The Quantum Mechanical Background of Quantum Computing

Isaac Hanna
Liberty University

The Quantum Mechanical Background of Quantum Computing

Isaac Hanna

Abstract

Quantum mechanics arose out of the question "Is light a particle or a wave?" and has laid forth a model of reality in which particles are modeled by wave functions. The particle is in a superposition of states and can be entangled with other particles to create more complex systems. Observation of the system collapses the wave function to a single point. By using quantum gates, we can manipulate these particles to create algorithms to solve computational problems. Quantum computing does not collapse the complexity hierarchy by providing an across the board exponential speedup but can provide such a speedup for certain problems using algorithms that are specifically tailored to the nature of the problem, most notable Shor's algorithm for integer factorization.

The Quantum Mechanical Background of Quantum Computing

The demise of Moore's Law and the increasing complexity of computational problems has led to a search for new ways of finding computational speedups. One potential solution at the forefront of computing research is quantum computing. Particles at the quantum level display unusual properties that can be very helpful for computing certain problems. While the speedup is not as extreme or widespread as it is sometimes made out to be, it does allow for faster solutions to some key problems.

Quantum Mechanics

In order to understand how quantum mechanics allows for computational speedup, we must first have a basic understanding of quantum mechanics. In this section, we will cover the development of quantum mechanics, the core properties, and some of the notation that will be helpful in understanding quantum computing.

Particle/Wave Duality

Prior to 1801, light was thought to consist of particles. In 1801, Thomas Young showed that it actually consists of waves. He shone a light through a barrier with two slits in it onto another surface. If light consisted of particles, the pattern would be a smooth curve with peak at the middle of the surface. If light instead consisted of waves, the waves coming through the two slits would interfere, creating a pattern of alternating light and dark spots on the surface. Young found the second of these patterns, demonstrating that light does consist of waves (Feynman, Leighton, and Sands, 1964).

In the late 1800s. Heinrich Hertz observed that the ability of light to dislodge electrons from a metallic surface is dependent not on the intensity of light–which would be akin to the size

of the wave if light is viewed as a wave– but on its frequency–the number of waves hitting it per second. This did not seem to fit with the wave nature of light, and so Einstein proposed a particle-based theory of light. This particle view, however, could not explain the wave-like nature that Young had observed (Zubairy, 2020).

Young's experiment has also been considered with electrons and the results are the same. Peculiarly, if we construct the experiment in such a way that we are unable to observe which path the electron or photon takes, we observe the wave pattern, even when firing them one at a time, suggesting that the electrons are passing through both holes and interfering with themselves, while if we construct it such that we can observe which hole the electron travels through, it only takes one path and the pattern we observe is the pattern we would expect with particles. Further, if we look specifically at the distribution of the electrons which passed through each hole, is the same as it is when we close the other hole. Observing the particles seems to impact how they behave (as a particle or a wave). This is an example of Heisenberg's uncertainty principle—that for certain pairs of properties, observing one disturbs the other. In this case, observing which hole the particle passes through disturbs the pattern that we get on the surface. (Feynman et al., 1964).

De Broglie finally reconciled the particle-wave question by proposing that all particles, classical or quantum, have a wave function with wavelength:

$$\lambda = \frac{h}{p}$$

where $h = 6.62607015 * 10^{-34}$ is Planck's constant and p is the particle's momentum. For a classical particle, this wavelength would be unobservable but for a quantum particle observed on the quantum scale, it would be significant (De Broglie, 1929).

With De Broglie's proposal and its subsequent verification came a new view of reality: every object has wave functions that describe the probability of observing its properties in particular states. When we observe a property, we collapse the wave function to a single value or smaller set of values but increase the uncertainty in another property. Given our classical understanding of the world, we would think that each of the properties already has a particular value, and we simply don't know what it is, suggesting that with better technology we could predict what the observed value will be. This would be in violation of the uncertainty principle, but it also has been shown to be incorrect because it would violate Bell's inequality (Aspect, Dalibard, and Roger, 1982) (Fry and Thompson, 1976). This means that the property actually is in multiple states at once, called a superposition of states.

Richard Feynman described the behavior of electrons as being like particles which follow a wave function (Feynman, Leighton, and Sands, 1964). This wave function is a superposition of locations and their intensities which collapses to a single location when we observe the electron. The intensities indicate the probability of observing the electron in that location. This explains the particle-like nature of an electron in the double-slit experiment when we observe it—it really is shifting from being in multiple places at once to being in a single place. This concept of a superposition also forms the foundation for quantum computing.

Representing Qubits

In the context of quantum computing, a particle is often referred to as a qubit–the quantum equivalent of a bit. A qubit's state can be represented as a vector of probability amplitudes:

$$a = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

where a_0^2 is the probability amplitude of observing the qubit to be in state 0 and a_1^2 is the probability of observing it to be in state 1. The normalization property states that $a_0^2 + a_1^2 = 1$ because the sum of the probabilities has to be 1. The state also has a relative phase term measuring a difference of phase between the two components of the vector. This can be thought of as being akin to the orientation of the qubit (Feynman et al., 1964). Using Euler's identity, the qubit can be represented by:

$$a = a_0\cos(\theta) + e^{i\phi}a_1\sin(\theta) = \begin{bmatrix} a_0\cos(\theta) \\ e^{i\phi}a_1\sin(\theta) \end{bmatrix}$$

As one might expect, we can also use different bases to measure a qubit. As a two-dimensional vector space, a basis can be defined by any two linearly independent vectors. A qubit that is in a definite state:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} or \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

in one basis will be in a superposition of states in any other basis. Three commonly used bases are the x, y, and z bases, listed below with their basis vectors, expressed in the z-basis ("IBM Quantum," 2021):

$$z\text{: } \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} x\text{:} \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} y\text{:} \frac{1}{\sqrt{2}}\begin{bmatrix} i \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} -i \\ 1 \end{bmatrix}$$

Another commonly used notation is Dirac's bra-ket notation. It gives us a convenient notation for expressing the state of a qubit and its projection onto another state. First, the "ket" notation $|a\rangle = a_0|0\rangle + a_1|1\rangle$ gives the probability amplitudes of the basis vectors for a basis. The "bra" notation $\langle b|$is used in conjunction with the ket notation to represent the projection of a onto b: $\langle b|a\rangle$. This is equivalent to an inner (dot) product $\langle b|a\rangle = \vec{a}\dot{\vec{b}} = a_0b_0 + a_1b_1$ and gives

the probability of finding a to be in state b when observed in b's basis. Clearly, if $b = a$, $\langle a|a\rangle = a_0^2 + a_1^2 = 1$ by the normalization property and if a is orthogonal to b, $\langle b|a\rangle = b \cdot a = 0$. (Zubairy, 2020)

Multiple Qubits and Entanglement

Thus far we have dealt only with single qubits. When we consider multiple qubits, the situation gets more complicated. A pair of qubits have four discrete states that they can be in: 00, 01, 10, 11, and of course can be in a superposition of these. The state is thus defined by the four probability amplitudes, often represented by a 4x1 vector as shown below:

$$a = \begin{bmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{bmatrix}$$

Similarly, a three-qubit system would be representd by:

$$a = \begin{bmatrix} p_{000} \\ p_{001} \\ p_{010} \\ p_{011} \\ p_{100} \\ p_{101} \\ p_{110} \\ p_{111} \end{bmatrix}$$

and so, on so that an n qubit state requires a 2^n x 1 matrix to represent it. We will stick most often to the two-qubit case because this is easier to model.

Multi-qubit states can be classified as either separable or entangled. A state is considered separable if it can be expressed as the product of two distinct single-qubit states. For example:

$$a_{12} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}$$

can be expressed as the product of:

$$a_1 = \begin{bmatrix}1\\0\end{bmatrix} * \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}.$$

An entangled state, meanwhile, cannot be expressed as the product of two separable states. The state:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}$$

is an example of such a state. The states of the two qubits are inextricably linked. If qubit a_1 is found to be a 1, we know that qubit a_2 will be a 0, while if qubit a_1 is found to be a 0, qubit a_2 will be a 1, As discussed earlier, each individual qubit is actually in both of these states and there is nothing inherent to the qubit that dictates in which state it will be found. Thus, the two particles are actually linked in some way that we do not understand (Zubairy 2020).

Quantum Computing

While quantum mechanics is counter-intuitive and can be difficult to grasp, the ability of a particle to be in multiple states at once with observed values following predictable probabilities can be harnessed to allow faster computation in specific cases. In this section, we will cover a few of the gates that are used to build a quantum computer and how they can be used to achieve computational advantage.

Quantum Gates

Just as the quantum equivalent of a bit is a qubit, so too logical gates have a quantum equivalent that enables us to harness the power of superposition and entanglement for computing purposes. The simplest gates are single qubit gates that operate about a basis. These gates can be represented by a 2x2 matrix which can be multiplied by the qubit's state vector to find the resulting state of the qubit. For example, to rotate about the x, y, or z axes in the sphere defined above we use:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Applying these we find:

$$Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix}$$

$$X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} * \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix}.$$

Notably, the basis vectors given earlier for each of these bases are the eigenvectors of the corresponding gate, meaning that they are uneffected by them. This makes sense because a vector falling along an axis would not be affected by a rotation about that axis ("IBM Quantum," 2021). To create a superposition, we can use the Hadamard gate:

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Where:

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

Each of these are specific cases of the general gate:

$$U(\theta, \phi, \lambda) = \begin{bmatrix} cos(\frac{\theta}{2}) & -e^{i\lambda} sin(\frac{\theta}{2}) \\ e^{i\phi} sin(\frac{\theta}{2}) & e^{i(\phi+\lambda)} cos(\frac{\theta}{2}) \end{bmatrix}$$

("IBM Quantum," 2021). We also can create gates for multiple qubits. As expected, these are 2^nx2^n gates. For example, the CNOT gate:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

performs an X gate on the second qubit if the first is a 1 and does nothing otherwise ("IBM Quantum," 2021). Since this creates a dependency of the second qubit upon the value of the first, if the first is in a superposition, it creates an entanglement between them. Again, it is important to remember that, when a particle is in a superposition, it is actually in both states, so that the second particle will also be in both states until one or the other is observed.

Advantages of Quantum Computing

A quantum computer provides the potential for great computational advantage over a classical machine in specific problems. The most obvious of these is simulating a quantum system. An entangled quantum state with n qubits will require 2^n complex numbers to track the states of the qubits. A quantum computer could, of course, model this system using n qubits. This suggests that a quantum computer could provide exponential speedups over classical computers, at least in certain problems, though such quantum supremacy has yet to be proven

(National Academies of Sciences et al., 2019) (Harrow and Montanaro 2018). This raises the question of whether this exponential speedup can be applied more generally? Using the entanglement of n qubits, we are able to store 2^n complex numbers and operate on all of them at once with an n-bit quantum gate (National Academies of Sciences et al., 2019). At first glance, this would seem to provide an exponential speedup, allowing for computation of NP or even exp problems in polynomial time. The class of problems that can be solved by a quantum computer in polynomial time with bounded error is referred to as BQP. This would thus be represented as $NP \subseteq BQP$ and $exp \subseteq BQP$. In 1997, however, Bennet et al showed that there is not an exponential speedup using a random oracle (i.e., when we don't consider the nature of the problem that we are trying to solve) (Bennett et al., 1997). This means that we do not get a simple reduction of NP to polynomial time. It is still possible that $NP \subseteq BQP$, but this would require considering the specific nature of each problem in NP to come up with an algorithm to solve it in polynomial time with bounded error on a quantum computer. Despite this discouraging result, it is still possible to achieve an exponential speedup using a quantum computer to solve specific problems with a specially crafted algorithm, for example in the simulation of the quantum system above, or of integer factorization (Shor 1999)

Conclusion

The particle/wave duality of light led to an understanding of the wave function-based nature of reality. Particles exist in a superposition of states and can be entangled with one another to create more complex systems. By using quantum gates to manipulate these particles in specific ways, we can create algorithms that can be run on a quantum computer. While quantum computers will not provide an across the board speedup, when we tailor our algorithms

specifically to the nature of the problem, it is possible to see an exponential speedup for certain problems by harnessing superposition and entanglement.

References

Aspect, Alain, Jean Dalibard, and Gérard Roger. 1982. Experimental test of Bell's inequalities using time—varying analyzers. *Physical Review Letters, 49*(25): 1804–7. https://doi.org/10.1103/PhysRevLett.49.1804.

Bell, John. 1964. ON THE EINSTEIN PODOLSKY ROSEN PARADOX. *Physics, 1*(3). https://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf.

Bennett, Charles H., Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. (1997). Strengths and weaknesses of quantum computing. *SIAM Journal on Computing, 26*(5): 14. https://doi.org/http://dx.doi.org/10.1137/S0097539796300933.

De Broglie, Louis. 1929. "The Wave Nature of the Electron." *Nobel Lecture*, December.

Feynman, Richard, Robert Leighton, and Matthew Sands. (1964). "Feynman Lectures on Physics Vol 3 Feynman, Leighton and Sands (1964)," December. https://www.academia.edu/30257311/Feynman_Lectures_on_Physics_Vol_3_Feynman_Leighton_and_Sands_1964_.

Fry, Edward S., and Randall C. Thompson. (1976). Experimental test of local hidden-variable theories." *Physical Review Letters* 37(8): 465–68. https://doi.org/10.1103/PhysRevLett.37.465.

Harrow, Aram W., and Ashley Montanaro. 2018. "Quantum Computational Supremacy." September. https://doi.org/10.1038/nature23458.

"IBM Quantum." (2021). https://quantum-computing.ibm.com/.

National Academies of Sciences, Engineering, and Medicine, Division on Engineering and Physical Sciences, Intelligence Community Studies Board, Computer Science and Telecommunications Board, Committee on Technical Assessment of the Feasibility and

Implications of Quantum Computing, Mark Horowitz, and Emily Grumbling. (2019). *Quantum Computing: Progress and Prospects*. Washington, DC: National Academies Press. http://ebookcentral.proquest.com/lib/liberty/detail.action?docID=5742474.

Shor, Peter W. 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, *41*(2): 303–32. http://www.jstor.org/stable/2653075.

Zubairy, M. Suhail. 2020. *Quantum mechanics for beginners: With applications to quantum communication and quantum computing*. Oxford University Press. https://doi.org/10.1093/oso/9780198854227.001.0001.