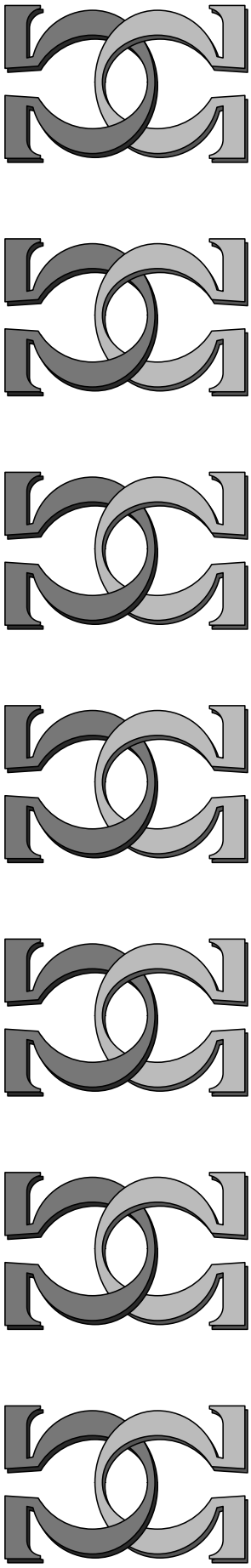

CDMTCS
Research
Report
Series

A New Quantum Algorithm for NP-complete Problems

Masanori Ohya
Igor V. Volovich
Science University of Tokyo
Steklov Mathematical Institute

CDMTCS-194
September 2002

Centre for Discrete Mathematics and
Theoretical Computer Science

A New Quantum Algorithm for NP-complete Problems *

Masanori Ohya and Igor V. Volovich †

Department of Information Sciences
Science University of Tokyo
Noda City, Chiba 278-8510, Japan

e-mail: ohya@is.noda.sut.ac.jp

Abstract

An approach to the solution of NP-complete problems based on quantum computing and chaotic dynamics is proposed. We consider the satisfiability problem and argue that the problem, in principle, can be solved in polynomial time if we combine the quantum computer with the chaotic dynamics amplifier based on the logistic map.

*To be presented at the Third International Conference on "Unconventional Models of Computation" (UMC'02), Kobe, Japan, October 2002.

†Permanent address: Steklov Mathematical Institute, Gubkin St.8, GSP-1, 117966, Moscow, Russia, volovich@mi.ras.ru.

1 Introduction

There are important problems such as the knapsack problem, the traveling salesman problem, the integer programming problem, the subgraph isomorphism problem, the satisfiability problem that have been studied for decades and for which all known algorithms have a running time that is exponential in the length of the input. These five problems and many other problems belong to the set of **NP**-complete problems. Any problem that can be solved in polynomial time on a nondeterministic Turing machine is polynomially transformed to an **NP**-complete problem [1].

Many **NP**-complete problems have been identified, and it seems that such problems are very difficult and probably exponential. If so, solutions are still needed, and in this paper we consider an approach to these problems based on quantum computers and chaotic dynamics.

It is widely believed that quantum computers are more efficient than classical computers. In particular Shor [2] gave a remarkable quantum polynomial-time algorithm for the factoring problem. However, it is unknown whether this problem is **NP**-complete.

The computational power of quantum computers has been explored in a number of papers. Bernstein and Vasirani [3] proved that **BPP**$\subseteq$**BQP**$\subseteq$ **PSPACE**. Here **BPP** stands for the class of problems efficiently solvable in the classical sense, i.e., the class of problems that can be solved in polynomial time by probabilistic Turing machines with error probability bounded by 1/3 for all inputs. The quantum analogue of the class **BPP** is the class **BQP** which is the class of languages that can be solved in polynomial time by quantum Turing machines with error probability bounded by 1/3 for all inputs.

The question whether **NP**$\subseteq$**BQP,** i.e., can quantum computers solve **NP**-complete problems in polynomial time, was considered in [4]. It was proved in [4] that relative to an oracle chosen uniformly at random, with probability 1, the class **NP** can not be solved on a quantum Turing machine in time $o\left(2^{n/2}\right)$. An oracle is a special subroutine call whose invocation only costs a unit time. This result does not rule out the possibility that **NP**$\subseteq$**BQP** but it does establish that there is no black-box approach to solving **NP**-complete problems in polynomial time on quantum Turing machines.

In this paper we suggest a new model of computations which combine quantum and classical machines. We would like to mention that above described results are not immediately applicable to the quantum chaos computer which we consider in this paper (see more discussion in Sect.3).

For a recent discussion of computational complexity in quantum computing see [5, 6, 7]. Mathematical features of quantum computing and quantum information theory are summarized in [8]. A possibility to exploit nonlinear quantum mechanics so that the class of problems **NP** may be solved in polynomial time has been considered by Abrams and Lloyd in [9]. It is mentioned in [9] that such nonlinearity is purely hypothetical; all known experiments confirm the linearity of quantum mechanics.

The satisfiability problem (SAT), which is **NP**-complete problem, has been considered in quantum computing in [10]. It was shown in [10] that the SAT problem can be solved in polynomial time by using a quantum computer under the assumption that a special

superposition of two orthogonal vectors can be physically detected . The problem one has to overcome here is that the output of computations could be a very small number and one needs to amplify it to a reasonable large quantity.

In this paper we propose that chaotic dynamics plays a constructive role in computations. Chaos and quantum decoherence are considered normally as the degrading effects which lead to an unwelcome increase of the error rate with the input size. However, in this paper we argue that under some circumstances chaos can play a constructive role in computer science. In particular we propose to combine quantum computer with the chaotic dynamics amplifier. We will argue, by using the consideration from [10], that such a quantum chaos computer can solve the SAT problem in polynomial time.

2 SAT Problem

Let $\{x_1, \cdots, x_n\}$ be a set of Boolean variables, $x_i = 0$ or 1. Then the set of the Boolean variables $\{x_1, \overline{x}_1, \cdots, x_n, \overline{x}_n\}$ with or without complementation is called the set of *literals.* A formula, which is the product (AND) of disjunctions (OR) of literals is said to be in the *product of sums* (POS) form. For example, the formula

$$(x_1 \vee \overline{x}_2)(\overline{x}_1)(x_2 \vee \overline{x}_3)$$

is in POS form. The disjunctions $(x_1 \vee \overline{x}_2), (\overline{x}_1), (x_2 \vee \overline{x}_3)$ here are called *clauses.* A formula in POS form is said to be *satisfiable* if there is an assignment of values to variables so that the formula has value 1. The preceding formula is satisfiable when $x_1 = 0$, $x_2 = 0$, $x_3 = 0$.

Definition (SAT Problem). The satisfiability problem (SAT) is to determine whether or not a formula in POS form is satisfiable.

The following analytical formulation of SAT problem is useful. We define a family of Boolean polynomials f_α, indexed by the following data. One α is a set

$$\alpha = \{S_1, ..., S_N, T_1, ..., T_N\},$$

where $S_i, T_i \subseteq \{1, ..., n\}$, and f_α is defined as

$$f_\alpha(x_1, \cdots, x_n) = \prod_{i=1}^{N} \left(1 + \prod_{a \in S_i}(1 + x_a) \prod_{b \in T_i} x_b\right).$$

We assume here the addition modulo 2. The SAT problem now is to determine whether or not there exists a value of $\mathbf{x} = (x_1, \cdots, x_n)$ such that $f_\alpha(\mathbf{x}) = 1$.

3 Quantum Algorithm

We will work in the $(n+1)$-tuple tensor product Hilbert space $\mathcal{H} \equiv \otimes_1^{n+1} \mathbf{C}^2$ with the computational basis

$$|x_1, ..., x_n, y\rangle = \otimes_{i=1}^{n} |x_i\rangle \otimes |y\rangle$$

where $x_1, ..., x_n$, $y = 0$ or 1. We denote $|x_1, ..., x_n, y\rangle = |\mathbf{x}, y\rangle$. The quantum version of the function $f(\mathbf{x}) = f_\alpha(\mathbf{x})$ is given by the unitary operator $U_f |\mathbf{x}, y\rangle = |\mathbf{x}, y + f(\mathbf{x})\rangle$. We assume that the unitary matrix U_f can be build in polynomial time, see [10]. Now let us use the usual quantum algorithm:

(i) By using the Fourier transform produce from $|\mathbf{0},0\rangle$ the superposition

$$|v\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}, 0\rangle .$$

(ii) Use the unitary matrix U_f to calculate $f(\mathbf{x})$:

$$|v_f\rangle = U_f |v\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}, f(\mathbf{x})\rangle$$

Now if we measure the last qubit, i.e., apply the projector $P = I \otimes |1\rangle \langle 1|$ to the state $|v_f\rangle$, then the probability to find the result $f(\mathbf{x}) = 1$ is $\|P |v_f\rangle\|^2 = r/2^n$ where r is the number of roots of the equation $f(\mathbf{x}) = 1$. If r is suitably large to detect it, then the SAT problem is solved in polynominal time. However, for small r, the probability is very small and this means we in fact don't get an information about the existence of the solution of the equation $f(\mathbf{x}) = 1$, so that in such a case we need further deliberation.

Let us simplify our notations. After the step (ii) the quantum computer will be in the state

$$|v_f\rangle = \sqrt{1 - q^2} |\varphi_0\rangle \otimes |0\rangle + q |\varphi_1\rangle \otimes |1\rangle$$

where $|\varphi_1\rangle$ and $|\varphi_0\rangle$ are normalized n qubit states and $q = \sqrt{r/2^n}$. Effectively our problem is reduced to the following 1 qubit problem. We have the state

$$|\psi\rangle = \sqrt{1 - q^2} |0\rangle + q |1\rangle$$

and we want to distinguish between the cases $q = 0$ and $q > 0$ (small positive number).

It is argued in [4] that a quantum computer can speed-up **NP** problems quadratically but not exponentially. The no-go theorem states that if the inner product of two quantum states is close to 1, then the probability that a measurement distinguishes which one of the two is exponentially small. And one could claim that amplification of this distinguishability is not possible.

At this point we emphasize that we do not propose to make a measurement which will be overwhelmingly likely to fail. Instead we propose to use the output $I |\psi\rangle$ of the quantum computer as an input for another device which uses chaotic dynamics.

The amplification would be not possible if we use the standard model of quantum computation with a unitary evolution. However the idea of our paper is different. We propose to combine a quantum computer with a chaotic dynamics amplifier. Such a quantum chaos computer is a new model of computation and we demonstrate that the amplification is possible in polynomial time.

One could object that we don't suggest a practical realization of the new model of computations. But at the moment nobody knows of how to make a practically useful

implementation of the standard model of quantum computing ever. Quantum circuit or quantum Turing machine is a mathematical model though convincing one. It seems to us that the quantum chaos computer considered in this paper deserves an investigation and has a potential to be realizable.

In this paper we consider only the mathematical model of computations. A possible specific physical implementation of quantum chaos computations will be discussed in a separate paper [13] based on the recently proposed atomic quantum computer.

This paper is a refined version of our previous paper [12].

4 Chaotic Dynamics

Various aspects of classical and quantum chaos have been the subject of numerious studies, see [14] and ref's therein.The investigation of quantum chaos by using quantum computers has been proposed in [15, 16, 17]. Here we will argue that chaos can play a constructive role in computations.

Chaotic behaviour in a classical system usually is considered as an exponential sensitivity to initial conditions. It is this sensitivity we would like to use to distinquish between the cases $q = 0$ and $q > 0$ from the previous section.

Consider the so called logistic map which is given by the equation

$$x_{n+1} = ax_n(1 - x_n) \equiv f(x), \quad x_n \in [0, 1]\,.$$

The properties of the map depend on the parameter a. If we take, for example, $a = 3.71$, then the Lyapunov exponent is positive, the trajectory is very sensitive to the initial value and one has the chaotic behaviour [14]. It is important to notice that if the initial value $x_0 = 0$, then $x_n = 0$ for all n.

It is known [18] that any classical algorithm can be implemented on quantum computer. Our quantum chaos computer consists of two blocks. One block is the ordinary quantum computer performing computations with the output $|\psi\rangle = \sqrt{1-q^2}\,|0\rangle + q\,|1\rangle$. The second block is a computer performing computations of the *classical* logistic map. This two blocks should be connected in such a way that the state $|\psi\rangle$ is transformed into the density matrix of the form

$$\rho = q^2 P_1 + \left(1 - q^2\right) P_0$$

where P_1 and P_0 are projectors to the state vectors $|1\rangle$ and $|0\rangle$. This connection is in fact nontrivial and actually it should be considered as the third block. One has to notice that P_1 and P_0 generate an Abelian algebra which can be considered as a classical system. In the second block the density matrix ρ above is interpreted as the initial data ρ_0, and we apply the logistic map as

$$\rho_m = \frac{(I + f^m(\rho_0)\sigma_3)}{2}$$

where I is the identity matrix and σ_3 is the z-component of Pauli matrix on $\mathbb{C}^2$. To find a proper value m we finally measure the value of σ_3 in the state ρ_m such that

$$M_m \equiv tr\rho_m\sigma_3.$$

After a simple computation we obtain

$$\rho_m = \frac{(I + f^m(q^2)\sigma_3)}{2}, \text{ and } M_m = f^m(q^2).$$

Thus the question is whether we can find an m in polynomially many steps of n satisfying the inequality $M_m \geqq \frac{1}{2}$ for very small but non-zero q^2. Here we have to remark that if one has $q = 0$ then $\rho_0 = P_0$ and we obtain $M_m = 0$ for all m. If $q \neq 0$, the stochastic dynamics leads to the amplification of the small magnitude q in such a way that it can be detected as is explained below. The transition from ρ_0 to ρ_m is nonlinear and can be considered as a classical evolution because our algebra generated by P_0 and P_1 is Abelian. The amplification can be done within atmost $2n$ steps due to the following propositions. Since $f^m(q^2)$ is x_m of the logistic map $x_{m+1} = f(x_m)$ with $x_0 = q^2$, we use the notation x_m in the logistic map for simplicity.

Proposition 1 *For the logistic map $x_{n+1} = ax_n(1 - x_n)$ with $a \in [0, 4]$ and $x_0 \in [0, 1]$, let x_0 be $\frac{1}{2^n}$ and a set J be $\{0, 1, 2, \cdots, n, \cdots, 2n\}$. If a is 3.71, then there exists an integer m in J satisfying $x_m > \frac{1}{2}$.*

Proof: Suppose that there does not exist such m in J. Then $x_m \leq \frac{1}{2}$ for any $m \in J$. The inequality $x_m \leq \frac{1}{2}$ implies

$$x_m = 3.71(1 - x_{m-1})x_{m-1} \geq \frac{3.71}{2}x_{m-1}.$$

Thus we have

$$\frac{1}{2} \geq x_m \geq \frac{3.71}{2}x_{m-1} \geq \cdots \geq \left(\frac{3.71}{2}\right)^m x_0 = \left(\frac{3.71}{2}\right)^m \frac{1}{2^n},$$

from which we get

$$2^{n+m-1} \geq (3.71)^m.$$

According to the above inequality, we obtain

$$m \leq \frac{n-1}{\log_2 3.71 - 1}.$$

Since $\log_2 3.71 \doteqdot 1.8912$, we have

$$m \leq \frac{n-1}{\log_2 3.71 - 1} < \frac{5}{4}(n-1),$$

which is definitely less than $2n - 1$ and it is contradictory to the statement "$x_m \leq \frac{1}{2}$ for any $m \in J$". Thus there exists m in J satisfying $x_m > \frac{1}{2}$. ■

Proposition 2 *Let a and n be the same in the above proposition. If there exists m_0 in J such that $x_{m_0} > \frac{1}{2}$, then $m_0 > \frac{n-1}{\log_2 3.71}$.*

Proof: Since $0 \leq x_m \leq 1$, we have

$$x_m = 3.71(1 - x_{m-1})x_{m-1} \leq 3.71x_{m-1},$$

which reduces to

$$x_m \leq (3.71)^m x_0.$$

For m_0 in J satisfying $x_{m_0} > \frac{1}{2}$, it holds

$$x_0 \geq \frac{1}{(3.71)^{m_0}} x_{m_0} > \frac{1}{2 \times (3.71)^{m_0}}.$$

It follows that from $x_0 = \frac{1}{2^n}$

$$\log_2 2 \times (3.71)^{m_0} > n,$$

which implies

$$m_0 > \frac{n-1}{\log_2 3.71}. \blacksquare$$

According to these propositions, it is enough to check the value x_m (M_m) around the above m_0 when q is $\frac{1}{2^n}$ for a large n. More generally, when q=$\frac{k}{2^n}$ with some integer k, it is similarly checked that the value x_m (M_m) becomes over $\frac{1}{2}$ within at most $2n$ steps.

One can think about various possible implementations of the idea of using chaotic dynamics for computations, about which we will discuss how one can realize nonlinear quantum gates on an atomic quantum computer in [13].

Finally we show in Fig.1 how we can easily amplify the small q in several steps.

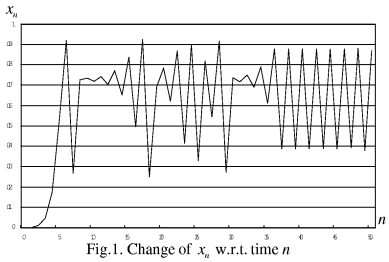

Fig.1. Change of x_n w.r.t. time n

5 Conclusion

The complexity of the quantum algprithm for the SAT problem has been considered in [10] where it was shown that one can build the unitary matrix U_f in the polynomial time.

We have also to consider the number of steps in the classical algorithm for the logistic map performed on quantum computer. It is the probabilistic part of the construction and one has to repeat computations several times to be able to distingish the cases $q = 0$ and $q > 0$. Thus it seems that the quantum chaos computer can solve the SAT problem in polynominal time.

In conclusion, in this paper the quantum chaos computer is proposed. It combines the ordinary quantum computer with quantum chaotic dynamics amplifier. We argued that such a device can be powerful enough to solve the **NP**-complete problems in the polynomial time.

Bibliography

[1] M. Garey and D. Johnson, *Computers and Intractability - a guide to the theory of NP-completeness*, Freeman, 1979.

[2] P.W. Shor, *Algorithm for quantum computation: Discrete logarithm and factoring algorithm*, Proceedings of the 35th Annual IEEE Symposium on Foundation of Computer Science, pp.124-134, 1994.

[3] E. Bernstein and U. Vazirani, *Quantum Complexity Theory*, in: Proc. of the 25th Annual ACM Symposium on Theory of Comuting, (ACM Press, New York,1993), pp.11-20.

[4] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani,
Strengths and Weaknesses of Quantum Computing, quant-ph/9701001

[5] L. Fortnow and J. Rogers, *Complexity Limitations on Quantum Computation*, cs.CC/9811023.

[6] R. Cleve, *An Introduction to Quantum Complexity Theory*, quant-ph/9906111.

[7] E. Hemaspaandra, L.A. Hemaspaandra and M. Zimand,
Almost-Everywhere Superiority for Quantum Polynomial Time, quant-ph/9910033.

[8] M.Ohya, *Mathematical Foundation of Quantum Computer,* Maruzen Publ. Company, 1998.

[9] D. S. Abrams and S. Lloyd, *Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems,* quant-ph/9801041.

[10] M.Ohya and N.Masuda, NP problem in quantum algorithm, Open Systems and Information Dynamics, Vol.7, No.1, 33-39, 2000.

[11] L.Accardi, R.Sabbadini: On the Ohya–Masuda quantum SAT Algorithm, in: Proceedings International Conference "Unconventional Models of Computations", I. Antoniou, C.S. Calude, M. Dinneen (eds.) Springer 2001

[12] M. Ohya and I.V. Volovich, M.Ohya and I.V.Volovich, Quantum computing, NP-complete problems and chaotic dynamics, in: *Quantum Information II*, eds. T.Hida and K.Saito, World Sci. 2000; quant-ph/9912100.

[13] M. Ohya and I.V. Volovich, An implementation of chaotic dynamics by atomic computer, in preparation.

[14] M. Ohya, *Complexities and Their Applications to Characterization of Chaos,* Int. Journ. of Theoret. Physics, 37 (1998) 495.

[15] S.A. Gardiner, J.I. Cirac and P. Zoller, Phys. Rev. Lett. 79(1997) 4790.

[16] R. Schack, Phys. Rev. A57 (1998) 1634; T. Brun and R. Schack, quant-ph/9807050.

[17] I. Kim and G. Mahler, *Quantum Chaos in Quantum Turing Machine,* quant-ph/9910068.

[18] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer,* Proc. of Royal Society of London series A, **400**, pp.97-117, 1985.

[19] J.I. Cirac and P. Zoller, Phys. Rev. Lett., 74 (1995) 74.

[20] N.A. Gershenfeld and I.L. Chuang, Science, 275 (1997) 350.

[21] G. Burkard, D. Loss and D.P. DiVincenzo, cond-mat/9808026.

[22] A. Ekert and R. Jozsa, *Quantum computation and Shor's factoring algorithm,* Reviews of Modern Physics, **68** No.3,pp.733-753, 1996.

[23] I.I. Sobelman, *Atomic Spectra and Radiative Transitions,* Springer-Verlag, 1991.

[24] Accardi, L. and Ohya, M.: *Teleportation of general quantum states,* Voltera Center preprint,1998.

[25] Fichtner, K.-H. and Ohya, M.:*Quantum Teleportation with Entangled States given by Beam Splittings, to appear in Commun. Math. Phys.*