Canadian Opportunities and Competitive Advantages in Quantum Computing

17 April 2002

(Replaces all previous versions)

By

Morley S. Lipsett
lipsett@sfu.ca

And

Richard G. Lipsey
rlipsey@sfu.ca

Centre for Policy Research on Science and Technology
Simon Fraser University at Harbour Centre
515 West Hastings Street
Vancouver, BC V6B 5K3

Prepared in cooperation with

Director, BC Regional Innovation
National Research Council of Canada
3250 East Mall
Vancouver, BC V6T 1W5

Canadian Opportunities and Competitive Advantages in Quantum Computing

EXECUTIVE SUMMARY

This document discusses the possibility of establishing a quantum computing technology cluster in Canada. This technology has great economic, industrial and academic potential, possibly comparable to the invention of the electronic computer or the laser.

The Vancouver region already possesses the necessary ingredients for technological and economic breakthroughs in quantum computing. Key personnel are in place, productive linkages exist with leading universities across the country, proprietary technology is being developed, and the resulting intellectual property is being given strong patent protection. Angel investors and venture capitalists with respected track records are bringing management strength, entrepreneurial experience, financial stability, and sources of subsequent financing to the scientific and industrial organizations that are developing to exploit this opportunity.

International competition is fierce and developments in other countries are receiving substantial financial assistance from public bodies. A relatively small injection of Canadian public money would be critical at this stage in allowing the Canadian group to solidify its competitive edge over the rest of the world and to proceed to the stage where private sector funding could carry the whole burden of further developments. What is urgently required now is an in-depth investigation directed towards formulating an action plan for government support using existing innovation support programs.

This brief document describes a vision for building a quantum computing industrial cluster in Canada centered in BC. It proposes a low-cost feasibility study that would culminate in an action plan appropriate to the opportunity.

Introduction

The special circumstances that created and built Vancouver's MDA, QLT, Dynapro Systems, Ballard Power, and Electronic Arts Canada are on the verge of doing it again. This time it is in a field of science that will revolutionize information technology by developing a quantum computer.

The science behind this new type of computer, quantum physics, sounds exotic and counter-intuitive. But this was equally true, until recently, of the transistor and the laser. Both of these sounded exotic and weird in the early days but now are they are a part of everyday life, even if the science behind both of them is still hard to explain in everyday language.

Several countries have groups of scientists and engineers working on quantum computing. Japan, the UK, and several European countries, are among the leaders in terms of size of the teams, their international prominence and the funding they receive. The US is also active in various research settings, including MIT, CalTech, the University of Texas, and Los Alamos National Labs. Substantial public sector funding is underpinning all these major efforts.

This attention is not surprising given the practical potential for a working quantum computer. For example, progress in biotechnology is currently hampered by the limitations of current computer technology. It takes an enormous amount of computation to explore and understand the way that specific proteins interact with specific human receptors in disease prevention and cure. Even if all of the computers and supercomputers in the world could work simultaneously on the same computational problem in biotechnology, they would still be inadequate for the job. Yet the power of such a hypothetical computing team would scarcely register on the scale of what a quantum computer could do.

Conventional computers are classical in their operation, and do things more or less one step at a time, albeit very quickly. Quantum computers, on the other hand, have no such restriction. One day soon they will be able to perform as many calculations in parallel as there are stars in the universe.

No other technology holds equivalent promise for rapidly solving so many practical mathematical riddles such as those associated with decryption, money laundering, protein molecular shapes, long-term weather forecasting, seismic predictions, image synthesis, and tracking covert criminal operations. The spin-offs will include, new products, new firms and many new jobs.

Canada is at the forefront of developments in this field, with noted scientists and engineers working in university and industrial labs in BC, Alberta, Ontario and Quebec. The University of British Columbia's Physics Department is particularly

prominent in this effort, thanks to a long history of world-class research in solid state and low temperature quantum physics.

The annual Canadian investment in quantum computing is on the order of several million dollars, which is small compared with the amounts being invested in other countries. However, no nation is closer to commercial and strategic exploitation than Canada. The Vancouver Company, D-Wave Systems Ltd. could well become the next QLT in terms of international recognition and impact. Like QLT, its success would result from long-term collaboration among universities, the financial sector, and government in a strategically important field of science and technology. Just as QLT did in its early years, D-Wave taps the concentration of scientific and technical knowledge that exists in Vancouver and links with top-ranking local, national and foreign universities. This concentration of quantum computing intellectual power and business acumen gives Canada a good chance of achieving renown and commercial success in this new, exotic, but potent technology. But, as with all really path breaking new technologies that require substantial scientific as well as technical advance, it is difficult to fund the early stages solely with private funds.

Recommendation

This paper recommends that government support be provided for an informal and low-key feasibility study. The study should include consultation with academic, business, government and financial sector stakeholders. It should culminate in a well-defined strategy for ways of fostering a quantum-computing cluster in British Columbia. This strategy should be appropriate to the identified opportunities and should use existing Canadian innovation support programs.

The technology of quantum computing

The contrast between classical computing and quantum computing

All of our familiar computers, including every PC, mainframe, supercomputer, game console, minicomputer, palmtop and laptop, are little more than complex sets of interconnected on/off switches. They are transistorized equivalents of ways to remember and record the precise setting of each switch. In some cases, the switches go on and off over 1 billion times per second, and millions of transistors participate in the rhythmic dance of the switches. They can do so only one step at a time, but this happens extremely rapidly – giving us the impressive computer technology.

In these solid-state devices information elements are encoded (carried) as bits. Each bit is lodged in a physical element less than ½ billionth of a metre. Computing processes are expressed as so many operations per second, sometimes billions per second. Even so, bit states can only be switched in a time-dependent sequence. Smaller size and faster operations improve computing power. More and more bits in a single device allow for representations of very large numbers, but only one at a time. An eight-bit device can represent $2^8 = 256$ different combinations of 0s and 1s and thus 250 different states but only one of them at any one time.

Computational speed has been doubling every 18 months to two years. More recently the doubling time has shrunk to 14-16 months. However, the physical limit to this increase is in sight, and the potential end-state power of such computers does not begin to compare with the potential of even early-stage, relatively crude computers based on quantum effects.

In quantum computing devices, discrete pairs of quantum states are used to represent information elements; i.e. quantum bits. This gives rise to the term ***qubit***. As presently conceived, qubits can be of various designs and sizes ranging from desk-size nuclear magnetic resonance apparatuses to specialized low-temperature solid-state devices the size of conventional computer chips.

Size is less an issue for qubits than for conventional microprocessors. This is because qubits do not need to be closely packed to attain remarkable properties. The larger qubits under development are cumbersome, but useful to demonstrate the principles of quantum computing. Such demonstration devices cannot be readily scaled up to large arrays of qubits. Others are comparatively tiny and, like nanotechnology devices, are based on only a small number of individual atoms or molecules. One of the most promising scalable designs is being developed in Vancouver. It is about the same size as Pentium IV structures, and lends itself to being arrayed as a multiplicity of qubits.

Qubits require a new way of thinking since they do not suffer from the one-at-a-time limitation of classical bits. Instead, they enjoy the unusual property of representing 2 bits of information at the same time. More and more qubits allow for the simultaneous representation of all possible combinations of very large numbers. A device consisting of eight associated qubits can represent 2^8, or all 256 possible combinations of zeros and ones *at the same time*. The number of possible simultaneous combinations represented by a 150-qubit device equals 2^{150}, which defies the imagination.

Combinations of classical bits can be switched rapidly but only follow a single path in time. Not so with Qubits. Qubit arrays allow many simultaneous computational streams – as many as there are possible combinatorial states of the array. Thus an 8-qubit device could bring the equivalent of 256 conventional computers to bear on a single computational problem simultaneously.

At this rate of exponential multiplication, it does not take very many more qubits to represent very large numbers. Our example of a 150-qubit device could harness the equivalent of more conventional computers than the number of atoms in the universe. This is why one focus in quantum computing research is to develop scalable technology – the inherent capacity to harness increasing numbers of qubits operating in tandem.

Timeline

It seems reasonable to expect that an operationally useful quantum computer will be achieved in from 5 to 10 years from now. The theoretical basis is sound, and the formerly intractable problem of noise in the machine has been solved. Methods for correcting errors in quantum computing circuits have been developed and shown to work in labs around the world. Laboratory-scale qubits already exist, albeit in cumbersome form and without easy mechanisms to scale them up. IBM has reported a 7-qubit quantum computer based on a non-scalable technology that uses the liquid-state nuclear magnetic resonance (NMR) technique.

At this point it appears that a solid-state physics approach relying on quantum superconducting phenomena realized in relatively small devices holds the greatest promise.

The present state of the art

Conventional approaches to software are unsuited to quantum computers. In recent years, however, approaches have been developed that could indeed be used to solve practical problems with quantum computers. For example, mathematical methods now exist for decryption (code breaking) using quantum computers.

Also, methods that are exponentially faster than classical computers exist for simulating the behaviour of molecules.

Quantum computer hardware is at a very early stage of development. Progress is slowed by the need to develop fabrication technology for the new kinds of devices that are being created. Progress by the Vancouver group is likely to yield one of the first, if not *the* first scalable multi-qubit solid-state quantum computers within 3 years. After that, progress should accelerate, and prototype quantum computers could become available for immediate application in such fields as biotechnology and quantum information technology.

The value of a breakthrough in computer technology

Ultra-massively parallel computing (quantum computing) would help us to:

- predict the three-dimensional structure of proteins from DNA sequence information (the "protein folding problem");
- design small molecule drugs;
- enable virtual high throughput screening for the drug discovery process;
- use computer models to predict whether a drug candidate will fail in clinical trials;
- predict the weather with increased reliability over longer periods of time;
- discover the clandestine connections around the world that finance organized crime and terrorism;[1]
- develop more-detailed pictures of our physical universe;
- understand and manage ecology;
- understand and manage biological processes;
- come closer to comprehending how the brain works.

Perhaps the first applications will be to model the way that complex quantum mechanical systems work, such as molecules, atoms, and nuclei. For example, D-Wave has developed applications for designing pharmaceutical products "from scratch." These include structure based drug design, virtual high-throughput screening, and predictive virtual ADME/Tox profiling. Breakthroughs in science at this level will undoubtedly lead to breakthroughs in other complex fields such as economics, engineering and epidemiology.

[1] We note, for example, that the US Department of Defence is reported to be *seeking innovative technology solutions in 38 different technologies. The intent of the solicitation process is to identify technologies and approaches that may provide near, mid, and long term solutions that enhance current capabilities to critical multi-agency and future threat requirements. A few examples of the many technologies sought include: automated speaker recognition, voice print recognition, tracking/locating remote sensors, locating/identifying faces in visual images, physical security, advanced distributed learning, tactical operations support, early warning devices, and chemical/biological/radiological/nuclear countermeasures.* http://strategis.gc.ca/SSG/wn00020e.html?hc=y

Each of these applications is also a commercial opportunity. Just as Ballard Power has given Canada domestic employment and prominence in hydrogen fuels and fuel-cell technology, a successful quantum computing cluster can be expected to bring high technology & biotechnology prominence and jobs to Canada in what is destined to become the next wave of technology.

Recommendation

It is recommended that Canadian opportunities for quantum computing be brought to the attention of senior levels of government. The purpose is twofold; to highlight the strategic importance and economic potential for quantum computing in Canada, and to propose that support be provided for the development of a Canadian strategy for quantum computing.

Without additional investigation, however, it would be premature to argue for specific budgets or policy intervention. This paper, therefore, recommends that modest funding be provided for a detailed feasibility study of ways to foster the creation of a Canadian quantum-computing cluster, centered around, but not exclusively based in, British Columbia. The study should culminate in a well-defined strategy and action plan, appropriate to the identified opportunities, and should be based on consultation with the academic, business, government and financial sector stakeholders.

We therefore also recommend that an ad-hoc meeting of stakeholders and experts be convened for the purpose of discussing the prospects for creating a quantum-computing cluster in BC. The deliberations should

a. Focus on establishing the terms of reference for the preparation of a strategic plan and proposal for the creation of such a cluster,
b. Offer suggestions and comments for the direction and management of the proposal,
c. Make recommendations with regard to the directions to be taken,
d. Identify support options to be considered, including
    - R&D contracts (in support of departments and agencies meeting operational needs)
    - Specialized innovation grants or co-funding, and
e. Make such other recommendations as may arise.

The composition of this ad-hoc group might include the following representation:

Director of the UBC and/or SFU University/Industry Liaison Office
Director of the NRC BC Regional Innovation
Dean of Business Administration, SFU
Directors of Departments of Physics, Computer Science & Chemistry at UBC and SFU

Adjunct Professor (Entrepreneurial Programs) at UBC
Emeritus Professor of Economics, and CIAR Fellow
University Research Associate, CPROST
Interested Federal and Provincial Departments and Agencies
President & CEO of D-Wave Systems Inc

The Centre for Policy Research on Science and Technology (CPROST) offers to host such a meeting in the near future at the Harbour Centre Campus.

If requested, CPROST will also serve as an interim secretariat for the group and will compile background information for the participants. Also, if requested and if acceptable to the participants, CPROST will coordinate the preparation of a strategic plan/feasibility study/business case for the creation of a quantum-computing cluster in Canada. Such further CPROST involvement would be partially co-funded through the existing budget of the Innovation Metrics and Policy Program. However additional funding would be required for background research, analysis, communication and meeting costs, and report preparation.

References and excerpts

Books

Quantum Computation and Quantum Information"
By Michael A. Nielsen & Isaac L. Chuang
Cambridge University Press, 2000

Considered the 'bible' of the field, this book is said to be a *comprehensive introductory text in the main ideas and techniques of quantum computation and quantum information. Answers questions about the physical limits to computation and communication, describing all kinds of quantum phenomena*.

Quantum Computing
By Jozef Gruska
McGraw Hill, May 1999

In quantum computing, we witness an exciting and very promising merge of two of the deepest and most successful scientific and technological developments of this century: quantum physics and computer science. In spite of the fact that its experimental developments are in their infancy, there has already been a variety of concepts, models, methods and results obtained at the theoretical level that clearly have lasting value.

Specialized web sites

Here are some representative sites:

Oxford University
www.qubit.org

The discovery that quantum physics allows fundamentally new modes of information processing has required the existing theories of computation, information and cryptography to be superseded by their quantum generalisations. The Centre for Quantum Computation, part of the University of Oxford, conducts theoretical and experimental research into all aspects of quantum information processing, and into the implications of the quantum theory of computation for physics itself.

CalTech
www.iqi.caltech.edu/qis.html

University of Montreal
www.iro.umontreal.ca/labs/theorique/index.html.en

University of Calgary
www.cpsc.ucalgary.ca/Research/quantum/

Review articles

MIT's Technology Review Magazine
Quantum Computing
By M. Mitchell Waldrop
May/June 2000
In the realm of subatomic weirdness, ones and zeroes dissolve into a muddle of probabilities. Out of the blur could come machines with unthinkable speed.

http://www.technologyreview.com/magazine/may00/waldrop.asp

New York Times
Gauging the Limits of Quantum Computing
By Sara Robinson
March 7, 2000

Six years ago, Dr. Peter Shor, a researcher at AT&T Labs, galvanized an obscure area of computer science when he published a recipe by which a computer based on the principles of quantum mechanics could break the cryptographic codes protecting data transmissions over the Internet.

Since then, top researchers around the world have joined forces to further explore how the power of the strange rules that prevail in the submicroscopic realm of the atom can be harnessed in a computer.

The Economist
Quantum dreams
Mar 10th 2001

In theory, quantum computers can do things ordinary computers cannot. In practice, a useful quantum computer is still a long way off.

Companies

MagiQ Technologies, Inc (American)
http://www.magiqtech.com/qinf

The aim (of this company) is to be developing commercial quantum information devices and building a portfolio of useful intellectual properties (IP), by performing research and development in the area of commercial exploitation of quantum information processing (QIP). All technologies related to QIP are of

interest ... from the short and medium term goal of quantum communication and quantum cryptography to the long term goal of large scale quantum computation.

MagiQ does not view QIP as "blue-sky" research but rather as a nascent group of disruptive technologies that will dramatically affect the future. We believe QIP will revolutionize the world of the 21st century in the same way that classical mechanics through the steam engine, electromagnetism through electricity, and quantum mechanics through transistors and lasers transformed the 19th and 20th centuries…. *MagiQ is investing early in promising areas of the subject in order to establish itself as the leader in this field.*

...A number of large, multinational corporations including AT&T, Bell Labs, IBM, Microsoft, NEC and NTT are doing research on the subject. Many universities (including MIT, Caltech, Stanford, and Princeton) are working on it. In the US, DARPA (Defense Advanced Research Projects Agency) has recently allocated $100 million over the next 5 years for research on quantum information processing, as part of their initiative to explore the future of computing beyond silicon technology.

D-Wave Systems, Inc. (Canadian)
www.dwavesys.com

D-Wave is a University of British Columbia spin-off company. It was created to capitalize on the intellectual resources of the company's founders. Its goal is to build an enterprise that brings the promise of quantum computing to commercial fruition. D-Wave is focused on the in-house development of chip-based quantum computers.

The company's current research team includes leading scientists and engineers from Canada, The United States, Germany, Sweden, Holland, Russia, Ukraine, and the Slovak Republic. The central areas of technical expertise are in nanofabrication, basic device physics and engineering, materials science and quantum information.

D-Wave recently received the *Investor's Choice* award at the 3rd Annual Pacific Northwest Venture Capital Forum, an event co-sponsored by the BCTIA and BC Biotech Alliance. The award recognized the company's on-chip quantum computing technology, the company's focus on applications in computational bioscience, and the prospects of creating the world's next "big technology" industry in BC.