A survey of quantum computing and automata

Elise de Doncker and Laurentiu Cucos
Department of Computer Science,
Western Michigan University,
Kalamazoo, MI 49008
{elise,lcucos}@cs.wmich.edu

ABSTRACT

In this paper we highlight important events in the development of quantum computing. Quantum parallelism, entanglement and interference underlie the computational model. We focus on the quantum finite state automaton as a special case and study its relevance in comparison with the classic finite state automata.

Keywords: quantum computing/algorithms, probabilistic/quantum finite state automata, NMR experiments.

1. BACKGROUND

We set out to give a brief review of quantum computing, from a theoretical and experimental point of view, starting with the important events in physics that generate today's discussion. In the 1920s, Bohr and Heisenberg's work lead to the interpretation that the (sub)atomic level is "a world of probabilities and potentialities rather than one of things and facts"[23]. While the Copenhagen interpretation abolished the notion of an independent "quantum reality", in favor of nonlocality or "action at a distance", Einstein challenged the quantum theory with a hypothetical experiment known as the EPR experiment [10]. The experiment was reformulated by John Bell based on a modification by David Bohm. In 1964, Bell's theorem [2] pointed to the existence of quantum correlations larger than the corresponding bound imposed by local reality assumptions, and which could hopefully be discerned experimentally. Subsequent experimental results have largely supported the nonlocal assumptions, even though critics have attempted to find loopholes in the experiments.

Not unlike our classical, local reality model is well-defined according to our perception, so is our classical computational model underlying today's computers. In order to increase the power of our current computers, engineers have increased the clock frequencies and shrunk the size of the silicon gates. It is conceivable that before long, the transistors will be so small and the wavelengths so short, that classical logic will be inadequate for their implementation.

2. QUANTUM COMPUTATION MODELS

A quantum system is in a superposition of configurations, each associated with a certain probability, and to which it may collapse as a result of measurement. Benioff [4] and Feyman [12] introduced the idea of a computation device based on quantum dynamics. Deutsch [8] described a universal quantum computer which he showed capable of "perfectly simulating any finite, realizable physical system". The universal quantum computer is thus compatible with his "physical version of the Church-Turing principle", which states that every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means. It is further noted that this version is not equivalent with the original Church-Turing thesis; in fact it is not satisfied by the universal Turing machine, since the possible states of a classical system form a continuum.

Quantum computation has a natural parallelism embedded in it. At each computation step, the quantum computer is in a superposition of configurations computed in parallel. Quantum computations may obtain deterministic results though interference, whereby some answers become more likely than others [24].

3. QUANTUM ALGORITHMS

More recent research has revealed highly efficient algorithms for quantum computers. Shor [30, 11] used a hypothetical quantum computer to solve the integer factoring problem in polynomial time (specifically, $\mathcal{O}(N^2 \log N \log\log N)$), whereas the best known algorithm on a classical computer is exponential in N (where N is the number of bits in the representation of the integer). The implications of Shor's factoring algorithm generate concern for the current cryptosystems, which are based on the general assumption that the factoring time required to break a security key is exponential in number of digits used. A 100 digits key requires billions of years of computation on a classical computer. The quantum implementation of Shor's algorithm reduces the time to a feasible range.

Grover [15] designed a search algorithm that requires $\mathcal{O}(\sqrt{N})$ steps to search an unsorted database of N records. Recently Grover's algorithm has also been used to explain genetic code [25].

A significant amount of research is being done on the subject of computational complexity from a quantum computation point of view (see, e.g., [32, 1, 3, 5]).

4. FINITE AUTOMATA

Classically, abstract machines/ models (such as Turing machines) have provided a basis to study computational power. Restricted models have been used to gain insight in particular aspects of computation, such as Two-way Probabilistic Finite Automata and Interactive Proof Systems to study randomization [9]. Note also the relevance of IPS to cryptography.

We focus on an analysis of machine power from the restricted point of view of Finite Automata. Common to the definitions of these machines are a finite set of states $S = \{s_0, s_1, \ldots, s_n\}$, a finite set of symbols (alphabet) Σ, an initial state $s_0 \in S$, and a set of final states $F \subseteq S$. From an input tape which contains strings from Σ^*, one symbol is read at a time, and the machine's read head advances either in one direction, or in two directions for two-way machines.

A DFA over alphabet Σ is a system $M = \langle S, \Sigma, \mathcal{T}, s_0, F\rangle$ where $\mathcal{T}$ is the transition function from $S \times \Sigma$ to S, such that if the system is in state s_i and the input is σ then the system will transfer to state s_j. DFA accept the regular languages. Rabin [27] and Shepherdson [29] proved that 2DFA are reducible to DFA; they accept the regular languages.

A One-way Probabilistic Finite Automaton (1PFA) over alphabet Σ is a system $M = \langle S, \Sigma, \mathcal{T}, s_0, F\rangle$ where $\mathcal{T}$ is a function from $S \times \Sigma$ to $[0, 1]^{n+1}$, which gives the probabilities of transition from a state s on input σ to all other states. For $(s, \sigma) \in S \times \Sigma$, $\mathcal{T}(s, \sigma) = (p_0(s, \sigma), \ldots, p_n(s, \sigma))$, where $p_i(s, \sigma)$ represents the probability of moving to state s_i, so $0 \leq p_i(s, \sigma) \leq 1$, and $\sum_{i=0}^{n} p_i(s, \sigma) = 1$ [28]. The DFA can be considered a special case of the 1PFA, with $p_i(s, \sigma) = 1$ for one value of i and 0 for all the other ones. 1PFA are more powerful than DFA in that they recognize certain nonregular languages. Denoting the probability of acceptance of string $x \in \Sigma^*$ by $p(x)$, $T(M, \lambda) = \{x \in \Sigma^* | \lambda < p(x)\}$ is defined as the set of strings accepted by M with cut-point λ $(0 \leq \lambda < 1)$, Rabin [28] gives a machine M for which there exist λ such that $T(M, \lambda)$ is not regular. If λ is rational, then $T(M, \lambda)$ is regular.

λ is an isolated cut-point with respect to M if there exists an $\varepsilon > 0$ such that $|p(x) - \lambda| \geq \varepsilon$. It is shown that in the latter case there is a DFA accepting the language $T(M, \lambda)$; furthermore, in the reduction of 1PFA to DFA, the minimal DFA may need more states than the corresponding 1PFA [28]. Acceptance with isolated cut-point is equivalent to bounded error recognition.

A Two-way Probabilistic Finite Automaton (2PFA) has a probabilistic control and a two way read head. 2PFA with isolated cut-point are referred to as 2BPFA [21]. It is shown in [17] that 1PFA and 2PFA, with all real or all rational transition probabilities, accept the same classes of languages. As the language $\{a^n b^n | n \geq 0\}$ is accepted by a 2BPFA [13], the class of languages accepted by 2BPFA is larger than that of the 1PFA with isolated cut-point.

In [9] it is further shown that a 2PFA recognizing a non-regular language (with bounded error probability) must use exponential expected time (for infinitely many inputs). Bounded error, polynomial expected time 2PFA are known to recognize only regular languages.

An Interactive Proof Systems (IPS) for membership in a language L is a two-party protocol whereby a prover convinces a verifier that that elements $x \in L$ are actually in L [9]. IPS are interesting if they allow the verifier to determine something that it cannot determine on its own. Different versions of IPS with 2BPFA verifier include IPS(2BPFA,public) and IPS(2BPFA,private) according to whether or not the random choices of the verifier are made known to the prover. The results of [9] include that IPS(2BPFA,public) $\subset$ IPS(2BPFA,private), i.e., IPS(2BPFA,private) are more powerful (where the inclusion remains proper if the verifier runs in polynomial expected time); and that IPS(2BPFA,public) are more powerful than 2BPFA.

Using the definition of [19], a Two-way Quantum Finite Automaton (2QFA) over Σ is a system $M = \langle S, \Sigma, \Gamma, \mathcal{T}, s_0, F_{acc}, F_{rej} \rangle$, where $F_{acc} \subset S$ is a set of accepting states, $F_{rej} \subset S$ is a set of rejecting states, $F_{acc} \cap F_{rej} = \emptyset$, $F_{acc} \cup F_{rej}$ consists of halting states and $S - (F_{acc} \cup F_{rej})$ of non-halting states. $\Gamma = \Sigma \cup \{\$, \cent\}$ is the tape alphabet, where \$ and $\cent$ ($\notin \Sigma$) are used as left and right end markers on the input tape. The transition function $\mathcal{T} : S \times \Gamma \times S \times \{-1, 0, 1\} \rightarrow \mathcal{C}$ is such that $\mathcal{T}(s, \sigma, s', d)$ represents the amplitude with which the machine M currently in state s and scanning symbol σ changes its state to s' and moves the tape head to the next symbol in the direction of d.

The tape (of length n) of the 2QFA is considered circular, so that its contents is described by a mapping $x : \mathcal{Z}_n \rightarrow \Gamma$ (referred to as a tape), and the set of configurations $C_n = S \times \mathcal{Z}_n$. A superposition of M on tape x is a mapping from C_n to $\mathcal{C}$ of norm 1, which belongs to the Hilbert space $\mathcal{H}_n = \ell_2(C_n)$. An element $|\Psi\rangle \in \mathcal{H}_n$ can be expressed as a linear combination of the basis vectors $|c\rangle$ where, for each $c \in C_n$, $|c\rangle$ denotes the mapping which is 1 at c and 0 otherwise. Then $|\Psi\rangle = \sum_{c \in C_n} \alpha_c |c\rangle$, where α_c is the amplitude associated with c. The transition function of M determines the amplitudes in the time evolution result of a configuration $|c\rangle = |s, k\rangle$. The time evolution result of a superposition $|\Psi\rangle$ is obtained through linearity. Note that the evolution operator is unitary.

Since bounded error, polynomial expected time 2PFA are known to accept only the regular languages [9], and 2QFA were shown in [19] to recognize the language $\{a^m b^m | m \geq 1\}$ (with one-sided bounded error) in linear time, 2QFA are more powerful than their 2PFA analogues.

One-way Quantum Finite Automata (1QFA) are defined similar to 2QFA, but with a one-way tape head (d fixed). 1QFA are less powerful than DFA, since they are unable to recognize all regular languages [19].

5. EXPERIMENTS

There have been three directions for the development of a quantum computer in the laboratory. Those use a) ion traps, b) optical cavities or c) Nuclear Magnetic Resonance (NMR). Using NMR, a number of experiments have successfully carried a computation. In short, an NMR machine uses nuclear magnetic spin orientation for encoding qubits (a qubit or quantum bit is the quantum unit of information). Spins "interact" with one another, via quantum entanglement and interference. The computation step is performed by applying a strong magnetic field to a mixture of atoms that have known spin values. The new spin state yields the result.

In 1998, Chuang et al. [6] developed a two qubit computation device that uses NMR to determine global properties of an unknown function in fewer steps than a classical computer. They used atoms of H^1 and C^{13} in a solution of $CHCl_3$. Using NMR, Laflamme [20] built a computer using three quantum bits. More recently, Marx et al. [22] demonstrated a 5-qubit NMR quantum computer. Knill et al. [18] established an algorithmic benchmark and its experimental realization based on NMR, which involves coherent manipulation of 7 qubits. It has been estimated that currently NMR techniques can be applied for machines of up to 10-15 qubit states.

The main problems in developing quantum computers involve quantum decoherence and result reading errors. Theoretical progress has been made by the introduction of error correction codes, whereby each qubit is encoded redundantly (and entangled) with a number of qubits [31, 26]. Shor has determined allowable bounds for the error probability per computation step. Cory [7] set up an experiment to prove that quantum error correction can be achieved.

6. CONCLUSIONS

Our survey presents the evolution of ongoing research on building quantum computation models and machines. As a result of that research, the theory of computation has been enriched with principles that originated in quantum mechanics.

Even though we are still far from building a quantum desktop computer, the established power of the new model as well as the preliminary experimental results give motivation to hope that this will lead to a new computational era.

References

[1] L. M. Adelman, J. Demarrais, M.-D. A. Huang, "Quantum computability", SIAM J. Comput., Vol. 26 (5), 1524-1540, 1997.

[2] J. Bell, "On the Einstein Podolsky Rosen Paradox", Physica, 1964.

[3] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, "Strengths and weaknesses of quantum computing", SIAM J. Comput., Vol. 26 (5), 1510-1523, 1997.

[4] P. Benioff, "The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines", J. Stat. Phys., Vol. 22, 1980.

[5] E. Bernstein, U. Vazirani, "Quantum Complexity Theory", SIAM J. Comput., Vol. 26 (5), 1411-1473, 1997.

[6] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, S. Lloyd, "Experimental realisation of a quantum algorithm", Nature, Vol. 393, 143, 1998.

[7] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, S. S. Samaraoo, "Experimental quantum error correction", Physical Review Letters, 81, 2152-2155, 1998.

[8] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", Proc. of the Royal Society A, Vol. 400, 97-117, 1985.

[9] C. Dwork, L. Stockmeyer, "On the Power of 2-Way Probabilistic Finite State Automata", Proc. of the 30th Annual Symposium on Foundations of Computer Science, 480-485, 1989.

[10] A. Einstein , B. Podolsky, N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", Physical Review, Vol. 47, 777-780, 1935.

[11] A. Ekert and R. Jozsa, "Shor's quantum algorithm for factorizing numbers", Rev. Mod. Phys., Vol. 68, 733-753, 1996.

[12] R. P. Feynman, "Simulating physics with computers", International Journal of Theoretical Physics, Vol. 21, 467-488, 1982.

[13] R. Freivalds, "Probabilistic two-way machines", Proc. MFCS, Lecture Notes in Computer Science, Springer-Verlag, New York, Vol. 118, 33-45, 1981.

[14] A. G. Greenberg and A. Weiss, "A lower bound for probabilistic algorithms for finite state machines", J. Comput. Syst. Sci., Vol. 33, 88-105, 1986.

[15] L. Grover, "A fast quantum mechanical algorithm for database search", Proc. of the 28th Annual ACM Symposium on the Theory of Computing 212-219, 1996.

[16] D. R. Hofstadter, "Gödel, Escher, Bach: An eternal golden braid", Vintage books, 1979.

[17] J. Kaneps, "Stochasticity of the languages recognizable by 2-way finite probabilistic automata, Diskret. Mat., 1, 63-77.

[18] E. Knill, R. Laflamme, R. Martinez and C. H. Tseng, "An algorithmic benchmark for quantum information processing", Nature, Vol. 404, 368-370, 2000.

[19] A. Kondacs, J. Watrous, "On the power of quantum finite state automata", Proc. of 38th Annual Symposium on the Foundations of Computer Science, 66-75, 1997.

[20] R. Laflamme, E. Knill, W. H. Zurek, P. Catasti, S. V. S. Mariappan, "NMR GHZ", quant-ph/9709025, 1997.

[21] I. I. Macarie, "Space-efficient deterministic simulation of probabilistic automata", SIAM J. Comput., Vol. 27 (2), 448-465, 1998.

[22] R. Marx, A. F. Fahmy, J. M. Myers, W. Bermel and S. J. Glaser, "Realization of a 5-bit NMR quantum computer using a new molecular architecture", quant-ph/9905087, at url http://xxx.lanl.gov

[23] W. Heisenberg, "Physics and Philosophy", Harper Torchbooks, New York, 1962.

[24] C. Paquin, "Computing in the quantum world", preprint 1998, at url http://www.iro.umontreal.ca/~paquin

[25] A. Patel, "Quantum algorithms and genetic code", quant-ph/0002037, 2000.

[26] J. Preskill, "Reliable quantum computers", quant-ph/9705031, 1997.

[27] M. O. Rabin, "Two-way finite automata", Proc. Summer Institute of Symbolic Logic, Cornell, 366-369, 1957.

[28] M. O. Rabin, "Probabilistic automata", Information and Control, Vol. 6 (3), 230-245, 1963.

[29] J. C. Shepherdson, "The reduction of two-way automata to one-way automata", IBM Journal of Research and Development, Vol. 3 (2), 198-200, 1959.

[30] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring" , Proc. of 35th Annual Symposium on Fundamentals of Computer Science, 124-134, 1994.

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

[32] D. Simon, "On the power of quantum computation", SIAM J. Comput. 26 (5), 1474-1483, 1997.