Quantum Entanglement and Qubit Interactions: The Key to Quantum Supremacy

Han Zhang

Muir College, University of California San Diego, CA, USA

Haz043@ucsd.edu

Abstract. Quantum computing operates in a fundamentally different way from classical computing by harnessing the principles of quantum mechanics to process information. Quantum supremacy is achieved when a quantum computer can solve problems that are beyond the capabilities of classical systems, including the human brain, showcasing its superior processing power. To attain quantum supremacy, quantum entanglement and qubit interactions play a pivotal role. Quantum entanglement occurs when qubits are interconnected in a manner where the state of one qubit directly influences the state of others, enabling the quantum computer to perform multiple operations simultaneously. Moreover, effective interaction between qubits is essential for the performance of complex calculations in quantum systems, highlighting the significance of coherence and error correction. Understanding the importance of coherence in preventing and rectifying errors in quantum computations is crucial. This paper aims to explore the critical aspects of quantum entanglement and qubit interactions, which are foundational to the operation of quantum computers. By delving into these key concepts, the paper aims to elucidate their significant roles in achieving quantum supremacy. The discussion will center on how quantum entanglement, which allows enhanced computational parallelism through qubit interconnection, and efficient qubit interactions vital for complex computations, contribute to surpassing the capabilities of classical computers. Comprehending these principles is crucial for advancing quantum computing technology and overcoming the challenges to unleash its full potential.

Keywords: Quantum Computing, Quantum Supremacy, Quantum Entanglement.

1. Introduction

Quantum information science is dedicated to comprehending and achieving quantum supremacy, the phenomenon where quantum computers consistently outpace classical ones. This idea, in turn, is based on the premise that it is impossible, or at least highly inefficient for classical systems to simulate quantum systems. In the past couple of decades, there has been a surge of interest in solving the "quantum control problem." Efforts to develop sufficiently large, controllable, macroscopic systems that exhibit purely quantum behaviours have intensified. But the logic behind these investigations follows directly from their assumption that achieving quantum supremacy is a worthwhile goal. Indeed, it could push the frontiers of physics into realms that have yet to explore. This paper investigates the essential features of quantum entanglement and qubit interactions, which form the basis of quantum computing. The first topic this paper cover is quantum entanglement. When qubits are connected in such a way that

the state of one qubit directly affects the state of the others, comes the entanglement. That's a pretty good beginning to understanding the principles of quantum mechanics [1,2].

From there, this paper go into the principles of superposition, which with entanglement and interaction, allows a quantum computer to perform operations in parallel and solve problems—all at an incredible speed. Systems of quantum computing require a delicate balance [1,2]. The interactions between qubits must be controlled as precisely as those in any well-coordinated orchestra. Each qubit must "do its part" without error, and all must "stay coherent" long enough to perform an undesirable calculation—one that even the fastest classical computers can find impractical. And yet this precision is necessary not just for meaningful calculations, but also for the performance of any calculations at all. Next, it will examine what qubit interactions mean for the "hardness" of calculations performed in a quantum system. After that, the paper will discuss various types of qubits, some of which are more promising than others for producing a precision computing system.

This paper will also underscore the need for clear signalling and "error-free" messaging for quantum supremacy to be achieved. For any two qubits to maintain their "next door neighbour" relationship, they must be coherent; that is, they must interact in a controlled fashion over a range of distances and over an adequate number of time steps, or computational "depth." This is not an easy requirement to meet and is arguably the most significant barrier to building large-scale quantum computers [3].

2. Fundamentals of Quantum Entanglement

The study of quantum non-locality began in 1935 with some early experiments and theoretical developments. A significant milestone was the formulation of the Einstein-Podolsky-Rosen (EPR) paradox. In their 1935 paper, Einstein, Podolsky, and Rosen used entanglement to question the completeness of quantum mechanics. They thought up a situation in which the measurement of an entangled particle's position or momentum would instantaneously determine the position or momentum of another entangled particle, no matter how far apart the two had been separated. This led to their argument against "spooky action at a distance" and their conclusion that quantum mechanics must be incomplete. Since then, the EPR paradox has been a huge driver of the study of entangled systems [4,5].

The local hidden variable concept subsequently took a hit from an unexpected quarter, John Bell, in the 1960s, when he shone a light of insight on it and laid it open for inspection. Bell's theorem expressed in simple but incisive terms what had long been suspected: if local hidden variables exist, then quantum mechanics is wrong; it does not correctly describe the world. Indeed, Bell and his followers in the 1970s and '80s conducted a most kind of mock trial. They pitted local hidden variables against quantum mechanics itself, a courtroom drama that invariably had the same outcome: the jury of experimenters in the '70s and '80s declared for quantum mechanics [4,6].

Entangled states are defined in such a way that measuring the position of one particle gives you the position of the other particle with pinpoint accuracy. Measuring the momentum of one particle gives you the momentum of the other particle with close to 100% certainty. Quantum non-locality is intimately connected to entanglement and is one of the key principles used to illustrate the "weirdness" of quantum behavior. Yet, at the same time, quantum non-locality is closely related to the concept of superposition, which is probably the most fundamental principle of quantum mechanics. Indeed, a quantum system exists in a kind of "schizophrenic" state, in which it simultaneously occupies several states or configurations, until the system is measured. And this principle is crucial for understanding the behavior of entangled particles [4,5].

The superposition collapses when the property of one particle is measured, defining the other particle's property instantaneously, no matter how far apart they are. This is not an analogy but a fact: when particles have correlated properties in a state of superposition, they behave just like waves in a fountain—exactly like waves in a fountain—when you measure one wave to result in a certain height. Your measurement instantaneously sets the water in a certain fountain state, defining changes in height all across the fountain from your "this wave, not that wave" measurement. The elegant equations of quantum mechanics can tell you not only that certain states are superposed but also the specific "height" your wavefunction is likely to take when you make that measurement [4,5].

An electron might have two distinct velocities or exist in two separate locations at the same time. This is what quantum mechanics tells us, and it is what quantum correlations are all about—correlations that are stronger than the strongest classical correlations and that can be produced only if it's involved within the entangled states. In classical mechanics, if there are two correlated particles, it can be explained their correlation by saying that they have a shared history or direct interaction. But in quantum mechanics, especially in a world of entangled states, it is no longer valid to persist with the idea that superposition states are either "real" or "not real." Correlations between particles in an entangled state cannot be understood from our classical intuition of the physical world. The particles do not possess definite states until the state is measured. When the state of one of the entangled particles is measured, the state of the other particle—regardless of the distance between the two—is instantaneously determined. These experiments have shown us that "spooky action at a distance" is a real phenomenon. How this can happen is one of the great unsolved mysteries of physics. For practical applications, understanding this phenomenon is crucial to the development of new technologies based on quantum mechanics. Matthew Hayward discusses in his paper "Quantum Computing and Shor's Algorithm" the propitious part that entanglement plays in quantum computing. He elucidates that entanglement is a crucial ingredient in the resource-based recipe for not just various quantum algorithms but also error correction methods. These are quantum computing's "baking a cake" moments, and they're well beyond the fundamentals of quantum physics. Yet even in the early 1990s, Hayward notes, it was evident that quantum computers could do certain things much better than classical computers. Thus, the potential of quantum computing became clear [6,7].

In 1994, a researcher named Peter Shor, who worked at Bell Labs, brought forth an astounding development. He introduced a polynomial-time algorithm for factoring large numbers. The key element here is "polynomial-time." A classical computer would take what may as well be an eternity to factor the numbers Shor worked with. Conversely, a quantum computer can use "superposition," the basic principle of quantum mechanics that allows a particle (an electron, say) to exist in multiple states simultaneously, to more efficiently arrive at the answer of "undoubtedly this, or surely that." Once a quantity can be factored, the computer employing Shor's algorithm can use the factor or factors to reconstruct the original problem's solution. number...n (with a representation of $\log n$ bits) operates in $O\left(e^{c(\log n)^{\frac{1}{3}}\log\log n^{\frac{2}{3}}}\right)$, which is exponential time. In contrast, Shor's algorithm runs in $O((\log n)^2 \log\log n)$ on a quantum computer and requires an additional $O(\log n)$ steps of post-processing on a classical computer. In summary, the algorithm operates in polynomial time, which is a significant advancement. Shor's algorithm has thus renewed and reinvigorated interest in quantum computing, considering that it could upend not only encryption but also a whole range of computational problems that require a similar sort of number-crunching prowess (they're mostly about multiplying and dividing large numbers) and that working in classical computing amounts to using a finite number of bits of memory and a finite number of steps to do that work. ... Two numbers are coprime if their greatest common divisor amounts to 1. A classical computer can calculate many such values only in a snail's pace because it cannot do them in parallel the way a quantum computer can, using its conservation of a "somewhat limitless" set of states to "achieve" the same series of operations in fewer steps [8].

Since F(a) is periodic, it has a period r, and x^0 mod n = 1 (because x^0=1), and thus x^r mod n = 1, x^{2r} mod n = 1, and so forth. Given this periodicity and through algebraic manipulation:

$$x^r \equiv 1 \bmod \text{n}, \tag{1}$$

$$(x^{r/2})^2 = x^r \equiv 1 \bmod \text{n} \tag{2}$$

If r is an even number:

$$(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \bmod \text{n}. \tag{3}$$

The product $(x^{r/2} - 1)(x^{r/2} + 1)$ is an integer multiple of n. So long $x^{r/2} \neq 1$, at least one of : $(x^{r/2} - 1)$ or $(x^{r/2} + 1)$ shares a nontrivial factor with n. Shor's algorithm does this cleverly, using a quantum memory register that has two parts. It first places a superposition of integers 0 to q-1 in the left

side of the register, where q is a power of 2 such that $n^2 \leq q < 2n^2$ (this is necessary so that it is working in an appropriate finite field). The 0s and 1s in the left register correspond to the a's in the function x^a mod n. The right side of the register is set up to hold the result of whatever function is calculated from the a's in the left side of the register [8].

The algorithm proceeds to calculate x^a mod n and keep that in the second part of the register. The number n is represented by a log n bit string. x^a mod n has to be calculated an exponentially large number of times relative to the length of the input but polynomial in n. After that, the second register and k collapses out of it into a specific value can be measured. This measurement also projects the first register into a state consistent with congruences. After measurement, the second register holds k, and the first one has a superposition of base states that evaluate in such a way that they give k when taken mod n [8].

Thanks to the periodic nature of x^a mod n, the first part of the quantum register holds probability amplitudes for the numbers c, c+r, c+2r, and so on, where c is the smallest integer such that x^c mod n = k. The next step is to apply the Fourier transform to the first part of the register. The Fourier transform amplifies the probability amplitudes for integer multiples of q/r, where q is the size of the first part of the register. When the first part of the register is measured after the Fourier transform, it will likely yield a multiple of the inverse period. A classical computer then decodes the instruction held in the quantum memory to yield the period, and from that, the factors of n [8].

3. Qubit Interactions and Their importances

In quantum computation, qubit interaction is fundamental to information processing. This is best understood by comparing qubit interaction to the two basic ways human beings can communicate. Direct interaction is like two people talking face-to-face, influencing one another directly through means like the electric or magnetic fields one person generates around himself or herself. Indirect interaction is like two people talking with a friend in between. The friend can tell either of the other two what the other has said without any direct influence from one of the talkers to the other. In indirect interaction, two qubits influence one another without direct physical contact. And these are the two basic ways qubits can interact in what named "quantum circuits.[9-11]"

Superconducting qubits have long been viewed as the leading platform for large-scale quantum computing due to their favorable coherence properties, ease of fabrication, and potential for integration within a highly scalable architecture. They are at heart Josephson junctions, which are non-linear inductors, and rely on the quantization of magnetic flux in superconducting loops. Despite these advantages, the primary challenge to building a fault-tolerant quantum computer with them has unfolded as their operational speed—what physicists refer to as the reset time—has not kept pace with the ability to implement error correction, a strictly required feature of any large-scale quantum processor. Individual ions that are confined and manipulated by electromagnetic fields serve as qubits, the basic units of information in a quantum computer. In terms of operations and coherence—that is, the ability of the system to maintain a superposition of quantum states—trapped ions come very close to perfection, and Häffner's group is working to make them the most robust, error-correctable system of qubits. This promise has led to a sharp increase in the number of research groups working with trapped ions. According to Häffner's journal, "Quantum Computing with Trapped Ions," about six groups were doing this work in 2000, and over 25 by 2008 [9-11].

In 1995, Cirac and Zoller suggested using groups of ions as the basis of a quantum computer. They introduced what one might call the "user manual" for establishing a quantum logic gate using an elementary operation similar to one performed in an ordinary logic gate: a conditional phase shift. This is like saying "if…then…" in a digital operation. Their ideas were notional, involving the motion of ions in potential energy wells created by carefully managed electromagnetic fields. But these ideas were put to work in what is essentially an industrial-strength laboratory—one belonging to David Wineland and his group at the National Institute of Standards and Technology. They were able to demonstrate a couple of elementary two-qubit operations and entangle up to four ions. The development of ion trap technologies has been greatly assisted by targeted research projects in Europe. These microfabricated

devices are becoming more and more sophisticated and could soon surpass the state-of-the-art superconducting qubit technologies. Meanwhile, quantum dots—tiny semiconductor particles that confine electrons—also hold great promise. The early 1980s saw the advent of a new form of lithography that allowed scientists to create structures that confine electrons in very small spaces. These structures are so small that they exhibit "quantum" behaviour. Quantum dots are tiny in size but are robust enough in their electronic behaviour to serve as the basic building blocks of several proposed quantum computing architectures [9-11].

Texas Instruments created the first quantum dots, 250 nm in size, using lithography. AT&T Bell Labs and Bell Communications Research later produced even smaller dots, 30-45 nm in diameter. Because the confined electrons in these dots behave similarly to those in atoms, scientists refer to them as "artificial atoms." In quantum dots, scientists have precise control over shape, size, and number of confined electrons, making these nanostructures highly valuable for studying complicated physical phenomena and for observing quantum effects in crystals. Researchers are particularly interested in the optical and electrical properties of quantum dots. Fundamental research and technological advances stand to benefit greatly from the use of quantum dots. Reed and his colleagues developed the original method for producing them. This technique involves using a structure whose essential component is a two-dimensional electron gas. The process starts with a sample that has one or more quantum wells. A polymer mask covers the sample's surface, followed by partial exposure to an electron or ion beam; the beam does not use light because high resolution is required. The exposed areas of the polymer do not change much; they remain mostly unchanged except for the "magic" of going from the mask to the sample. These areas receive a metal deposition. When the sample is done being worked on, the remaining mask is removed, and voilà! The sample has only the metal layer in certain areas, on the surface, and it is clean [9-11].

Areas unprotected by the metal mask are removed using chemical etching, which undercuts the last quantum well and the buffer layer. The pillars left behind are ten to 100 nanometres in diameter, and contain the fragments of a quantum well. A base of chromium-doped GaAs beneath the last quantum well feeds in carriers. The carriers flow into the twenty GaAs quantum wells above. The etching creates a structure in which the flow of carriers is well controlled, with a remaining gold mask acting as an electrode. By applying a voltage between the mask and the base, one can control the number of carriers in the structure.

Finally, the use of photons as qubits in photonics makes them very effective for quantum communication. This is because photons exhibit very little interaction with their environment; in other words, they are very "quiet" in that the states they occupy do not change much when they are subjected to various environmental conditions. For this reason, photons are able to maintain their "quantum-ness" for a long time and travel long distances with minimal decoherence and, hence, no significant drop in signal strength. This characteristic makes using photons and fiber optics very attractive for constructing quantum networks, because the use of signals in the form of light—that is, in the form of photons—will make these signals very secure and very hard to eavesdrop on.

In addition, photonic networks can be readily joined with current fiber-optic infrastructures, enabling the actual deployment of quantum networks. Optical technologies that people have in hand, and know well how to use, can efficiently create, manipulate, and detect the quantum carriers of the information—photons. These are "light" networks in a very real sense; the quantum states of the photons are used to encode and process the information. And the properties of the photons themselves allow us to think of new ways to encode that information, which supports the development of protocols for much more complex, and much more powerful, quantum networks.

To conclude, employing photons as qubits in photonic systems builds a strong and scalable basis for quantum communication and offers a potential future for sending information that is both secure and efficient.

4. Achieving Quantum Supremacy

The key moment when a quantum computer surpasses a classical computer in terms of raw capability occurs when quantum phenomena like entanglement, superposition, and interference are used to create speed, capacity, and error-protected pathways that enable solving extremely difficult problems. These problem-solving pathways are evident in what is termed quantum supremacy – the moment when a quantum computer can solve a computationally hard problem in a significantly shorter time and with far fewer steps than a classical computer can. For instance, Google's Sycamore performed a hard computation on a "quantum volume" of 64, with an error rate well within tolerances, in just 200 seconds. When you consider that the same task would take an estimated 10,000 years on a classical supercomputer, you gain a sense of what might be referred to as a quantum moment. Decoherence is one of the primary barriers to achieving quantum supremacy [12,13].

Using the two-slit experiment, scientists can demonstrate interference from the type of systems that might potentially achieve quantum supremacy. However, in attempting to create more complex systems that can perform computations, scientists must be wary of decoherence impeding their efforts. The two-slit experiment also serves as a useful metaphor for considering how much advancement we have made toward true quantum computers. In the two-slit experiment, a beam of particles is detected at a second screen after passing through the first screen with two slits. Probability-wise, using classical physics, one might expect a distribution of particles on the second screen that resembles the two-slit setup itself. The duration for which a quantum sensor can maintain coherence determines its sensitivity. The nature of decoherence – and its impact on the operation of quantum devices – runs parallel to the processes that ordinary sensors go through. When you make something capable of sensing a specific measurement in an ordinary way, you have to work really hard to find and fix the errors that the device makes as it goes through its ordinary life. The same goes for quantum devices, except that you must find and fix errors that occur in a parallel universe before they can affect the practical existence of ordinary objects [12,13].

Quantum devices are currently built in two ways that I know of: in an environment where decoherence doesn't happen, and in a space where we're transitioning between bits. When sensing using a qubit, you're working under an umbrella that keeps noise from the outside world from affecting the qubit. The more you listen using any of the strategies above, the more you cancel out the noise from inside the generally noisy quantum circuit and the outside world.

5. Conclusion

Achieving quantum supremacy is not just a matter of stuffing a bunch of superconducting qubits at a frigid temperature in the right place and hoping for the best. You have to make those qubits interact in a very particular way. Entanglement is key. While a classical computer might perform a calculation in two steps, a quantum computer could do the same task in parallel and in half the time, with the qubits or entangled pairs of qubits, sort of half-seeing each other and swapping states. That's the working theory, anyway. Google's Sycamore processor purportedly achieved this effect with 53 superconducting qubits last year, in a landmark demonstration of quantum supremacy. The processor performed 200 seconds of quantum entangled time on a problem that a classical supercomputer would take 10,000 years to solve.

The challenges of realizing the full potential of quantum computing are the sorts of problems that physics departments live to solve. They are hard, and they require imaginative solutions. Imagine, for instance, trying to ensure that the basic unit of quantum computing, the qubit, remains in the fragile quantum state needed to perform a long series of calculations. If it can hardly be done with the five or six atoms that some groups have used to represent a single qubit, how is it going to be done with the tens or hundreds of qubits needed for any useful computation?

There are many different strategies to create and manipulate qubits, with each offering distinct advantages and facing its own unique challenges. For example, superconducting qubits are known for their rapid operation speed, whereas qubits made from trapped ions afford much greater precision and much longer coherence times. On the other hand, quantum dots have the potential for extremely high integration densities, and qubits based on photons might be the best bet for building a quantum

communicator, given how well they interact with one another and how poorly they interact with their environment.

To conclude, the quest for quantum supremacy is both impressive and intimidating. It has seen some great successes in the lab but has also faced some serious challenges. At the center of this work is the use of a basic element of quantum mechanics—quantum entanglement. The interplay of entanglement and qubit interactions is at the heart of the supremacy argument, and working with these systems is at the heart of the development of a useful quantum computer.

References

[1]   Preskill J 2012 Quantum computing and the entanglement frontier 25th Solvay Conf.

[2]   Harrow A W and Montanaro A 2017 Quantum computational supremacy Nature 549 203

[3]   Achieving Quantum Supremacy 2019 The Current, news.ucsb.edu/2019/019682/achieving-quantum-supremacy (Accessed 1 July 2024)

[4]   Methot A A and Scarani V 2007 An anomaly of non-locality Quantum Information and Computation 7 1–2

[5]   Einstein B, Podolsky N and Rosen N 1935 Can quantum-mechanical description of physical reality be complete? Physical Review 47 777–80

[6]   Bell J S 1964 On the Einstein-Podolsky-Rosen paradox Physics 1 195–200

[7]   What Is Superposition and Why Is It Important? Caltech Science Exchange, scienceexchange. caltech.edu/topics/quantum-science-explained/quantum-superposition (Accessed 2 July 2024)

[8]   Hayward M 2008 Quantum computing and Shor's algorithm Sydney: Macquarie University Mathematics Department 1

[9]   Devoret M H, Wallraff A and Martinis J M 2004 Superconducting qubits: A short review arXiv preprint cond-mat/0411174

[10]   Haffner H, Roos C F and Blatt R 2008 Quantum computing with trapped ions Phys. Rep. 469 155–203

[11]   Jacak L, Hawrylak P and Wojs A 1998 Quantum Dots Springer

[12]   Bacciagaluppi G 2020 The Role of Decoherence in Quantum Mechanics The Stanford Encyclopedia of Philosophy (Fall 2020 Edition) Edward N Zalta (ed.) https://plato.stanford. edu/archives/fall2020/entries/qm-decoherence/

[13]   Salhov A, Cao Q, Cai J, Retzker A, Jelezko F and Genov G 2024 Protecting Quantum Information via Destructive Interference of Correlated Noise Phys. Rev. Lett. 132 223601