Quantum Computing – An Introduction to What it is, Why We Want it, and How We're Trying to Get it

Sara Gamble
US Army Research Office

Introduction

Quantum mechanics emerged as a branch of physics in the early 1900s to explain nature on the scale of atoms and it has since given us advances such as transistors, lasers, and magnetic resonance imaging. The idea to merge quantum mechanics and information theory arose in the 1970s but garnered little attention before a talk by physicist Richard Feynman in 1982 in which he reasoned that computing based on classical logic could not tractably process calculations describing quantum phenomena. Computing based on quantum phenomena configured to simulate other quantum phenomena, however, would not be subject to the same bottlenecks. This application, despite later turning into the field of "quantum simulation," still didn't spark much research activity at the time.

In 1994, however, interest in quantum computing changed dramatically when mathematician Peter Shor developed a "quantum algorithm" which could find the prime factors of large numbers efficiently. Here, "efficiently" means in a time of practical relevance, which is beyond the capability of state-of-the-art classical algorithms. While this may seem simply like an oddity, it's actually impossible to overemphasize the importance of Shor's insight as the security of nearly every electronic transaction we conduct online relies on an RSA cryptosystem which hinges on the intractability of the factoring problem to classical algorithms.

Quantum Computing – What is it?

Quantum and classical computers both try to solve problems, but the way they manipulate data to get answers is fundamentally different. Here, we'll discuss what makes quantum computers unique by introducing two principles of quantum mechanics crucial for their operation, superposition and entanglement.

Superposition is the counterintuitive ability of a quantum object, like an electron, to simultaneously exist in multiple “states.” With an electron, one of these states may be the lowest energy level in an atom while another may be the first excited level. If an electron is prepared in a superposition of these two states it has some probability of being in the lower state and some probability of being in the upper. A measurement will destroy this superposition and only then can we say it is in the lower or upper state.

Understanding superposition allows us to understand the basic component of information in quantum computing, the “qubit.” In classical computing bits are transistors which can be off or on, which correspond to the states 0 and 1. In qubits such as electrons, 0 and 1 simply correspond to states like the lower and upper energy levels discussed above. It is the ability of qubits to be in superpositions with varying probabilities which can be manipulated by quantum operations during computations that distinguishes them from classical bits, which must always be in the 0 or 1 state.

Entanglement is a phenomenon in which quantum entities are created and/or manipulated such that none of them can be described without referencing the others. Individual identities are lost. This concept is exceedingly difficult to conceptualize when one considers how entanglement can persist over long distances. A measurement on one member of an entangled pair will immediately determine measurements on its partner, making it appear as if information can travel faster than the speed of light. This apparent action at a distance was so disturbing that even Einstein dubbed it “spooky.”

The popular press often writes that quantum computers obtain their speed-up by trying every possible answer to a problem in parallel. In reality a quantum computer leverages entanglement between qubits and the probabilities associated with superpositions to carry out a series of operations (a quantum algorithm) such that certain probabilities are enhanced (ie those of the right answers) and certain probabilities are depressed, even to zero, (ie those of the wrong answers). When a measurement is made at the end of a computation, the probability of measuring the correct answer should be maximized. The way quantum computers leverage probabilities and entanglement is what makes them so distinct from classical computers.

Quantum Computing – Why Do We Want It?

The promise of developing a quantum computer sophisticated enough to execute Shor's algorithm for large numbers has been a primary motivator for the field. To develop a broader view of quantum computers, however, it's important to understand that they will likely deliver tremendous speed-ups for only specific types of problems. Researchers are currently working to both understand which problems are suited for quantum speed-ups and develop the algorithms which will demonstrate them. In general, it is believed that quantum computers will help us immensely with problems related to optimization which would impact everything from defense to financial trading.

Separately, there are several additional applications for qubit systems which are not related to computing or simulation and are beyond the scope of this overview. Two of the most prominent are quantum sensing & metrology, which leverage the extreme sensitivity of qubits to the environment to realizing sensing beyond the classical shot noise limit, and quantum networks & communications which may lead to revolutionary ways to share information.

Quantum Computing – How Are We Trying To Get It?

Building quantum computers is incredibly hard. Many candidate qubit systems exist on the scale of single atoms and the physicists, engineers, and materials scientists who are trying to execute quantum operations on these systems constantly deal with two competing requirements. First, one needs to protect qubits from the environment because it can destroy the delicate quantum states needed for computation. The longer a qubit survives in its desired state the longer its “coherence time” is. From this perspective, isolation is prized. Second, however, for algorithm execution qubits need to be entangled, shuffled around physical architectures, and controllable on demand. The better these operations can be carried out the higher their “fidelity” is. Balancing the required isolation and interaction is difficult, but there are a few systems which, after decades of research, are emerging as top candidates for large scale quantum information processing.

Superconducting systems, trapped atomic ions, and semiconductors are some of the leading platforms for building a quantum computer. Each of these has advantages and disadvantages related to coherence, fidelity, and ultimate scalability to large systems. It is clear, however, that all of these platforms will need some type of error correction protocols to be robust enough to carry out meaningful calculations, and how to design and implement these protocols is currently a large area of research in and of itself. For an overview of quantum computing which includes more comprehensive detail regarding experimental implementations, see reference 1.

Up to this point we have essentially used “quantum computing” as a blanket term describing all computations utilizing quantum phenomena. In practicality, there are multiple types of operational frameworks. Logical, gate based, quantum computing is probably the best recognized. In it, qubits are prepared in initial states and then subject to a series of “gate operations,” which in practicality are things like current or laser pulses depending on qubit type. Through these gates the qubits are entangled, put in superpositions, and subject to logic operations like the AND, OR, and NOT gates of traditional computation. Ultimately, the qubits are measured and a result obtained. Another framework is measurement based computation. Here, highly entangled qubits serve as the starting point. Then, instead of performing manipulation operations on qubits, single qubit measurements are performed which leave the targeted single qubit in a definitive state. Based on the result, further measurements are carried out on other qubits and eventually an answer is reached. A third framework is topological computation. Here, qubits and operations are based on quasiparticles and braiding operations of these quasiparticles. While nascent implementations of the components of topological quantum computers have yet to be demonstrated, the approach is attractive because these systems are theoretically protected against noise which destroys the coherence of other qubits. Finally, there are the analog quantum computers or quantum simulators envisioned by Feynman. Quantum simulators can be thought of as special purpose quantum computers which can be programmed to model quantum systems. With this ability they can target problems such as how high temperature superconductors work, or how certain chemicals react, or how to design materials with certain properties.

Conclusions & Outlook

Quantum computers have the potential to revolutionize computation by making certain types of classically intractable problems solvable. While no quantum computer sophisticated enough to carry out calculations a classical computer can't exists today, great progress is underway. A few large companies and small start-ups now have functioning non-error corrected quantum computers composed of several tens of qubits and some of these are even accessible to the public through the cloud such as IBM's Q Experience. Additionally, quantum simulators are making strides in fields varying from molecular energetics to many body physics. As these small systems come online a field focused on near-term applications of quantum computers is starting to burgeon so we can, hopefully, actualize some of the benefits and insights of quantum computation long before the quest for a large scale error corrected quantum computer is complete.

References:

1. T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, & J. L. O'Brien Quantum Computers. *Nature* 464, 45-53 (2010).