Quantum Algorithms for Modeling and Simulation: A Grand Challenge for Modeling and Simulation

Thomas L. Clarke
Institute for Simulation and Training
University of Central Florida
3280 Progress Drive, Orlando, FL 32826
tclarke@ist.ucf.edu (407)882-1327

D. J. Kaup
Mathematics Department
University of Central Florida
Orlando, Florida 32816-1364
kaup@mail.ucf.net

Keywords: quantum computing, Markov model, linear logic, algorithm, game theory

ABSTRACT

The end of the wild computational sleigh ride of Moore's Law is the basis for this grand challenge. The doubling of computing performance every 18 months predicted by Moore's law nearly 50 years ago will soon end. The number of active atoms in a computational device reduce to "one" sometime between 2010 and 2020. Barring some unforeseen invention, this is the end of the road for the current approach. But the problem suggests the solution; atoms are inherently quantum by nature and use of quantum effects in computation provides another route to increased computational power.

Quantum computers require very different algorithms and the grand challenge for modeling and simulation is to develop simulation algorithms adapted to the coming era of quantum computing. In a few years of research, quantum algorithms for searching and factoring large numbers have already been found. Applying these ideas to simulation and developing quantum algorithms specifically for simulation is the challenge.

If quantum algorithms are not developed for modeling and simulation, modeling and simulation will never be able to make use of the exponential power provided by the quantum computer, and the end of Moore's Law will determine the maximum speed of modeling and simulation computation. Many modeling and simulation problems ranging from terrain correlation and intervisibility, to solving nonlinear differential equations, could certainly make use of effective quantum algorithms, if they can be developed.

INTRODUCTION

Simulation should pay close attention to developments in quantum computation. Where simulation has ridden the exponential growth in computer power described by Moore's Law [Clarke, 1995], quantum computation researchers believe a truly quantum computer will provide an unprecedented leap forward in ability to compute [Bennet, 1995]. This "quantum leap" in computational ability may be necessary before one can hope to implement truly intelligent "computer generated forces". But in any case, it will provide greater capability to simulate processes of all varieties [Lloyd, 1995]. There are also interesting connections between quantum computation and other logic and computational paradigms [Clarke, 1998].

There are many possible approaches to the actual implementation of quantum computers. However, the only approach to date that has actually resulted in a quantum mechanical computation, is quantum computation based on nuclear magnetic resonance technology (as in MRI scanners). The Stanford-Berkeley-MIT-IBM Quantum Computation Research Project and others are actively pursuing the possibility of using the precession of atomic nuclei in magnetic fields [Gershenfeld and Chuang, 1998]. The precession and rotation of nuclei can be described by quantum mechanics, so with the proper manipulation and measurement procedures, quantum computation could be achieved.

In brief, quantum computation operates by utilizing qbits (quantum bit) instead of bits. A qbit is the state of a quantum entity like a nuclear spin that generally can be regarded as neither true or false, but as a combination, a superposition, of both. According to quantum mechanics, since 1925 it has been generally accepted that a quantum system is in a superposition of states, and only becomes fixed in any one state when it is measured. Properly utilizing this strange but true fact of nature would enable the quantum computer to simultaneously execute both branches of a conditional, and thereby potentially enormously expanding the power of a quantum computer.

SURVEY OF QUANTUM SIMULATION

In this section some recent articles pertaining to the use of quantum computation in simulation will be discussed along.

Game Theory

Training simulation uses computer generated force (CGF) software to provide challenging exercises to the trainee. It is essential that CGF behavior be realistic but not predictable. Game theory can provide a rational basis for CGF, but avoiding predictability can be a problem. Some of the most elegant applications of quantum computing have been to game theory, and a quantum game may provide just the unpredictably rational behavior needed for a CGF. Quantum games are small problems and have already been implemented on available quantum computing hardware so a quantum CGF may be a relatively near term possibility.

The first paper on quantum games the author is aware of is "Quantum Strategies" by David Myer [1999]. In this article the redoubtable Captain Picard of the Enterprise is pitted against his nemesis Q in the traditional game of matching pennies. As might be expected Picard is limited to a classical strategy whereas Q can employ a quantum strategy. Perhaps not surprisingly, a quantum strategy can beat even an optimal classical strategy. Myer [2000] has since gone on to show how the concept of quantum game against a classical player can be viewed as a quantum algorithm for an oracle. He formalizes this correspondence and gives examples of games (and hence oracle problems) for which the quantum player can do better than would be possible classically.

Since the introduction of the ideas of quantum games and quantum strategies the ideas have been taken in several directions. A recent comprehensive article is that by Eisert and Wilkens [2000] who study quantum games with classical analogs in order to highlight the peculiarities of quantum games, giving special emphasis to a detailed investigation of different sets of quantum strategies. Piotrowski and Sladkowski [2001] apply quantum-like descriptions to the analysis of markets and economics. Their paper focuses on quantum bargaining games, which are a special class of quantum market games without institutionalized clearinghouses.

Dynamical Computation

Feynman's early work on quantum computation was motivated by the difficulty of solving the dynamical equations of quantum mechanics. Simulating a quantum system on a classical computer is exponentially hard, but relatively easy (and in fact, natural) on a quantum computer. There is thus a natural match between quantum computation and quantum dynamical computation. Several recent papers have explored these applications and the authors believe that quantum computers will prove useful for solving propagation problems by making use of the correspondence between the parabolic wave equation and the Schrodinger equation. The utility of inverse scattering transforms for soliton problems, also suggests that quantum computers will be extremely useful for soliton and nonlinear wave problems.

In "Efficient Quantum Computing of Complex Dynamics" Benenti et al [2001] propose a quantum algorithm which optimally uses qubits to efficiently simulate a physical model described by the quantum sawtooth map. This model has rich and complex dynamics, which is accurately reproduced up to a time scale which is polynomial in the number of qubits. However, the authors find that the errors generated by static imperfections in the quantum computer hardware to be more dangerous than the errors of random noise in gate operations.

Searching

Grover's $O(\sqrt{n})$ search algorithm is one of the big two quantum algorithms that spurred interest in quantum computing. It is also one of the few quantum algorithms that has been executed on hardware to date. Since Grover's discovery of the algorithm, it has been generalized in many directions. Set into the simulation context, Grover's algorithm should find use in calculating visual primitives in graphics system. For example, the intervisibility predicate is essentially a search for objects that are visible. Within the graphics hardware, hidden line removal can also be cast as a search. When quantum hardware becomes generally available, visual simulation should thus greatly benefit.

Murphy [2001] has looked at the generalizations for searching over structured databases, such as are found in graphics systems. Murphy presents an algorithm for structured database searching and uses it to solve the set partition problem. $O(n)$ oracle calls are required in order to obtain a solution, but the probability that this solution is optimal decreases exponentially with problem size. Since each oracle call is followed by a measurement, it is only necessary to maintain quantum coherence for one oracle call at a time.

Factoring

Factoring large composite numbers is a key application of quantum computing. The basis of the algorithm was outlined above. With the promise of cracking public keys and other cryptographic codes, Shor's discovery of an algorithm that can factor numbers in polynomial time was what spurred the current interest in quantum computing.

For simulation, it is the techniques that led to Shor's factoring algorithm rather than Shor's factoring algorithm that should prove to be significant. These techniques include notably the quantum Fourier transform whose applications are explored in more detail in the section on signal processing. For the interested reader, a few recent references to recent extensions of Shor's ideas are

mentioned below. Lomanco [2000] is a compact introduction to Shor's algorithm.

Signal Processing

Richard Jozsa [1997] describes the quantum algorithms of Deutsch, Simon and Shor, in a way which highlights their dependence on the Fourier transform. The general construction of the Fourier transform on an Abelian group is outlined and this provides a unified way of understanding the efficacy of these algorithms. He also describes an efficient quantum factoring algorithm based on a general formalism of Kitaev, and contrasts its structure to the ingredients of Shor's algorithm.

Hales and Hallgren [1999] isolate and generalize a technique implicit in many quantum algorithms, including Shor's algorithms, for factoring and discrete log (the discrete log of h base g is an integer x such that $g^x = h$). In particular, they show that the distribution sampled after a Fourier transform over $\boldsymbol{Z}^p$ can be efficiently approximated by transforming over $\boldsymbol{Z}^q$ for any q in a large range. Their result places no restrictions on the superposition to be transformed, generalizing the result implicit in Shor's work, which applies only to periodic superpositions. In addition, their proof easily generalizes to multi-dimensional transforms for any constant number of dimensions.

Simulation

Work in this section is distinctly different from the use of quantum computers to dynamically model physical systems, mentioned above. These simulations below are aimed at mathematical applications and modeling discrete systems. When quantum computers become practical, these types of simulations should find use in control and AI applications.

Obenland and Despain [1998] describe a parallel simulator, which accesses the feasibility of quantum computers. They also derive and validate an analytical model of execution time for the simulator, which shows that parallel quantum computer simulation is very scalable.

Tucci [2000] proposes a new family of quantum computing algorithms, which generalize the Deutsch-Jozsa, Simon and Shor ones. The goal of his algorithms is to estimate conditional probability distributions. Such estimates are useful in applications of Decision Theory and Artificial Intelligence, where inferences are made based on uncertain knowledge. The family of algorithms that he proposes is based on a construction method that generalizes a Fredkin-Toffoli (FT) construction method used, in the field of classical reversible computing. FT showed how, given any binary deterministic circuit, one can construct another binary deterministic circuit which does the same calculations in a reversible manner. Tucci shows how, given any classical stochastic network (classical Bayesian net), one can construct a quantum network (quantum Bayesian net) which can perform the same calculations as the classical one, but in a (piecewise) reversible manner. Thus, he extends the FT construction method so that it can be applied to any stochastic circuit, not just binary deterministic ones.

Carlini and Hosoya [2000] present a quantum version of the classical probabilistic algorithms *a la* Rabin. The quantum algorithm is based on the essential use of Grover's operator for the quantum search of a database and of Shor's Fourier transform for extracting the periodicity of a function, and their combined use in the counting algorithm originally introduced by Brassard et al. One of the main features of their quantum probabilistic algorithm is its full unitarity and reversibility, which would make its use possible as part of larger and more complicated networks in quantum computers. As an example of this, they describe polynomial time algorithms for studying some important problems in number theory, such as the test of the primality of an integer, the so called 'prime number theorem' and Hardy and Littlewood's conjecture about the asymptotic number of representations of an even integer as a sum of two primes.

RESEARCH at UCF

At UCF we have been struck by some parallels between the structure of quantum computation, and the mathematics developed for modeling and simulation in other domains. The parallels that have been most deeply explored are in the areas of logic and hidden Markov modeling, and are briefly discussed in what follows.

Linear logic, since its introduction by Girard [1987], has proven expressive and powerful. Linear logic has provided natural encodings of Turing machines, Petri nets and other computational models. Linear logic is also capable of naturally modeling resource dependent aspects of reasoning. Wave logic was first described by Orlov in 1978. Related to quantum logic, wave logic has not yet found wide application. Two theorems detailing the reduction of the logics, one to the other, have been proved. Lie groups provide the connection between the exponential modal storage operators of linear logic and the eigenfunctions of wave logic.

One of the more successful approaches to speech recognition is the use of hidden Markov models (HMM). In brief a HMM assumes that the speech signals are functions of the states of an unobservable Markov process. The formalism of quantum mechanics can in some ways be viewed as a complex-valued hidden Markov model. A quantum system is described by a unit-length vector in an Hilbert space. Hilbert space can be thought of as a complex-valued vector space with the usual vector and operator (think of matrix) operations. The space may be

infinite-dimensional but for purposes here, can be thought of having *n* dimensions, so that the state vector is $\psi? = (z_1,...z_n)$, where z_i is a complex number.

There is thus a clear analogy between the Hilbert space mathematics of quantum mechanics and the probabilistic mathematics of hidden Markov models. Both are characterized by a unobservable state that evolves according to a matrix (*A* in HMM, *U* in complex HMM). The state is manifest through a random observation process: the functions *B* for HMM and the operator Φ for quantum mechanics.

While the Vitterbi algorithm used for solving hidden Markov models can be formally translated into a complex form, it is not clear that this is the best approach. While there are many similarities between HMM and its quantum-like complex generalization, there are also many differences. Time in quantum mechanics is inherently continuous, whereas it is discrete in Markov modeling; continuous time in the form of variable state durations can only be incorporated with some difficulty into HMMs. The restrictions on the unitary matrix *U* are much milder than those on the Markovian matrix *A*.

REFERENCES

Bennet, C. H. (1995) "Quantum Information and Computation" *Physics Today*, Vol. 48, No. 10, pages 24-30; October 1995.

Benenti, G. Casati, G., Montangero, S., and Shepelyansky, D.L. (2001) "Efficient Quantum Computing of Complex Dynamics" http://xxx.lanl.gov/abs/quant-ph/0107036

Carlini, A. and Hosoya, A. (1999) "Quantum Probabilistic Subroutines and Problems in Number Theory" *Report-no: TIT/HEP-426/COSMO-94* http://xxx.lanl.gov/abs/quant-ph/9907020

Clarke, T.L. (1998) "A Comparison of Linear Logic with Wave Logic" *Fifth International Symposium on Artificial Intelligence And Applied Mathematics*

Clarke, T. L. (1998); "Superregenerative Quantum Neural Computation" *ICCIN 98 Conference.*

Clarke, T.L. (1998) "Simulation's Ultimate Challenge", *I/ITSEC 1998.*

Eisert, J. and Wilkens, M. (2000) "Quantum Games" *J. Mod. Opt. 47* 2543 http://xxx.lanl.gov/abs/quant-ph/0004076

Gershenfeld, N. and Chuang, I.L. (1998) "Quantum Computing with Molecules" *Scientific American*, Vol 276, No 6.

Girard, J.Y., (1987) "Linear Logic" *Theoretical Computer Science*, 50:1-102, 1987.

Hales, L. and Hallgren, S. "Sampling Fourier Transforms on Different Domains" (1998) http://xxx.lanl.gov/abs/quant-ph/9812060

Jozsa, R. (1997) "Quantum Algorithms and the Fourier Transform" *Proceedings of Santa Barbara Conference on Quantum Coherence and Decoherence*, http://xxx.lanl.gov/abs/quant-ph/9707033

Lloyd, S. (1995) "Quantum-Mechanical Computers," *Scientific American*, *Vol. 273, No. 4*, pp.140-145.

Lomonaco, S.J. Jr (2000) "Shor's Quantum Factoring Algorithm" http://xxx.lanl.gov/abs/quant-ph/0010034

Meyer, David A. (2000) "Quantum games and quantum algorithms" *AMS Contemporary Mathematics volume: Quantum Computation and Quantum Information* http://xxx.lanl.gov/abs/quant-ph/0004092

Meyer, D.A. (1999) "Quantum strategies" *Phys.Rev.Lett. 82* (1999) 1052-1055 http://xxx.lanl.gov/abs/quant-ph/9804010

Obenland, K.M. and Despain, A.M. (1998) "A Parallel Quantum Computer Simulator" *Presented at High Performance Computing 1998*, http://xxx.lanl.gov/abs/quant-ph/9804039

Piotrowski, E. W. and J. Sladkowski (2001) "Quantum Bargaining Games" http://xxx.lanl.gov/abs/quant-ph/0106140

Salgado, D. and Sanchez-Gomez, J.L. (2001) "QSES's and the Quantum Jump" *Proceedings of the 3rd Workshop on Mysteries, Puzzles and Paradoxes in Quantum Mechanics, Z. Naturforsch. 56a* pp.228-229 http://xxx.lanl.gov/abs/quant-ph/0106116

Shor, P.W. (1994) "Algorithms for Quantum Computation: Discrete Logarithms and Factoring" *35th Annual Symposium on Foundations of Computer Science, IEEE*, pp.124-134.

Tucci, R.R. (2000) "Quantum Computer as an Inference Engine" http://xxx.la