Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment

Scott Aaronson
MIT

Dave Bacon
University of Washington

Version 6: December 12, 2008[1]

For the last fifty years computers have grown faster, smaller, and more powerful — transforming and benefiting our society in ways too numerous to count. But like any exponential explosion of resources, this growth — known as Moore's law — must soon come to an end. Research has already begun on what comes after our current computing revolution. This research has discovered the possibility for an entirely new type of computer, one that operates according to the laws of quantum physics — a quantum computer.

A quantum computer would not just be a traditional computer built out of different parts, but a machine that would exploit the laws of quantum physics to perform certain information processing tasks in a spectacularly more efficient manner. One demonstration of this potential is that quantum computers would break the codes that protect our modern computing infrastructure — the security of every Internet transaction would be broken if a quantum computer were to be built. This potential has made quantum computing a national security concern. Yet at the same time, quantum computers will also revolutionize large parts of science in a more benevolent way. Simulating large quantum systems, something a quantum computer can easily do, is not practically possible on a traditional computer. From detailed simulations of biological molecules which will advance the health sciences, to aiding research into novel materials for harvesting electricity from light, a quantum computer will likely be an essential tool for future progress in chemistry, physics, and engineering. Finally, quantum computers represent a fundamentally new way of approaching information processing and, because this approach is based more closely on how our universe operates, it is likely that building a quantum computer will lead to unforeseen technologies and transform our understanding of the possibilities and limits of computation. For these reasons, as well as increasing international competition in the area, a major national investment should be undertaken in quantum computing and information as part of the new Administration's science and technology agenda.

What is at Stake

First, quantum computing must be considered a national security issue. Since quantum computers break the codes used ubiquitously to protect transactions over the Internet, any country obtaining a scalable quantum computer would have the ability to disrupt electronic communication. If the US is not the first to enter into the quantum computing age, the consequence could be loss of control over computer security. At the same time that we pursue the construction of a quantum computer, we should also put resources into understanding how to build codes which are not breakable by quantum computers.

Second, quantum information science research will help to maintain the US's scientific and technological advantages. A quantum computer, because it could simulate the physics that dominates at atomic and molecular scales, would give any country that possesses it great

[1] For the most current version of this essay, as well as related essays, visit http://www.cra.org/ccc/initiatives

strengths in its fundamental sciences and applied technologies. Just as computers revolutionized the Human Genome Project by allowing an information-theoretic shotgun approach to assembling the genome, quantum computers offer the potential to probe, simulate, and study quantum systems that are currently inaccessible using the fastest supercomputers. In fact, if one is to gain traction in understanding many physical systems of great import (such as complex biological molecules or complex materials), a quantum computer represents the only path known to be able to efficiently simulate these systems.

Third, quantum computing is the study of the fundamental limits of computing and, as such, offers the potential to revolutionize our understanding of computation itself. As technology shrinks to nanoscale levels, quantum effects need to be dealt with whether we want them or not. Because we now know that information processing at this quantum level differs significantly from traditional information processing, it is likely that a whole series of novel quantum devices could be harvested from quantum computing research.

Fourth, the study of quantum computers is already producing useful spinoffs for computer science and physics. These spinoffs include new insights into the power of existing classical computers, better algorithms for simulating certain kinds of quantum systems on classical computers, and better experimental techniques for the control of quantum systems. Since quantum computing is the most fundamental model of computation based on known laws of physics, we fully expect more such insights in the future.

Finally, we believe that a national initiative in quantum computing is vital to maintaining the United States as the world leader in computing technologies, and, in particular, to stop a brain drain of researchers from the United States. Quantum computing has excited tremendous interest around the world, as one of the major new developments in physics and computer science within the last two decades. We therefore believe that a national initiative in quantum computing offers enormous bang for the buck: not only is it groundbreaking fundamental science geared directly at producing workable new technologies, but it draws many of the best and brightest students and researchers from around the world.

Where We Stand

The US has long dominated computing technology. The transistor and integrated circuit were invented in the US, and Silicon Valley has been the preeminent creator of computing technologies over the last few decades. It is critical that the US continue to lead with the computing technologies of the 21st century. Recently Singapore invested over $100 million in quantum computing research. The Canadian government has contributed over $50 million to the University of Waterloo's Institute for Quantum Computing and the Perimeter Institute for Theoretical Physics, both of which have become world leaders in quantum computing and information. European spending on quantum computing is comparable to that of the US. In short, while the US has funded quantum computing research, it has done so only at a level sufficient enough to barely keep up with the rest of the world. In some areas of quantum computing, for instance in the theory of these computers, the US is being eclipsed by the rest of the world.

A Proposed Program

Current funding for quantum computing is split over numerous agencies, the larger portion coming from defense and intelligence agencies (iARPA, DARPA, etc.) and a smaller portion coming from the National Science Foundation. If a national investment in quantum computing is undertaken, we believe that NSF is the natural agency for such an investment

to be housed. First, this is because the majority of currently active research groups are centered around academic computer science, physics, and mathematics departments. Second, many of a quantum computer's first applications will not be in the national security arena – it is far more likely that small quantum computers will be put to use studying chemistry or physics and thus fall much more naturally under the fundamental science purview of the NSF.

We suggest that the NSF fund several large centers, based upon existing experimental efforts around the United States, which are specialized to the major approaches being taken toward building a quantum computer. These centers should have sufficient resources to fund their own internal effort as well as to support external efforts to develop the technologies needed for quantum computation. A goal should be set for these centers of building a quantum computer which outperforms today's classical computers at quantum simulation tasks within the next decade. We also believe it is essential that a significant NSF program be established to deal with computer security in a post-quantum-computing world. Such a program would focus on cryptography that is resistant to quantum attacks, the capabilities and limits of quantum computers, and the limits of feasible computation more generally. Finally, to support these efforts, we recommend that the NSF's existing modest investment in the theoretical foundations of computer science be enhanced.

A Call to Action

Building a quantum computer is daunting challenge. Current progress toward this goal is best described as piecemeal. However, we are currently approaching a tipping point for quantum computers: the most promising technologies have demonstrated all the necessary building blocks of a quantum computer. A large effort to carry these technologies forward and put these blocks together is now prudent, and, we believe, likely to produce future technological spin-offs. The national security consequences of delayed investment in quantum computing, the valuable return on this investment, and the long-term benefits of putting the US at the front of this 21st-century intellectual endeavor, all argue for support of a serious national initiative in quantum computing.