-correction (to correct for the noise) in order to allow the qubits to perform desired calculations.
- No Cloning Theorem: The no-cloning principle is a fundamental property of quantum mechanics which states that, given a quantum state, there is no reliable way of producing extra copies of that state. This means that information encoded in quantum states is unique. This is sometimes annoying, such as when we want to protect quantum information from outside influences, but it is also sometimes especially useful, such as when we want to communicate securely with someone else.
- Oracle: A subroutine that provides data-dependent information to a quantum algorithm at runtime. It is often used in the context of "how many questions must be asked before an answer can be given" in order to confirm or establish quantum advantage.
- Quantum Algorithm: An algorithm is a collection of instructions that allows you to compute a function, for instance the square of a number. A quantum algorithm is exactly the same thing, but the instructions also allow superpositions to be made and entanglement to be created. This allows quantum algorithms to do certain things that cannot be done efficiently with regular algorithms.
- Quantum Development Kit (QDK): A number of providers offer different types of QDK's including some that are proprietary and others that are open source. It generally contains the programming language for quantum computing along with various libraries, samples and tutorials. QDK's are available from the following companies (with their QDK name in parentheses): D-Wave (Ocean), Rigetti (Forest), IBM (Qiskit), Google (Cirq), Microsoft (Microsoft QDK), Zapata (Orquestra), 1Qbit (1Qbit SDK), Amazon (Braket), ETH Zurich (ProjectQ), Xanadu (Strawberry Fields) and Riverlane (Anian).

- Quantum Error Correction: The environment can disturb the computational state of qubits, thereby causing information loss. Quantum error correction combats this loss by taking the computational state of the system and spreading it out over an entangled state using many qubits. This entanglement allows observers to identify and remedy disturbances without observing the computational state itself, which would collapse it. However, many 100's or 1000's of error correcting qubits are required for each logical qubit.
- Speedup: The improvement in speed for a problem solved by a quantum algorithm compared to running the same problem through a conventional algorithm on conventional hardware.
- Coherence/Decoherence: Coherence is the ability of a qubit to maintain its state over time. Decoherence generally occurs when the quantum system exchanges energy with its environment, typically from gravity, electromagnetism, temperature fluctuation or other physical inputs (see "Noise"). Longer coherence times generally enable more computations and therefore more computational power for QC.

Applications

- Quantum Cloud: Access to Quantum Computers via a cloud-based provider. Some prominent firms currently offering such access includes IBM, Amazon, Google, and Microsoft, among others. Two benefits of such QC access included lower up-front costs (users do not need to buy any hardware) and futureproofing (i.e., as the QC makers create more powerful machines, cloud access can be directed to the newer machines without any added investment required by the users).
- Quantum Communication: A method of communication that leverages certain features of quantum mechanics to ensure security. Specifically, once a given qubit is "observed" or measured, it collapses to either a "1" or a "0". Therefore, if anyone intercepts or reads a secure quantum message, the code will have changed such that the sender and receiver can see the impact of the breach. QKD or quantum key distribution is an existing technology that is already in use over fiber optics, certain line-of-sight transmissions, and recently by China via a special satellite, between Beijing and Austria.
- Shor's Algorithm: An integer factorization algorithm written in 1994 by American mathematician Peter Shor. It is open-sourced and currently available to anyone to use to break RSA encryption or other protocols relying on the difficulty of factoring large numbers. For this reason, it is often cited as a clear example of the need and desire for a powerful enough QC to run the algorithm. No QCs are yet powerful enough to use this algorithm to circumvent RSA or related encryption, but that will change at some point in the coming years. "Post-Quantum" encryption is generally meant as a protocol that would not be vulnerable to Shor's Algorithm.
- Grover's Algorithm: Another open-source algorithm already written, intended for search optimization. For most current computer searches, the target samples must either be processed one at a time until the desired result is found, or the data must be organized (i.e., put in numerical or alphabetical order) to be searched more efficiently. Grover's algorithm can simultaneously search much of the entire field (depending on the power of the QC) and therefore find results much faster. Shor's and Grover's algorithms are often the first two algorithms cited when discussing quantum supremacy and are elegant examples of the speedup that QC's can provide.

I hope this glossary is a useful companion for your journey in understanding and appreciating Quantum Computing. Feedback is always invited.

***Disclosure**: I have no beneficial positions in stocks discussed in this review, nor do I have any business relationship with any company mentioned in this post. I wrote this article myself and express it as my own opinion.*

References:

Quantum Computing: Progress and Prospects, The National Academies Press, 2019

Azure Quantum Glossary, Microsoft.com, accessed January 22, 2022

The Rise of Quantum Computing, McKinsey & Company, December 14, 2021

Glossary, Dotquantum.io, accessed January 22, 2022

Dilmegani, Cem, Quantum Computing Programming Languages, AI Multiple, published April 11, 2021, updated January 4, 2022.

Parker, Edward, "Commercial and Military Applications and Timelines for Quantum Technology" Rand Corporation, July, 2020.

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.