

Vladyslav Kruk

IT 103, section 006

February 28, 2011

Quantum Computers

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on <http://academicintegrity.gmu.edu/honorcode/> . I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on <http://universitypolicy.gmu.edu/1301gen.html> web site."

4/7/2011

X Vladyslav Kruk

Introduction

In this essay, I am going to write about quantum computers, their development, benefits they can bring to the society as well as a number of ethical, legal, and social issues related to them. This topic is interesting because quantum computers and computing is a new development in the field of information technology that looks very promising to the scientists. As the name implies, this development brings together two different disciplines: physics and computing with “potential [...to create] extremely small computer processors or extremely powerful processors of current size” (Steinberg, 2008, p. 107). Recently, scientists made a number of important discoveries that moved them closer to their goal, which is to create an efficient quantum computer. Although a few decades ago it seemed like an impossible dream, now, with the current developments, this goal is closer than we might think.

Background

There are a few important events in the history of quantum computer I am going to focus on. According to Schiller (2009), Feynman, a physicist, in 1981 “proposed the basic model for a quantum computer that would be capable of [‘simulating an evolution of a quantum system’],” initiating the research and development of a quantum computer (p. 28). A few years later, in 1985 Deutsch “described the first universal quantum computer” (Schiller, 2009, p. 28). According to an article about timeline of quantum computing, in 1994, Peter Shor discovered an algorithm that “allowed a quantum computer to factor large integers quickly” and solve factoring

and log problems (Wikipedia, 2011). To correct the quantum errors, Shor and Steane in 1995 proposed a device called “decoherence-free subspaces,” (Wikipedia, 2011) which addressed the important security concerns of this developing technology. In the 1990s, the scientists and government became increasingly interested in the research and development of quantum computers (Shiller, 2009, p. 30). According to Shiller (2009), in 1998 the first working 2 and 3 qubit NMR (nuclear magnetic resonance) quantum computers were created by scientists from Oxford, Stanford Universities and MIT (p. 30-31). In the subsequent years, the groups of scientists spent time perfecting the existing NMR computers and making them more efficient by adding additional qubits, creating a qubyte (8 qubits), and studying the properties of electrons, photons and other subatomic particles and how they can be used in the further development of quantum computers (Wikipedia, 2011). As we see, the developments in quantum computing and computers went a great length from 1980s (first proposals) to 2000s (first NMR quantum computers). Although scientists created the first NMR quantum computers, these cannot be used the same way we use silicon-based computers and it will take a lot of research and experiments to create a real quantum computer that can be used in the future (Bronsor and Strickland, 2011).

Potential benefits

According to AT&T Labs official website (2011), the interconnection between quantum physics and computing did for computing “what the assembly line did for manufacturing,” showing that the computation efficiency has increased dramatically, and this achievement helped the overall progress in both fields. The main reason why quantum computers are more efficient than ordinary computers is that a bit represents only one possibility (0 or 1) while a qubit “can represent an array of possibilities that can be calculated simultaneously, while taking probabilities into account” (AT&T Labs, 2011). To expand on this, according to Quantiki article

about quantum computation (2010), the qubit can actually be in both states (1 and 0); therefore, when calculations are done, “a system with n qubits can perform 2^n calculations at once,” which exponentially increases the number of calculations done. According to Gary Taubes ScienceWatch interview with Ignacio Cirac (2009), one of the most important researchers in the field, the theories developed in the field of quantum computing “can be applied in other fields of physics, specifically in condensed matter physics,” showing not so obvious benefits of developing quantum computers. According to Bronsor and Strickland (2011), the quantum computers can be used to encrypt and decode secret information, search for large databases quickly and study quantum mechanics. Shiller (2009) also includes quantum communication systems that “allow a sender and receiver to agree on a code without ever meeting in person” and creation of artificial intelligence using quantum computers as possible applications of quantum computers (p. 22).

Disadvantages and Security

The main disadvantage or problem in creating quantum computer lies in removing quantum decoherence (Wikipedia, 2011). Decoherence is a security issue when there are too many interacting qubits so that “quantum information will spread outside the quantum computer and be lost into the environment, thus spoiling the computation” (Quantiki, 2010). One of the ways to battle quantum decoherence is introduction of decoherence-free subspaces, which help to “prevent destructive environmental interactions by isolating quantum information” (Wikipedia, 2010). One of the things related to the security of the quantum computer is a field of quantum cryptography, which helps to “secure message transmission” and achieves a higher level of security than “purely classical schemes” (Quantiki, 2006). Although there are some

disadvantages to quantum computers, the scientists work hard to remove them, which can lead to a better security of the information stored on these computers.

A way to move forward

According to the ScienceWatch interview (2009) with Ignacio Cirac, one of the properties of qubits that does not exist in classical mechanics is entanglement or correlation between two or more qubits that are related to each other (the qubit can have values 0 and 1 at the same time in the same place). Understanding entanglement can help scientist create a potential quantum computer in the future (ScienceDaily, 2011). To expand on this, I have found an article that discusses recent scientific developments in quantum entanglement. According to JCNNewswire (2011), about a month ago scientists in the Kohei Itoh Laboratory have made a dramatic breakthrough in their research in quantum entanglement. They have “successfully generated and detected quantum entanglement between electron spin and nuclear spin in phosphorus impurities added to silicon,” which means that this is the “first successful generation and detection of entanglement, which is essential for quantum computing” (JCNNewswire, 2011).

When will quantum computers be available to the general public?

Although no one knows the exact date, scientists are still thinking about the impact this discovery will have on the society and how it will transform our lives. For example, according to PBS article “Will Computers Take A Quantum Leap?” (2003), this discovery can be used in such diverse fields as medicine (to create new drugs), global positioning systems, and electronics as well as communication. Innovations in all of these fields can directly affect peoples’ lives; therefore, subsequent innovations in quantum computers have a potential to improve the lives of many people as well as advance different fields of science and technology. Also, I want to mention another important aspect of quantum computing in relation to robots. According to a

journal article by Hans Moravec (1998), “humanlike robots are likely to arrive without [the help of quantum computers],” but the prototype chips “will probably incorporate a growing number of quantum interference components,” which means that “[the] 100 million MIPS (million instructions per second) to match human brain power will then arrive in home computers before 2030.” This is a very interesting connection between quantum computing and robotic technology.

Conclusion

I chose this topic because of its relevance to today’s world and because the discoveries in this field can significantly impact our future. I covered the main aspects of quantum computers as well as their benefits to society, their applications in other fields as well as current scientific research and development on this subject. Although no potential quantum computer has been built, scientists made a groundbreaking research in recent decades, which leads them closer to building one.

References

Schiller, J. (2009). *Quantum Computers* (1st ed., Vols. 1-1). Charleston, SC: CreateSpace. Retrieved

from

http://books.google.com/books?id=l217ma2sWkoC&printsec=frontcover&dq=quantum+computers&hl=en&ei=nLImTYm9D8H68AbLsaSKCw&sa=X&oi=book_result&ct=result&resnum=2&ved=0CDQQ6AEwAQ#v=onepage&q&f=false (Accessed on Thursday, February 10, 2011)

Annotation: This source is relevant to my research paper because it gives a detailed timeline on the history of quantum computers and computing.

Timeline of quantum computing. (n.d.). In *Wikipedia*. Retrieved February 12, 2011, from

http://en.wikipedia.org/wiki/Timeline_of_quantum_computing

Annotation: This source was another good way to complete my Background section of the paper to make a detailed timeline about the development of quantum computers. It includes the chronological timeline.

Quantum Decoherence. (n.d.). In *Wikipedia*. Retrieved February 19, 2011, from

http://en.wikipedia.org/wiki/Quantum_decoherence#Examples_of_non-unitary_modelling_of_decoherence

Annotation: This website helped me when I searched for the problems with quantum computers. It includes the information about quantum decoherence and examples of it.

Bonsor, K., & Strickland, J. (2000, December 8). *How Quantum Computers Work*. Retrieved February 17, 2011, from HowStuffWorks.com: <http://computer.howstuffworks.com/quantum-computer.htm>

Annotation: This source is helpful because it contains the information about the recent developments in quantum computers as well as how they theoretically work.

What is Quantum Computation? (2010, April 22). Retrieved February 14, 2011, from Quantiki: http://www.quantiki.org/wiki/What_is_Quantum_Computation%3F

Annotation: This source explains what the qubits are, what values they have, and how the quantum computer is supposed to work as well as the quantum decoherence.

Lloyd, S., Divincenzo, D., & Whaley, B. (2003). Will Computers Take A Quantum Leap? (R. Kuhn, Interviewer) Retrieved February 17, 2011, from PBS: http://www.pbs.org/kcet/closetotruth/explore/show_08.html

Annotation: This source is very credible because it is based on the discussion of the three leading scientists in the field of quantum computing who participated on the PBS show. They talked about the future prospects of quantum computers.

1999: Quantum Computing. (2011). Retrieved February 15, 2011, from AT&T Labs: <http://www.corp.att.com/attlabs/reputation/timeline/99quantum.html>

Annotation: This source is also reputable because AT&T Labs did a lot of research in the field of quantum computing and this is their official website. The information included is mainly about qubits and the differences between quantum and classical computer.

Newswire, J. (2011, January 21). Keio University and Oxford University Researchers Succeed in Entanglement, Essential for Quantum Computers, in Silicon Semiconductor. *JCN Network*. Retrieved February 18, 2011, from http://www.japancorp.net/Article.Asp?Art_ID=23639

Annotation: This article is new and covers an interesting discovery by researchers, which I thought would add more fresh information to my paper. It is about the quantum entanglement in silicon semiconductor.

University of Oxford (2011, February 9). Ultrafast quantum computer closer: Ten billion bits of entanglement achieved in silicon. *ScienceDaily*. Retrieved February 24, 2011, from <http://www.sciencedaily.com/releases/2011/01/110122110640.htm>

Annotation: This source also talks about entanglement of bits in silicon and the implication it might have for future developments of quantum computers. This source from ScienceDaily is the most recent.

Cirac, I. (2009, April). Author Commentaries – From Special Topics. (G. Taubes, Interviewer). Retrieved February 15, 2011, from <http://sciencewatch.com/ana/st/quantum/10aprSTQuanCira/>

Annotation: This source is also relevant because it is an interview with one of the noted researchers in the field of quantum computing. Ignacio Cirac explains what quantum entanglement is and how important it is for his and other scientists' research.

Moravec, H. (1998). When will computer hardware match the human brain. *Journal of Evolution and Technology*, 1(1).

Annotation: This source is reputable because it is a science journal article. It talks about computer hardware and memory, but also about the link between robots and quantum computer.

Quantum Cryptography. (2006, February 27). Retrieved February 15, 2011, from Quantiki: http://www.quantiki.org/wiki/Quantum_cryptography

Annotation: This source is reputable because I took it from the website of an educational organization that helps people to learn more about quantum computers and computing in general. This article is about quantum cryptography and its importance to the security of quantum computers.

Decoherence-free subspaces. (n.d.). In *Wikipedia*. Retrieved February 12, 2011, from

http://en.wikipedia.org/wiki/Decoherence-free_subspaces

Annotation: This source is reliable because it provides a detailed analysis on how to avoid decoherence in quantum computers by using the method called decoherence-free subspaces. It helped me to explain what decoherence is and how it is related to the security.

Steinberg, G. (2008). *Introduction to Computer Information Systems*. Dubuque, IA: Kendall/Hunt Publishing Company.

Annotation: This is a reputable source because it is a college textbook and because it gives brief but informative material, which might interest the reader to research more on the topic of quantum computers.