13th Symposium on Theoretical Aspects of Computer Science
Grenoble, France 22–24 February 1996

New Trends in Quantum Computing

Gilles Brassard *

Université de Montréal, Département d'informatique et de recherche opérationnelle
C. P. 6128, Succursale Centre–Ville, Montréal (Québec), Canada H3C 3J7
email: brassard@iro.umontreal.ca

Abstract. Classical and quantum information are very different. Together they can perform feats that neither could achieve alone, such as quantum computing, quantum cryptography and quantum teleportation. Some of the applications range from helping to preventing spies from reading private communications. Among the tools that will facilitate their implementation, we note quantum purification and quantum error correction. Although some of these ideas are still beyond the grasp of current technology, quantum cryptography has been implemented and the prospects are encouraging for small-scale prototypes of quantum computation devices before the end of the millennium.

1 Introduction

Classical and quantum information are very different. Classical information can be read, copied and transcribed into any medium; it can be transmitted and broadcast. Quantum information cannot be read or copied without disturbance, but it can exist in superposition of classical states. Together, the two kinds of information can perform feats that neither could achieve alone, such as quantum computing, quantum cryptography and quantum teleportation. These concepts could result in a revolution in computer science that may dwarf that created decades ago by the transistor.

In principle, computers could be built to profit from quantum phenomena that have no classical analogue, sometimes providing exponential speed-up compared to classical computers. The most famous example of an algorithm for the quantum computer, due to Shor, allows for the polynomial-time factorization of large integers, a task believed to be intractable for classical computers. Because of the pivotal nature of this problem in modern cryptography, a full-scale working quantum computer could be used by spies to allow them nearly unlimited access to your electronic transactions. On the other hand, quantum information is also at the core of other phenomena that would be impossible to achieve in a purely classical world, such as the unconditionally secure distribution of secret cryptographic key material. Therefore quantum techniques may cause the collapse of much of classical cryptography, yet they may also offer the cure to make unconditionally secure communication possible.

* Research supported in part by Canada's Nserc and Québec's Fcar.

2 Review of Quantum Techniques

For a comprehensive review of quantum techniques in computer science, I suggest you read my earlier essay "A Quantum Jump in Computer Science" [12]. Although this section provides a very superficial one-page introduction to these topics, my purpose in these Proceedings is to report on new ideas and developments that were not yet available at the time "A Quantum Jump" went to press. These developments range from new theoretical ideas to actual implementation proposals for quantum computation. To emphasize how active and exciting the field has become, I deliberately restricted my coverage to papers that have appeared in 1995 or later, or yet-unpublished manuscripts that were written in the same period. Please consult "A Quantum Jump" for proper credit and references to the early ideas reviewed in this section.

In classical information theory, a bit can take either value 0 or 1. According to quantum mechanics, a quantum bit, or *qubit*, can be in linear *superposition* of the two classical states, with complex coefficients. This is best visualized as a point on the surface of a unit sphere whose North and South poles correspond to the classical values. This is entirely different from taking a value *between* 0 and 1 as in classical analogue computing. In general, qubits cannot be measured reliably: not more than one classical bit of information can be extracted from any given qubit and the more information you obtain about it, the more you disturb it irreversibly.

The impossibility to measure quantum information reliably is at the core of quantum cryptography. When information is encoded with non-orthogonal quantum states, any attempt from an eavesdropper to access it necessarily entails a probability of spoiling it irreversibly, which can be detected by the legitimate users. This phenomenon can be exploited to implement a key distribution system that is secure even against an eavesdropper with unlimited computing power. Several prototypes have been built, including one that is fully operational under laboratory conditions over 30 kilometres of ordinary optical fibre. In another experiment, quantum transmission was successful over a distance of 23 kilometers under Lake Geneva [29]. Quantum techniques may also assist in the achievement of subtler cryptographic goals, such as protecting private information while it is being used to reach public decisions.

Independent qubits are sufficient to produce nontrivial cryptographic phenomena, but they are not very interesting for computational purposes. For this, we must consider quantum *registers* composed of n qubits. Such registers can be in an arbitrary superposition of all 2^n classical states. In principle, a quantum computer can be programmed so that exponentially many computation paths are taken simultaneously in a single piece of hardware, a phenomenon known as *quantum parallelism*. What makes this so powerful—and mysterious—is the exploitation of constructive and destructive *interference*, which allows for the reinforcement of the probability of obtaining desired results while at the same time the probability of spurious results is reduced or even annihilated. In the words of Feynman, "it appears as if the probabilities would have to go negative".

3 Good Starting Points

In addition to my "Quantum Jump" article [12], several excellent introductions to quantum computing have been written recently. Let us mention [27] in *Scientific American*, [23] in *Discover*, [7] in *Nature*, [4] in *Physics Today*, [21] in *Science*, and [10]. In addition, Shor has written a very nice account of his quantum factorization algorithm [32], which introduces the basic concepts of quantum computing.

4 The Power of Quantum Computing

Quantum computing was considered at best as a curiosity by most researchers until Shor discovered in 1994 that it could be used to extract discrete logarithms and factorize large numbers very efficiently. This attracted considerable attention, not only because of its tremendous cryptographic significance, but also because it gave the first indication that quantum computers could be genuinely faster than classical probabilistic computers for solving natural problems of a mathematical nature. The obvious question that followed was: "What else are quantum computers good at?"

Unfortunately, Shor's discovery was not followed by a flurry of other natural problems that the quantum computer could solve much more efficiently than using the best algorithm available for a classical computer. Nevertheless, a few such results have emerged already and perhaps still others are waiting in the wings. Using a method similar to Shor's, Boneh and Lipton [11] showed that any cryptosystem based on what they call a "hidden linear form" can be broken in polynomial time on a quantum computer. In particular, a quantum computer can solve the discrete logarithm problem efficiently over *any* group including Galois fields and elliptic curves.

Another extension to Shor's result is due to Kitaev [24], who discovered how to solve the Abelian stabilizer problem efficiently on a quantum computer. This method provides an efficient quantum Fourier transform algorithm for an arbitrary Abelian group.

5 Experiments in Quantum Computing

As I explained in "A Quantum Jump", the discovery that universal quantum circuits could be built around two-qubit gates was very significant because the technological difficulties would be even more daunting if it had been necessary to make qubits interact three at a time. Unfortunately I gave only reference to the work of DiVincenzo [20] in my earlier essay. The same result was found independently by Barenco [1] and by Sleator and Weinfurter [33]. It was subsequently discovered by Chau and Wilczek [14] that six two-qubit gates are sufficient to implement the quantum Fredkin gate, which is a natural three-qubit universal gate; this result was improved by Smolin and DiVincenzo [34] to needing only five two-qubit gates for the same purpose. In fact, almost *any* two-qubit gate is universal, as Deutsch, Barenco and Ekert [19] and Lloyd [26] discovered independently. The most significant result along these lines is probably the discovery that the quantum exclusive-or gate, which maps (x, y) to $(x, x \oplus y)$, is universal for quantum computation in the sense that all unitary operations on arbitrarily many qubits can be expressed as compositions of these gates together with appropriate one-qubit gates [2].

This begs the question: how hard is it to implement the quantum exclusive-or gate? Several approaches have been proposed for this purpose. Cirac and Zoller proposed to use cold trapped ions [18]. An actual implementation of the quantum exclusive-or gate using beryllium ions in an atom trap has been tested with encouraging results by Monroe, Meekhof, King, Itano and Wineland [28] at NIST in Boulder, Colorado. Another team led by Hughes at the Los Alamos National Laboratory has received funding for experimenting with cold trapped calcium ions. They hope to be able to implement a small-scale version of Shor's quantum factorization algorithm within a few year. Their initial goal is to factorize the number 4 before the end of the millennium, but they are confident that this will only be a beginning.

Another approach to the implementation of basic quantum gates, using cavity quantum electrodynamics, has been proposed by Sleator and Weinfurter [33]. Initial experiments on similar ideas, using atomic interferometry and microwave cavities, have been performed at the École Normale Supérieure in Paris by Domokos, Raimond, Brune and Haroche [22]. Experiments are also under way at the California Institute of Technology, where Turchette, Hood, Lange, Mabuchi and Kimble are investigating photon qubits interacting in an optical microcavity [36]. See also [3].

An explicit construction of quantum networks for performing arithmetic operations from basic quantum gates is given by Vedral, Barenco and Ekert [38]. This may prove important for an actual implementation of Shor's algorithm, which requires basic arithmetic from addition to modular exponentiation. In particular, this paper shows that the amount of auxiliary storage required to implement Shor's algorithm grows linearly with the size of the number to be factorized.

Yet another proposal for the construction of a "simple quantum computer" comes from Chuang and Yamamoto [17].

6 The Problem of Decoherence

Despite the reasons to be optimistic that the work described in the preceding section might generate, it may be that quantum computing will never become practical because of the technological difficulties in preventing unwanted interactions with the environment: such interactions cause *decoherence*, which in effect ruins the quantum computation. An early—and rather discouraging—study of the effect of decoherence on quantum computers was carried out by Unruh [37].

Other difficulties with the implementation of quantum computers have also been pointed out repeatedly by Landauer [25].

The effect of decoherence on Shor's algorithm has been studied explicitly by Chuang, Laflamme, Shor and Zurek [16] and by Plenio and Knight [30].

7 Quantum Error Correction

Error correction is used routinely when dealing with classical information. However, it is not obvious that error-correction schemes can exist for quantum information because it cannot be measured without disturbance. In particular, a simple repeat code is out of the question since quantum information cannot be cloned. Nevertheless, quantum information needs to be protected from errors even more than classical information in view of its susceptibility to decoherence. An early scheme for quantum error correction, proposed by Deutsch, was investigated by Berthiaume [9] and Jozsa.

Assuming that the decoherence process affects the quantum computer's qubits independently, Shor has found a technique that allows the storage of an arbitrary state of n qubits using $9n$ qubits in a decoherence-resistant way: even if one of the qubits decoheres, the original state can be reconstructed perfectly [31]. Subsequently, Shor improved on his original idea in collaboration with Calderbank, making it possible to recover the original quantum state even if several qubits decohere [13]. Other quantum error-correction techniques have been proposed by Chuang and Laflamme [15] and by Steane [35].

Another approach to quantum error correction is based on the ideas of entanglement concentration [5] and entanglement purification [6]. The latter is a technique that allows near perfect entanglement to be distilled from imperfect entanglement that may have been caused by partial decoherence—or by eavesdropping for quantum cryptographic applications. This is accomplished by local operations and the exchange of classical messages. Because perfect entanglement can be used for the purpose of teleporting quantum information, entanglement purification can be used to transmit quantum information with arbitrary fidelity over a noisy quantum channel supplemented by a good classical channel. More advanced ideas, such as "teleportation from the present to the future, rather than from here to there" can be used to design a quantum error-correction scheme from quantum purification and quantum teleportation [8].

8 The Art of Quantum Programming

By now, I am sure you are itching to write your first program for the quantum computer. In that case, you will be happy to learn that Baker is in the process of developing Q–GOL, a high-level language for the quantum computer. You can find more information on the World Wide Web (WWW) at URL

`http://www.rp.csiro.au/~gbaker/q-gol/`

9 Quantum Information on the Internet

Many WWW sites have blossomed with information on quantum computation, quantum cryptography and quantum information theory in general. The following URLs are excellent starting points for a fascinating journey into the quantum world. Nearly all the papers cited as "manuscript" or "in press" in the references at the end of this essay can be downloaded from the quantum physics archive at Los Alamos National Laboratory. Have fun!

`http://xxx.lanl.gov/archive/quant-ph`
: Quantum Physics Archive at Los Alamos National Laboratory

`http://eve.physics.ox.ac.uk/QChome.html`
: Quantum Computation and Cryptography Home Page at Oxford

`http://aerodec.anu.edu.au/~qc/index.html`
: Quantum Computing Home Page
at Australian National University

`http://feynman.stanford.edu/qcomp/`
: Quantum Computation Archive at Stanford

`http://vesta.physics.ucla.edu/~smolin/`
: John Smolin's Quantum Information Page

`http://www.cwi.nl/~berthiau`
: André Berthiaume's Home Page

`http://www.iro.umontreal.ca/labs/theorique/index_en.html`
: Laboratoire d'informatique théorique et quantique
at Université de Montréal

In addition, you can find tutorials at the following URLs.

`http://chemphys.weizmann.ac.il/~schmuel/comp/comp.html`
: Samuel L. Braunstein's Tutorial on Quantum Computation

`http://eve.physics.ox.ac.uk/QCresearch/cryptoanalysis/qc.html`
: Artur Ekert's "Introduction to Quantum Cryptoanalysis"

`http://www.cwi.nl/~berthiau/publications/CTR.ps`
: André Berthiaume's Tutorial on Quantum Computation [10]

10 Do you Need a Daily Fix?

If you cannot live without knowing what is new every day, send electronic mail to `quant-ph@xxx.lanl.gov` with subject "subscribe" and let it guide you!

Acknowledgements

I am very grateful to all those who helped me put this essay together: Charles H. Bennett, David DiVincenzo, Artur Ekert, Christopher Fuchs, Richard Hughes, Michael Kernaghan, Christopher Monroe, Peter Shor and Andrew Steane.

References

[1] A. Barenco, "A universal two-bit gate for quantum computation", *Proceedings of the Royal Society*, London, Series A, Vol. 449, 1995, pp. 679 – 683.

[2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. W. Shor, T. Sleator, J. A. Smolin and H. Weinfurter, "Elementary gates for quantum computation", *Physical Review A*, Vol. 52, 1995, pp. 3457 – 3467.

[3] A. Barenco, D. Deutsch, A. Ekert and R. Jozsa, "Conditional quantum dynamics and logic gates", *Physical Review Letters*, Vol. 74, 15 May 1995, pp. 4083 – 4086.

[4] C. H. Bennett, "Quantum information and computation", *Physics Today*, October 1995, pp. 24 – 30.

[5] C. H. Bennett, H. Bernstein, S. Popescu and B. Schumacher, "Concentrating partial entanglement by local operations", *Physical Review A*, in press.

[6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels", *Physical Review Letters*, in press.

[7] C. H. Bennett and D. P. DiVincenzo, "Quantum computing: Towards an engineering era?", *Nature*, Vol. 377, 5 October 1995, pp. 389 – 390.

[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error correcting codes", manuscript, 1995.

[9] A. Berthiaume, "L'ordinateur quantique: Complexité et stabilisation des calculs", PhD Thesis, Université de Montréal, 1995.

[10] A. Berthiaume, "Quantum computation", in *Complexity Theory Retrospective II*, L. A. Hemaspaandra and A. Selman, editors, Springer-Verlag, Berlin, in press.

[11] D. Boneh and R. J. Lipton, "Quantum cryptanalysis of hidden linear functions", *Advances in Cryptology—Crypto'95 Proceedings*, Lecture Notes in Computer Science, Vol. 963, Springer-Verlag, Berlin, 1995, pp. 242 – 437.

[12] G. Brassard, "A quantum jump in computer science", in *Computer Science Today*, J. van Leeuwen, editor, Lecture Notes in Computer Science, Vol. 1000 (special anniversary volume), Springer-Verlag, Berlin, 1995, pp. 1 – 14.

[13] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist", manuscript, September 1995.

[14] H. F. Chau and F. Wilczek, "Simple realization of the Fredkin gate using a series of two–body operators", *Physical Review Letters*, in press.

[15] I. L. Chuang and R. Laflamme, "Quantum error correction by coding", manuscript, September 1995.

[16] I. L. Chuang, R. Laflamme, P. W. Shor and W. Zurek, "Quantum computers, factoring, and decoherence", manuscript, March 1995.

[17] I. L. Chuang and Y. Yamamoto, "A simple quantum computer", manuscript, May 1995.

[18] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions", *Physical Review Letters*, Vol. 74, 15 May 1995, pp. 4091 – 4094.

[19] D. Deutsch, A. Barenco and A. Ekert, "Universality in quantum computation", *Proceedings of the Royal Society*, London, Series A, Vol. 449, 1995, pp. 669 – 677.

[20] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation", *Physical Review A*, Vol. 51, February 1995, pp. 1015 – 1022.

[21] D. P. DiVincenzo, "Quantum computation", *Science*, Vol. 270, 13 October 1995, pp. 255 – 261.

[22] P. Domokos, J.–M. Raimond, M. Brune and S. Haroche, "Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances", *Physical Review A*, November 1995, pp. 3554 – 3559.

[23] T. Folger, "The best computer in all possible worlds", *Discover*, October 1995, pp. 90 – 99.

[24] A. Yu. Kitaev, "Quantum measurements and the Abelian Stabilizer Problem", manuscript, November 1995.

[25] R. Landauer, "Is quantum mechanically coherent computation useful?", in *Proceedings of the Drexel-4 Symposium on Quantum Nonintegrability—Quantum Classical Correspondence*, D. H. Feng and B.–L. Hu, editors, International Press, 1995.

[26] S. Lloyd, "Almost any quantum logic gate is universal", *Physical Review Letters*, Vol. 75, 10 July 1995, pp. 346 – 349.

[27] S. Lloyd, "Quantum-mechanical computers", *Scientific American*, October 1995, pp. 44 – 50.

[28] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano and D. J. Wineland, "Demonstration of a fundamental quantum logic gate", *Physical Review Letters*, Vol. 75, 1995, pp. 4714 – 4717.

[29] A. Muller, H. Zbinden and N. Gisin, "Underwater quantum coding", *Nature*, Vol. 378, 30 November 1995, page 449.

[30] M. B. Plenio and P. L. Knight, "Realistic lower bounds for the factorization time of large numbers on a quantum computer", submitted to *Physical Review A*, November 1995.

[31] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", *Physical Review A*, Vol. 52, October 1995, pp. 2493 – 2496.

[32] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", manuscript, August 1995.

[33] T. Sleator and H. Weinfurter, "Realizable universal quantum logic gates", *Physical Review Letters*, Vol. 74, 15 May 1995, pp. 4087 – 4090.

[34] J. A. Smolin and D. P. DiVincenzo, "Five two-bit quantum gates are sufficient to implement the quantum Fredkin gate", *Physical Review A*, in press.

[35] A. Steane, "Multiple particle interference and quantum error correction", submitted to *Proceedings of the Royal Society*, London, Series A, 1995.

[36] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi and H. J. Kimble, "Measurement of conditional phase shifts for quantum logic", manuscript, June 1995.

[37] W. G. Unruh, "Maintaining coherence in quantum computers", *Physical Review A*, Vol. 51, February 1995, pp. 992 – 997.

[38] V. Vedral, A. Barenco and A. Ekert, "Quantum networks for elementary arithmetic operations", submitted to *Physical Review A*, 1995.

This article was processed using the LaTeX macro package with LLNCS style