Quantum Computing: Theory into a Predicted Reality

Mona Abou Taka

Athabasca University

October 26, 2015

Abstract

This year's celebration of the fiftieth anniversary of Moore's Law has shown the world that modern technology is strong and will continue evolving. The Law states that microchip's processing power will almost double every eighteen months to two years. However, if a fully utilized quantum computing principle using quantum theory in the operation of its processor becomes ready for commercial use in the near future, then the outcome may go beyond the known prediction of Moore's Law, and will create a new era in computing power. Quantum computing is a young discipline interfacing between computer science and quantum physics, and creating an economical sized quantum computer is a work in progress. Furthermore, quantum computing will solve important problems regarding large computations and cryptography that classical computers and supercomputers cannot. So far, small quantum computing systems have demonstrated that it can calculate numeric results and simulate physical systems far beyond what humans can do by hand, but not widely used or tested other than in experimental technical labs in universities. However, over the recent years, D-Wave Systems Inc. in Burnaby, British Columbia, Canada has manufactured two of the five known in the world quantum computers that are the size of a room. Unfortunately, many researchers dedicated to quantum computing theory and application are skeptical of the true utilization of quantum power in these D-Wave computers. With this skepticism, funding by large players dedicated to manufacturing computer systems into the research of the field of quantum computing continues. With that dedication, quantum computing may soon be a reality with a potential of speeding up calculations, database searches, and producing sophisticated encryption codes.

Keywords: quantum computing, quantum computers, quantum physics, classical computers, supercomputers.

Quantum Computing: Theory into a Predicted Reality

In 1982, Richard Feynman, an American theoretical physicist, suggested the possible usage of a quantum system for computations, and the proof in 1985 of the possibility of creating a quantum computer to be more powerful than the classical one is the beginning of realizing the potential of this theory. The memory of a classical computer is composed of 0's and 1's, and can only calculate a set of numbers at the same time. However, the memory of a quantum computer is in a quantum state using quantum bits (qubits) that can be a superposition of different numbers. It means that it is performing computations on different numbers at the same time with various results narrowed down to one single answer. Although that incredible power predicted is a work in progress, classical computers are still a commercial success because of their economical size. Quantum computers built so far are occupying rooms, lack mobility, and lack fully quantum functional processing speeds with proper error detection. In addition, this paper also examines the potential of quantum computers to successfully speed up computations, break current encryption codes and create unbreakable ones, and be a part of a new era of computational power that many are eager to witness.

Background and History

Researchers envisioning quantum computing power was in the latter part of the twentieth century, and predicted to become real in the twenty-first century. However, merging the idea of computer science and quantum theory took a very long time. It all began in the mid 1960's when researchers began thinking of the idea of quantum information science. According to Bacon et al. (2007), there was a quest to build a quantum computer, and there was apparent dominance of quantum theory in nature and the rise of computational success. Yet, only a small group of interested researchers believed in its legitimacy, and "in 1994, that all changed and quantum computing moved into the limelight where Peter Shor, [an American professor of applied mathematics at Massachusetts Institute of Technology,] discovered that quantum computers could efficiently factor and compute discrete logarithm" (Bacon et al, 2007, 56). However, researchers from the years 1995 to 1997 quickly realized that building a quantum computer requires sophisticated quantum error-correcting codes, but it is difficult to clone quantum information. Therefore, a proof of this theory regarding cloning quantum data and producing error-correcting codes "exist and are effective in protecting quantum data from the effects of quantum noise" (Bacon et al, 2007, 57).

Unfortunately, building and showing the world a fully functional quantum computer and every component of it can possibly fail due to noise is still a work in progress. It seems to be the one aspect of the build that researchers are continually facing failure until this day; however, one company called D-Wave Systems in the year 2013 built a functioning 512-qubit computer. They "all operate using quantum rules instead of those defining classical physics. Quantum rules include some very odd principles, including the uncertainty principle and superposition" (Castelluccio, 2014, 60). Moreover, many researchers are not convinced that the generation of actual quantum states with these D-Wave calculations are true. Fortunately, organizations such as Google, NASA, and the past month Intel are "heavily investing in research on running Artificial Intelligence (AI) programs on quantum systems" (Castelluccio, 2014, 60).

Discussion

To comprehend the motives of building a fully functional quantum computer, one has to understand what quantum physics is and its significance to the computing power anticipated to achieve. Quantum physics is a strange phenomenon, and the theory behind it states that in nature, particles and atoms move in many directions at once. Hence, the possibility of using quantum theory and applying it to quantum computing raised the attention of the scientific community. The idea of building a computer processor that can use the laws of quantum physics is an exciting thought, and it will raise computing power to greater heights.

An Overview of Quantum Computing

According to Valiron et al. (2015) study, “quantum computation is a computing paradigm where data is encoded in the state of objects governed by the laws of quantum physics” (2015, 52). The underlying principle behind the computations is that quantum properties represent data and structure, and the mechanism it follows in a devised build performing operations with the quantum data.

To understand how quantum data interacts, the processor has quantum bits or qubits that have the same properties of a classical or conventional bit, but they are in superposition and the values 0 or 1 are in a simultaneous state. However, it cannot be certain the state of the qubit, and the assumption it is in all states at once. According to Kabachinski’s (2013) article, two qubits are in four states at the same time (00, 01, 10, and 11), and the possible number of states is N, then the number of qubits is 2^N. The number reflects the qubit power of a computer, and the higher it is such as a 5-qubit computer then it can represent 2^5 or 200,000 values all at the same time. “This enables the scientific community to be able to apply mathematical operations to all [200,000 values] all at the same time” (Kabachinski, 2013, 504).

Predicted usage. Factoring large numbers is an important feature that these quantum computations can do, and will help guess passwords or encryption hash codes. In other words, it will represent a huge advantage for cryptography and decryptology. The notion of decrypting the most sophisticated encryption codes was inconceivable just a few years ago, and the ability to do that with quantum computing has gotten more attention. In addition, quantum computing has inspired new ideas in physics and computer science such as "efficient simulation of certain quantum systems, better formulation of the blackhole information loss paradox, quantum proofs for exponential lower bounds on classical locally decoded codes, elegant quantum proofs for properties of classical complexity classes …" (Bacon et al., 2007, 59), speeding up computations and running artificial intelligence programs with this quantum power. These predictions help alleviate the continued research and effort that many researchers are dedicating their time to, and justify many large players interest and continued financial support in this research such as NASA, Google and Intel.

Barriers. With such power predicted come a few barriers that are hard to ignore and are hindering the progress of building a fully functional quantum computer. In this paper, there was previous discussion of the problems that error-correcting codes are still facing, and the continued process of trying to completely filter the noise produced during quantum computing. In addition, Paraoanu (2011) states another problem in the architecture of a quantum processor is the smallness of the photon-photon interaction that is responsible for entanglement. Quantum computers need to get more photons entangled or a higher probability of getting entangled pairs in order to utilize their projected power.

Moreover, there are a few other barriers facing quantum computers such as their economical size and mobility. In this era, people are used to holding a supercomputer in their hands to produce amazing results that were unfathomable a decade ago, but quantum computers are not appealing to the masses as of yet, and are not aligned with the interest of the general population. The possibility of advertising quantum computing commercially is presenting their incredible speeds in computations and searching, and that maybe is a great selling point for larger players as well.

Building a quantum computer. It may seem as another engineering task in creating a fully functioning quantum processor, but it depends on the fundamental understanding and application of the physical world. In an article by Van Meter et al. (2013), they discussed the blueprint in building a quantum computer. They explained that developing a quantum computer architecture depends on understanding how classical computer architecture works. Quantum information demands that memory elements be very active and the long wires inside a quantum computer are either non-existent requiring nearest neighbour's cellular automation transfer, or using quantum teleportation and error management techniques during the transfer of one qubit from place to place. "Thus, the principles of classical computer architecture can be applied, but the answers arrived at likely will differ substantially from classical architectures" (Van Mater et al, 2013, 86).

The build will be composed of two stacks at lower and higher levels of the architecture. The lower level's job is determining how individual qubits or qubit interconnect and communicate in order to process data. The second level, or higher level is the microarchitecture for quantum computers where algorithms run and error-correcting codes come into play. As discussed earlier in this paper, it is the biggest obstacle in the performance of a fully functional quantum computer and not been solved yet. In the design and theoretical speculation, the error-correcting codes operate on the physical ability of qubits to combine or entangle and form one or more logical qubits. Moreover, "physical qubits per logical qubit is determined by the quantum operation error rates, the physical memory lifetime, and the accuracy required of the algorithm …" (Van Meter et al, 2013, 89). If enough physical qubits interact to make logical qubits, the error correction will keep the quantum computer error-free during the run time of an algorithm.

Programming for a quantum computer. It has been determined in the past few months of the possibility of programming a fully functioning algorithm that runs on a quantum computer. "A quantum programming language should have a sound, well-defined semantics permitting mathematical specifications of program behavior and program correctness proofs. It is also beneficial for the language to have a strong static type system that can guarantee the absence of most runtime errors …" (Valiron et al., 2015, 57-58).

Moreover, Valiron et al. (2015) stated in the article that the quantum programming language (QPL) probably would run in the beginning on a quantum computer that does not have many qubits, and the language should include tools to estimate resources running in a particular piece of code. The algorithm will have two styles; the first style will determine if the algorithm naturally describes a mathematical formula, and the second style will determine if the algorithm has a sequence of low-level gates. These two styles will be guidelines in the design of the quantum programming language. Therefore, the programs written in a quantum programming language should be close as possible to high-level descriptions with an output suitable for a quantum coprocessor model.

Differences between classical computers and quantum computers. The biggest challenge facing quantum computers and classical computers is the success of classical computing systems. In order to be commercially viable, quantum computers must surpass the wildly successful classical computer in what they can already do, and minimize their physical size in order for the general population to use it in their everyday lives. Classical computers are using bits 0 and 1 and so are quantum computers, but quantum computers "can do an arbitrary reversible classical computation on all numbers simultaneously" (Elteja, 2013, 209). If a quantum computer can compute all these numbers simultaneously to get one single answer at predicted incredible speeds, it makes it much more powerful than a classical one. Moreover, according to Moore's Law, the number of transistors of a microprocessors will continue to double every eighteen months and quantum computer's qubits will also double in that period, but one qubit is already enough to double the speed according to the projected speed increase of a classical computer. Yet, quantum computers will have several qubits running and increasing its power to more than just doubling it. With that power, quantum computers will define a new era in computing power that classical computers and even supercomputers can never achieve.

There have been many questions asked over the past twenty-five years of how can theories like this turn to a reality. If properly solved error-correcting codes ready for commercial use, continuation of consistent funding into the research, the presence of intelligent questions and proper choices defining problems to attack, and utter impatience to solve problems and deploy systems such as this is the ultimate goal, then it will lead to the success in solving quantum computer's problem.

Conclusion

Over the recent years, classical computers and supercomputers dominated the general population's life and perspective of what the usage of a computer and the information it produces. The faster the outcome it produces, the better the chances that it will become a primary tool. Many are optimistic that a new era of computing that is beyond the prediction of Moore's Law is on the horizon. That projection includes the true utilization of quantum computing to produce unfathomable results at incredible speeds. Quantum computing based on classical physics' quantum definition can be successful if the true nature of quantum physics applied when building these powerful systems. Computer bits known to be a part of it, but act differently and they are in different states at the same time producing one single result.

However, many skeptics are still present and will downgrade the current companies invested in the build of quantum computers, but it is best to ask those intelligently finding a solution to the problem at hand, when will quantum computers become readily available for commercial use?

References

Bacon, D., & Leung, D. (2007). Toward a World of Quantum Computers. *Communications Of The ACM*, *50*(9), 55-59. doi:10.1145/1284621.1284648

Castelluccio, M. (2014). Quantum Computers. *Strategic Finance*, *96*(3), 59-60.

Elteja, S. M. (2013). The Approach of Classical Computer to Quantum Computer. *Journal Of Science & Arts*, *13*(2), 209-212.

Glick, B. (2015). Moore's Law still a benchmark for progress. *Computer Weekly*, 15.

Kabachinski, J. (2013). The promise of quantum computing. *Biomedical Instrumentation & Technology*, *47*(6), 504-506 3p. doi:10.2345/0899-8205-47.6.504

Pandhare, A. V., Tanzeem, S., & Gupta, S. (2012). Quantum Computing: A Future Trends in Computing. *International Journal Of Advanced Research In Computer Science*, *3*(3), 697.

Paraoanu, G. (2011). Quantum Computing: Theoretical versus Practical Possibility. *Physics In Perspective*, *13*(3), 359-372. doi:10.1007/s00016-011-0057-6

Valiron, B., Ross, N. J., Selinger, P., Alexander, D. S., & Smith, J. M. (2015). Programming the Quantum Future. (cover story). *Communications Of The ACM*, *58*(8), 52-61. doi:10.1145/2699415

Van Meter, R., & Horsman, C. (2013). A Blueprint for Building a Quantum Computer. *Communications Of The ACM*, *56*(10), 84-93. doi:10.1145/2494568

Van Meter, R. (2014). Quantum Computing's Classical Problem, Classical Computing's Quantum Problem. *Foundations Of Physics*, *44*(8), 819-828. doi:10.1007/s10701-014-9807-z