The Promise of Quantum Computing and Quantum Information Theory - Quantum Parallelism (The Abstract of a Tutorial)

Dan C. Marinescu
School of Computer Science
University of Central Florida
Orlando, Fl, 32816
Email: dcm@cs.ucf.edu
http: //www.ucf.edu/ dcm

In 1985 Richard Feynman wrote: "..it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms and quantum behavior holds sway." Quantum properties such as superposition, entanglement, uncertainty, and interference, form the foundation of a new brand of theory, where computational and communication processes rest upon fundamental physics.

Heat dissipation, leakage, and other physical phenomena limit our ability to build increasingly faster solid state devices, while quantum computation holds out the promise to solve efficiently most difficult problems in computational sciences such as simulation of quantum systems, integer factorization, database searching and the computation of discrete logarithms.

In quantum systems an exponential increase in parallelism requires only a linear increase in the amount of space needed. The major difficulty in exploiting quantum parallelism lies in the fact that access to the results of a quantum computation is restricted because measurements disturb the quantum state, a process known as *decoherence*. Eavesdropping on a quantum communication channel can be detected with very high probability. Quantum information theory allows us to design algorithms for dense coding, quantum teleportation, and quantum key distribution.

Quantum computing and communication is a very exciting field. As Feynman said: "A description of the world in which an object can apparently be in more than one place at the same time, in which a particle can penetrate a barrier without braking it, in which widely separated particles can cooperate in an almost psychic fashion, is bound to be both thrilling and bemusing."

"Quantum" is a Latin word meaning "some quantity". Quantum mechanics is a mathematical model of the physical world; the postulates of quantum mechanics: (i) identify the "mathematical universe" for modeling quantum phenomena (as n-dimensional Hilbert spaces with n the maximum number of distinguishable states of the system); (ii) establish a correspondence between a quantum system and its mathematical abstraction (the state of a quantum system is a "ray" in a n-dimensional Hilbert space); (iii) describe the spontaneous evolution of an isolated quantum system (it is a unitary transformation); and tell us (IV) how to represent composite systems (as the tensor product of the Hilbert spaces representing each sub-system) and (V) how to observe a system in this universe (a measurement of a quantum system corresponds to a projection of its state onto orthogonal sub-spaces; the sum of these projections is one).

Quantum information is stored as the state of atomic or sub-atomic particles. A *qubit* is an elementary unit of quantum information. Some of the physical embodiments of a qubit considered today:

- A photon. The information is encoded as the photon polarization.
- An electron. The information is encoded as the spin of the electron.
- Quantum dots. Small devices that contain a tiny droplet of free electrons. The size and shape of these structures and therefore the number of electrons they contain, can be precisely controlled; a quantum dot can have anything from a single electron to a collection of several thousands. Fabricated in semiconductor materials; typical dimensions between nanometres to a few microns. The

Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)
1530-2075/05 $ 20.00 IEEE

information is encoded as the presence/absence of electrons.

- A two-level atom in an optical cavity.
- Two internal states of an ion in a trap.
- Liquid-state NMR (Nuclear Magnetic Resonance).
- NMR spin lattices.
- Macroscopic gas clouds.
- Nitrogen vacancies in diamond.
- Josephson junctions.

Quantum information has special properties: the state of a quantum system cannot be measured or copied without disturbing it; quantum state can be *entangled*, two systems have a definite state though neither has a state of its own; superposition - we cannot reliably distinguish non-orthogonal states of a quantum system.

Decoherence, the randomization of the internal state of a quantum computer due to interactions with the environment, is a major problem in quantum computing. Conceptually, decoherence can be prevented using: (i) quantum fault-tolerant circuits; (ii) quantum error-correcting codes; (iii) entanglement purification and distillation - means to extract a subset of states of high entanglement and high purity from from a large set of less entangled states. Substantial progress should be made in all these areas before quantum computing becomes a reality.

In this tutorial we introduce basic concepts and some of the applications of quantum computing and quantum information theory. We discuss first the physical limitations of solid state technology, then we present a few experiments which reveal quantum effects. We survey the basic principles of quantum mechanics necessary to understand the behavior of quantum devices.

We discuss quantum gates and quantum circuits used to transform the state of a quantum system and thus to process information. Any classical logic circuit can be implemented using only `AND`, `OR`, and `NOT` gates. Similarly, we can simulate any complex n-qubit quantum circuit using a small set of one-qubit gates and `CNOT`s. We present universal quantum gates and show that: (i) Any unitary transformation A on n qubits can be carried out as a product of unitary transformations, U_k, which act only upon two or fewer computational basis states. (ii) Each transformation U_k can be expressed exactly as a product of transformations carried out by one-qubit gates and `CNOT`s. (iii) A transformation carried out by a one-qubit gate can be approximated arbitrarily well by the transformation carried out by the three gates in the set (H, S, T).

In the second part of the tutorial we discuss in some depth the concept of *quantum parallelism.* When we process classical information and we wish to compute all values of a function $f(x)$ of a binary vector x of length n we need either: one copy of the circuit and 2^n time steps (assuming that it takes one time step to compute the value of the function for one argument), or one time step and 2^n copies of the circuit. Due to superposition effects, a single quantum circuit is able to compute all 2^n values of the function in a single time step. The output of the circuit is in a superposition state consisting of all possible values of $f(x)$.

We illustrate quantum parallelism with the example of an "oracle" capable to establish if a binary function is balanced or not (the so-called Deutsch's problem). A necessary but not sufficient condition for a voting machine to function correctly is a practical example of a test to see if a function is balanced or not. Assume you have a voting machine with two input buttons, one for each candidate, and an output display. We press the buttons, one at a time, and examine the results. If the two results are identical the machine is not functioning correctly. If the two results are different the machine may, or may not, function correctly.

We present a quantum circuit for solving Deutsch's problem and illustrate the general strategy to calculate the output of a quantum circuit: (i) decompose the circuit into a number of stages; (ii) calculate the transfer matrix of each stage as the tensor product of the the transfer matrices of the gates transforming each qubit; (iii) calculate the state at the input of the circuit as a tensor product of `ket` vectors (in Dirac's notation) representing the individual states of the qubits; (iv) calculate the state after the first stage as the product of the transfer matrix of the first stage and the input state vector; (vi) repeat previous step for each stage until we obtain the output state.

We outline Shor's algorithm for integer factorization and if time permits discuss concepts from quantum information theory, and provide some insights into dense coding, and quantum teleportation.

The potential impact of quantum computing and quantum information theory is astounding. Reversible quantum computers avoid logically irreversible operations and can, in principle, dissipate arbitrarily little energy for each logic operation. By contrast, solid state devices vintage year 2000 require some 3×10^{-18} Joules/switching operation. In 1992, Ralph Merkle from Xerox PARC calculated that a 1 GHz computer operating at room temperature, with 10^{18} gates packed in a volume of about 1 cm^3 would dissipate 3 MW of power. The power dissipation of solid state devices increases with the cube of the clock rate; when we double

Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)
1530-2075/05 $ 20.00 IEEE

the speed of a device, its power dissipation increases 8 (eight) fold.

To exploit the immense power of a quantum computer we need to develop quantum algorithms. In 1944, Peter Shor found a polynomial time algorithm for the factorization of n-bit numbers on quantum computers. The algorithm reduces the integer factorization problem to *order finding* which, in turn, requires an an algorithm for *phase estimation*. Simon's algorithm for phase estimation uses *Quantum Fourier Transform* (QFT). In 1996, Grover described a quantum algorithm for searching an unsorted database containing N items in a time of order $\sqrt{N}$ while on a classical computer the search requires a time of order N. The speedup is achieved by exploiting both quantum parallelism and the fact that in quantum theory a probability is the square of an amplitude. In Grover's algorithm all N strings are represented with an amplitude $1/\sqrt{N}$. Then the initial state is rotated in order of $\sqrt{N}$ steps to a state in which the string we search for is represented with an amplitude of order one. In 1997, Charles Bennett showed that Grover's algorithm is optimal. No quantum algorithm can solve this problem faster than time of order $\sqrt{N}$.

Only few quantum algorithms have been discovered so far and even from our succinct presentation of quantum algorithms it should be clear why; quantum computing requires a substantial adjustment to our way of thinking. Quantum effects are counterintuitive; we need to understand the physics and be familiar with the sophisticated mathematical apparatus of quantum mechanics. We should also ponder how to educate our students and allow them to contribute to the development of this exciting field.

The roadblocks on the way to quantum computing are staggering. The immense costs to develop quantum computers could only be justified if new quantum algorithms and applications of quantum computing and communication are discovered. The discovery of new algorithms and applications of quantum computing requires computer scientists to play an increasingly more significant role in this interdisciplinary research field. Stronger interactions of computer scientists with theoreticians and experimentalists in several areas of physics would help accelerate the progress in the field of quantum computing and quantum information theory.

Virtually all major funding agencies support research in quantum computing and quantum information theory. More information regarding the state of the art, as well as the open problems in this exciting discipline, can be found in an April 2004 document produced by a team of experts in the field: "A Quantum Information Science and Technology Roadmap" (http://qist.lanl.gov).

In the preface of our book *Approaching Quantum Computing* we write: "...we are years, possibly decades, away from building a quantum computer requiring little, if any power at all, filling up the space of a grain of sand, and computing at speeds that are unattainable today even by covering tens of acres of floor space with clusters made from tens of thousands of the fastest processors built with current state of the art solid-state technology. All we have at the time of this writing is a seven-qubit quantum computer capable of computing the prime factors of a small integer, 15. To break a code with a key size of 1024 bits requires more than 3000 qubits and 10^8 quantum gates."

Biographical Sketch. Dan C. Marinescu joined the Computer Science Department at University of Central Florida in August 2001 as Professor of Computer Science. He has been an Associate and then Full Professor of Computer Science at Purdue University, in West Lafayette, Indiana, since 1984. He is the Interim Director of the I^2Lab, an organization supporting interdisciplinary research in computer and information sciences (http://I2lab.ucf.edu) at UCF.

He is conducting research in parallel and distributed systems, computational biology, ubiquitous computing, and Petri nets and has published more than 160 papers in journals and referred conference proceedings in these areas. He is the author of "Internet-Based Workflow Management: Towards a Semantic Web," published by Wiley in 2002 and has co-edited "Process Coordination and Ubiquitous Computing." The book "Approaching Quantum Computing," co-authored with Gabriela M. Marinescu was published in September 2004 by Prentice Hall.

Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)
1530-2075/05 $ 20.00 IEEE