QUANTUM COMPUTING

Paul Vitányi
CWI, Kruislaan, Amsterdam, The Netherlands

Keywords: Quantum computing, entanglement, coherent quantum superposition, quantum interference, reversible computing; miniaturization in computing, heat dissipation, parallel interconnect problem, EPR paradox, EPR pairs, Shor's quantum factoring, Grover's quantum search, quantum, computational complexity, quantum information theory, quantum Kolmogorov complexity, quantum error-correcting codes; decoherence

Contents

Summary

The laws of physics impose limits on increases in computing power. Two of these limits are interconnect wires in multicomputers and thermodynamic limits to energy dissipation in conventional irreversible technology. Quantum computing is a new computational technology that promises to eliminate problems of latency and wiring associated with parallel computers and the rapidly approaching ultimate limits to computing power imposed by the fundamental thermodynamics. Moreover, a quantum computer will be able to exponentially improve known classical algorithms for factoring, and quadratic ally improve every classical algorithm for searching an unstructured list, as well as give various speed-ups in communication complexity, by exploiting unique quantum mechanical features. Finally, a quantum computer may be able to simulate quantum mechanical systems, something which seems out of the

question for classical computers, thus reaching the ultimate goal of replacing actual quantum mechanical experiments with simulated ones. On the downside, for some problems quantum mechanical computers cannot significantly improve the performance of classical computers.

1. Introduction

Apparently, the earliest mention of quantum computing is by Paul Benioff who demonstrated how to implement a classical Turing machine using quantum mechanical processes. In 1982 Richard Feynman raised the question of simulating elementary quantum mechanical systems by computer. A quantum mechanical system with 2^n basis states —for example an n-bit memory —has pure quantum states that consist of a superposition of all of the basis states. Every basis state in this superposition has a probability amplitude (a complex real) that indicates the probability of observing this basis state in an appropriate measurement. To simulate the evolution of such a system, one needs to track the evolution of the 2^n probability amplitude parameters per simulated step. It is not known how to do this classically in time less than exponential in n. To overcome this problem, Feynman suggested to fight fire with fire: A quantum mechanical computer may possibly be able to simulate every quantum mechanical system in polynomial time since it operates on the same principles. In a way this boils down to the time-honored method of analogue computing, where an appropriate model of the simulated system is built —like wind tunnels to test turbulence and experimental simulation of water systems. The next step to digital quantum computing was taken by David Deutsch who defined a quantum mechanical version of the classical Turing machine and in turn raised the question whether such computers could possibly speed up classical digital computations significantly over what is achievable by classical computers. The field attracted some interest but remained esoteric: Problems were formulated that benefited from the quantum mechanical approach but they looked rather contrived. The field gained momentum in 1994 when Peter Shor proposed a fast quantum factoring algorithm. This algorithm (probabilistically) factors a composite l-bit number in slightly over l^2 steps, while the best known classical algorithm, the number field sieve, takes $2^{cl^{1/3}\log^{2/3} l}$ (c constant) steps. The apparent difficulty of factoring composite numbers with only large factors is the basis of almost all commonly used cryptographic systems in financial bank transactions and internet security. The fact that a quantum computer (if it can be build) will compromise such systems galvanized the physics and computer science research communities. A subsequent quantum mechanical algorithmic improvement to searching an unstructured data base excited the interest even further. Apart from some other less straightforward improvements (below), however, these remain the only genuine successes of quantum algorithmics today. Worse, it can be shown that for many problems quantum mechanical methods don't help significantly, like, for example, with binary search. While the jury is still out whether quantum mechanical computing is the greatest thing in computing since the invention of personal computing, it seems evident that the advent of the quantum computer is unavoidable since improvement of computing by parallelizing and further miniaturizing of classical methods runs into problems. The purpose of this writing is to give an outline of the area of quantum computing without going into much detail —a general textbook treatment of both the theory and experimental can be found in the references.

1.1 Wither Classical Computing?

In performance analysis of classical sequential computation such as performed by a Turing machine or a von Neumann architecture computer —the common computer — one can safely ignore many physical aspects of the underlying computer system and analyze the computational complexity of an algorithm or program in a purely logical fashion. One cannot always ignore the reality of the physical world we live in to such an extent. The appropriateness of the analysis may stand or fall with the account taken of physical reality: Non-classical or non-standard physical realizations of computers may have totally unexpected properties, such as, for example, the quantum computer. To see why quantum computing may be the natural next step in computing technology, let us analyze some problems attending the further improvement of classical computing. Two natural ways to improve classical computing are continued miniaturization and large-scale parallelization.

1.1.1 The Cooking Problem

Computers increasingly pervade our society. This increasing influence is enabled by their ever increasing power, which has roughly doubled every 18 months for the last half-century (Moore's law). The increase in power, in turn, is primarily due to the continuing miniaturization of the elements of which computers are made, resulting in more and more elementary gates with higher and higher clock pulse per unit of silicon, accompanied by less and less energy dissipation per elementary computing event. Roughly, a linear increase in clock speed is accompanied by square increase in elements per silicon unit —so if all elements compute all of the time, then the dissipated energy per time unit rises cubically (linear times square) in absence of energy decrease per elementary event. The continuing dramatic decrease in dissipated energy per elementary event is what has made Moore's law possible. But there is a foreseeable end to this: There is a minimum quantum of energy dissipation associated with elementary events. This puts a fundamental limit on how far we can go with miniaturization, or does it?

Both classical and quantum physics are believed to be strictly reversible at the fundamental level: A complete description of the microscopic state of the system uniquely determines the earlier and future states of the system —this holds not only in Newtonian mechanics but for example also for the unitary evolution of every quantum mechanical system. Currently, computations are commonly irreversible, even though the physical devices that execute them are fundamentally reversible. This irreversibility is due to the fact that information tends to be erased all the time: computing a function like $a+b=c$ one inputs a and b and obtains output c. From c one cannot uniquely retrieve a and b. The contrast between the physics of the computing machinery which is reversible and the executed irreversible computation is only possible at the cost of efficiency loss by generating thermal entropy into the environment. With computational device technology rapidly approaching the elementary particle level this effect gains in significance to the extent that efficient operation (or operation at all) of future computers requires them to be reversible. The `logically irreversible' operations in a physical computer necessarily dissipate $kT\ln 2$ energy by generating a corresponding amount of entropy for every bit of information that gets irreversibly erased; the logically reversible operations can in principle be performed dissipation-free. Here k is

Boltzmann's constant and T the absolute temperature in degrees Kelvin, so that $kT \approx 3 \times 10^{-21}$ Joule at room temperature.

Extrapolations of current trends show that the energy dissipation per binary logic operation needs to be reduced below kT (thermal noise) within 15 years. Even at kT level, a future laptop containing 10^{13} gates operating at 100 gigahertz dissipates 3,000 watts. For thermodynamic reasons, cooling the operating temperature of such a computing device to almost absolute zero (to get kT down) must dissipate at least as much energy in the cooling as it saves for the computing.

Especially Landauer has argued that it is only the *irreversible* elementary events (like erasing information) that necessarily dissipate energy; there is no physical law that requires *reversible* events (like negation) to dissipate energy. It has been shown that all irreversible computations can be performed logically reversibly at the cost of possibly increasing computation time and memory. It remains to develop the technology to implement the physical reversible execution of the logically reversible computation in a dissipation-free manner. Reversible computers can be implemented using quantum-mechanical technologies; quantum-mechanical computers are reversible except for the observation phases. So far the development of computation machinery is mostly based on the principles of classical physics and irreversible components. At the basic level, however, matter is governed by quantum mechanics, which is reversible. Further miniaturization will very soon reach scales where quantum mechanical effects take over and classical laws cease to apply accurately. The mismatch of computing organization and reality will express itself in friction: increasingly powerful computers will dissipate increasing and unsustainable amounts of energy unless their mode of operation becomes quantum mechanical (and thus reversible). That is, harnessing quantum mechanical effects may be essential for further miniaturization and hence acceleration of classical computing methods.

There is an added bonus: once we get involved in quantum effects, it appears we can go further than just miniaturizing classical computers to the quantum scale. Quantum mechanics may actually spawn a *qualitatively new* kind of computing: a kind which profits from quantum effects to boost computation to such an extent that things are achieved that would forever be out of reach of classical computers, even if these could be miniaturized to the same level.

1.1.2 The Spaghetti Problem

Parallel computation that allows processors to randomly access a large shared memory, or rapidly access a member of a large number of other processors, will necessarily have large latency. If we use n processing elements of, say, unit size each, then the tightest they can be packed is in a 3-dimensional sphere of volume n. Assuming that the units have no “funny”shapes, assume for example they are spherical, some units are at distance equal to the radius R from one another,

$$R = \left(\frac{3n}{4\pi} \right)^{\frac{1}{3}}$$

Because of the bounded speed of light, it is impossible to transport signals over $n^{\alpha}(\alpha > 0)$ distance in $o(n)$ time. In fact, the assumption of the bounded speed of light says that the lower time bound on *any* computation using n processing elements is linear in $n^{1/3}$ outright.

The *spaghetti* problem is as follows: We illustrate the approach with a popular architecture, say the *binary d-cube*. Recall, that this is the network with $n = 2^d$ nodes, each of which is identified by a d-bit name. There is a two-way communication link between two nodes if their identifiers differ by a single bit. The network is represented by an undirected graph $c = (V, E)$, with V the set of nodes and $E \subseteq V \times V$ the set of edges, each edge corresponding with a communication link. There are $d2^{d-1}$ edges in C. Let C be embedded in 3-dimensional Euclidean space, each node as a sphere with unit volume. The distance between two nodes is the Euclidean distance between their centers.

Lemma 1 *The average Euclidean length of the edges in the 3-space embedding of* C *is at least* $7R/(16d)$.

One can derive a general theorem that gives similar lower bounds that are optimal in the sense of being within a constant multiplicative factor of an upper bound for several example graphs of various diameters. At present, many popular multi-computer architectures are based on highly symmetric communication networks with small diameter. Like all networks with small diameter, also asymmetric ones like complete binary trees, such networks will suffer from the communication bottleneck above, necessarily contain *some* long interconnects (embedded edges). However, the desirable fast permutation routing properties of symmetric networks don't come free, since they require that the average of *all* interconnects is long. Then, the ratio between the volume of the combined processing elements and the required volume of the wires vanishes — even for moderate numbers the processors become needles in a haystack of wires. Here we have not yet taken into account that longer wires need larger drivers and have a larger diameter, that the larger volume will again cause the average interconnect length to increase, and so on, which explosion may make embedding altogether impossible with finite length interconnects. It appears that the "spaghetti" problem too may be resolved —in a fashion —by the inherent parallelism of coherent quantum computation.

-
-
-

Bibliography

A. Ambainis, A better lower bound for quantum algorithms searching an ordered list, *Proc. 40th IEEE Symp. Foundat. Comput. Sci.*, 352--357, 1999. [Gives the currently best lower bounds on the complexity of quantum binary search, within a factor 9 of the known complexity of classical binary search.]

A. Ambainis, Quantum lower bounds by quantum arguments, *Proc. 32nd ACM Symp. Theor. Comput.*, 2000. [Gives a novel method based on quantum mechanical considerations of proving lower bounds on the complexity of quantum computations.]

R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proc. 39th IEEE Symp. Foundat. Comput. Sci.*, 1998, 352--361. [Gives a novel method based on quantum mechanical considerations of proving lower bounds on the complexity of quantum computations.]

C.H. Bennett. Logical reversibility of computation. *IBM J. Res. Develop.*, 17(1973), 525--532. [Shows that every common (irreversible) computation can be performed reversibly; introduces reversible Turing machines, and a universal reversible Turing machine. This is the original paper introducing the mathematical notion of reversible computations and algorithms.]

C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, Experimental quantum cryptography, *J. Cryptology*, 5:1(1992), 3-28; C.H. Bennett, G. Brassard and A. Ekert, Quantum cryptography, *Scientific American*, Oct. 1992, 50-57. [Popular exposition of what has been experimentally achieved on quantum cryptography.]

C.H. Bennett and P.W. Shor, Quantum information theory, *IEEE Trans. Inform. Th.*, IT-44:6(1998), 2724--2742. [A general exposition of quantum information theory and the new quantum error-correcting codes which are vital for the realization quantum computation by maintaining coherent superposition. These codes in a sense form a completion of the classical theory of error-correcting codes, much as the complex numbers are a completion of the real numbers.]

E. Bernstein and U. Vazirani, Quantum complexity theory, *SIAM J. Comput.*, 26:5(1997), 1411--1473. [Original paper defining and exhibiting polynomial time simulation of arbitrary quantum Turing machines by a universal quantum Turing machines, and developing the first complexity theory of quantum computation.]

R. Cleve and H. Buhrman, Substituting quantum entanglement for communication, Physical Review A, 56:2(1997),1201-1204. [Original paper showing that using Einstein-Podolsky-Rosen pairs (entangled qubits) one can reduce classical communication in a distributed computation to below the classical lower bound, even though by the finiteness of the speed of light it is known that EPR pairs cannot be used to communicate information. Thus, quantum communication complexity (in terms of exchanges of classical bits) is shown to be below the proven classical lower bounds by using entangled qubits as resource.]

M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000. [This is the standard reference- and textbook on the subject.]

H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proc. 30th ACM Symp. Theor. Comput.*, 1998, 63--68. Shows that communication complexity using exchanged qubits can be exponentially less than communication complexity in exchanged classical bits, for certain problems in distributedly computing a function.]

L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th ACM Symp. Theor. Comput.*, 1996, 212--219. [Paper that showed for the first time that there is a natural problem on which quantum computers perform faster than is classically possible: searching an unstructured database can be done in a number of quantum operations that is the square root of the number of operations that are classically required. This paper has a considerable spin-off in terms of other problems.]

P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:5(1997), 1484--1509. [Paper that started the quantum computing boom: showed that using quantum computation one can factor an integer in time square in the integers length, whereas every deterministic or randomized classical algorithm that is known requires time exponential in the square root of the length or cube root of the length, respectively. Since virtually all internet security and bank transaction security depend on the (classical) difficulty of factoring numbers consisting of two large prime factors, realization of a quantum computer would compromise all this security---and currently there is no viable alternative.]

P.W. Shor, Introduction to quantum algorithms, http://xxx.lanl.gov/abs/quant-ph/0005003 [Short and simple introduction to quantum computing.]

P. Benioff, J. Stat. Phys., 22(1980), 563--591, also *J. Math. Phys.*, 22(1981), 495--507, *Int. J. Theoret. Phys.*, 21(1982), 177--201, *Phys. Rev. Letters*, 48(1982), 1581--1585, *J. Stat. Phys.*, 29(1982), 515--546, *Phys. Rev. Letters*, 53(1984), 1203, *Ann. New York Acad. Sci.*, 480(1986), 475--486. [Original paper talking about the possibility of quantum mechanical computers, here rather as an quantum mechanical implementation of classical computing, rather than as something that is better.]

D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, B.M. Terhal, Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement, http://xxx.lanl.gov/abs/quant-ph/9908070 [Develops new algebraic theory analyzing until then unknown properties of different forms of quantum entanglement.]

D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Royal Society London, Series A*, 400(1985), 97--117; see also *Proc. Royal Society London, Series A*, 425(1989), 73--90; with R. Josza, *Proc. Royal Society London, Series A*, 439(1992), 553--558. [Series of papers recasting the "analog" quantum computing proposal of Richard Feynman in terms of a "digital" version---the effect being a fundamental switch of paradigm comparable with the classical situation when the digital computer entered the scene asopposed to previously proposed analog computers that had little lasting impact.]

R.P. Feynman, Simulating physics with computers, *Int. J. Theoret. Physics*, 21(1982), 467--488; Quantum mechanical computers. *Foundations of Physics*, 16(1986), 507--531. (Originally published in *Optics News*, February 1985); Tiny Computers Obeying Quantum Mechanical Laws. In: *New Directions in Physics: The Los Alamos 40th Anniversary Volume,*, N. Metropolis and D. M. Kerr and G. Rota, Eds.,Academic Press,, Boston, 1987, 7--25. [Original paper of Feynman proposing quantum mechanical computers exploiting unlimited parallellism in the form of coherent superposition, essentially in the form of analog computing. Feynman's goal was touse such a computer to simulate the evolution of quantum mechanical systems in time polynomial in the number of particles involved (although up to the present time such a simulation method has not been exhibited). Classically, this task seems to require exponential time for every step in the evolution.]

R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Develop.*, 5(1961), 183--191. [Fundamental paper showing that whereas irreversible computation necessarily reduces entropy at the cost of generating heat into the environment (at the level of at least thermic noise energy), it is physically possible in principle to have a reversible computation running without generating heat or using energy at all. This excited interest in reversible computing, of which quantum computation (but for the observation steps) is an example.]

A.K. Lenstra and H.W. Lenstra, Jr. (Eds.), *The Development of the Number Field Sieve*, Lecture Notes in Mathematics, Vol. 1554, Springer-Verlag, Berlin, 1993. [Survey of what is known about algorithms and complexity of factoring integers.]

M. Li and P.M.B. Vitányi, *An Introduction to Kolmogorov Complexity and Its Applications*, 2nd Edition, Springer-Verlag, New York, 1997. [Standard reference and textbook on algorithmic information theory (Kolmogorov complexity): information in individual objects and randomness of individual objects.]

Unruh, W. G., Maintaining coherence in quantum computers, *Physical Review A*, 51(1995), 992--. [Analyzes physical aspects of the problem of maintaining pure quantum superposition in a computation---as required by quantum computing. Some problems are possibly led to rest by the development of quantum error-correcting codes.]

L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, R. Cleve, I. L. Chuang, Experimental realization of order-finding with a quantum computer, http://xxx.lanl.gov/abs/quant-ph/0008065 [Exciting experiment actually implemented the quantum mechanical part of Shor's fast factoring algorithm and showed that it works. Uses five-qubit quantum registers embedded in large molecules containing chloride isotopes subjected to quantum mechanical operations implemented in NMR technology.]

P.M.B. Vitányi, Area penalty for sublinear signal propagation delay on chip, *Proc. 26th IEEE Symp. Foundat. Comput. Sci*., 1985, 197--207. [Examines tradeoff between speed of signal propagation and volume of interconnects (and layout) on chips as required by physics and electromagnetic theory.]

P.M.B. Vitányi, Locality, communication and interconnect length in multicomputers, *SIAM J. Computing, 17 (1988), 659--672.* [Examines the mathematical consequences of the bounded speed of light (and signal propagation) on physical space embeddings of parallel computer architectures, network topologies, and component placement on chip. Low diameter, symmetric, network arrangements aof large number of components are out of the question: this mathematical conclusion has since been evidenced by the demise of large scale parallel classical computer construction efforts.]

P.M.B. Vitányi, Quantum Kolmogorov Complexity Based on Classical Descriptions, *IEEE Trans. Inform. Th., 47(2001)*, September. [Introduces Kolmogorov complexity of quantum states: algorithmic quantum information theory.]

C. Zalka, Efficient simulations of quantum mechanical systems by quantum computers, *Proc. Royal Soc. London, Ser. A*, 454(1998), 313--322. [Some development in Richard Feynman's motivation of introducing quantum computing: to simulate evolution of quantum systems efficiently.]

W.H. Zurek, Decoherence and the transition from quantum to classical, *Physics Today*, 44(1991), 36--44. [Clear account by one of the originators of decoherence theory: how a pure superposition of a quantum state under influence of the remainder of the universe deteriorates (decoheres or collapses) to a classical state. That is why, on the macro level, we perceive the world as classical.]

Biographical Sketch

Paul M.B. Vitányi received his Ph.D. from the Free University of Amsterdam (1978). He holds positions at the national CWI research institute in Amsterdam, and he is Professor of Computer Science at the University of Amsterdam. He serves on the editorial boards of Distributed Computing, Information Processing Letters, Theory of Computing Systems, Parallel Processing Letters, Journal of Computer and Systems Sciences (guest editor), and elsewhere. He has worked on cellular automata, computational complexity, distributed and parallel computing, machine learning and prediction, physics of computation, reversible computation,quantum computation, and algorithmic information theory (Kolmogorov complexity). Together with Ming Li they pioneered applications of Kolmogorov complexity and co-authored ``An Introduction to Kolmogorov Complexity and its Applications," Springer-Verlag, New York, 1993 (2nd Edition 1997), parts of which have been translated into Chinese, Russian and Japanese.