Open Sys. & Information Dyn. **11**: 219–233, 2004

Printed in the Netherlands

A Stochastic Limit Approach to the SAT Problem

Luigi Accardi

Centro V. Volterra
Università di Roma Torvergata
Via Orazio Raimondo, 00173 Roma, Italia
e-mail: accardi@volterra.mat.uniroma2.it

Masanori Ohya

Department of Information Sciences
Tokyo University of Science
Noda City, Chiba 278–8510, Japan
e-mail: ohya@is.noda.tus.ac.jp

(Received: January 26, 2004)

Abstract. There exists an important problem whether there exists an algorithm to solve an NP-complete problem in polynomial time. In this paper, a new concept of quantum adaptive stochastic systems is proposed, and it is shown that it can be used to solve the problem above.

1. Introduction

Although the performance of computers is highly progressed, there are several problems which may not be solved effectively, namely, in polynomial time. Among such problems, so-called NP-problems and NP-complete problems are fundamental. It is known that all NP-complete problems are equivalent and an essential question is *whether there exists an algorithm to solve an NP complete problem in polynomial time*. Problems of this kind have been studied for decades and so far all known algorithms have an exponential running time in the length of the input. The standard definition of P- and NP-problems is the following [14, 17, 20]:

DEFINITION 1 Let n be the size of input.

(1) A P-problem is a problem such that the number of elementary steps needed to solve it is polynomial in n. Equivalently, it is a problem which can be recognized in time which is polynomial in n by a deterministic Turing machine.

(2) An NP-problem is a problem which can be solved in polynomial time by a nondeterministic Turing machine.

This can be understood as follows: Let us consider a problem to find a solution of $f(x) = 0$. We can check in time polynomial in n whether x_0 is a solution of $f(x) = 0$, but we do not know whether we can find the solution of $f(x) = 0$ in such time.

DEFINITION 2 An NP-complete problem is a problem to which any other NP-problem can be polynomially transformed.

We take the SAT (satisfiability) problem, one of the NP-complete problems, to study whether there exists an algorithm showing NPC = P. Our aim of this paper and the previous ones [10, 12, 13] is to find a quantum algorithm solving the SAT problem in polynomial time in the size of data.

Let $X \equiv \{x_1, \ldots, x_n\}$ be a set. Then x_k and its negation $\bar{x}_k$ $(k = 1, 2, \ldots, n)$ are called literals and the set of all such literals is denoted by $X' \equiv \{x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n\}$. The set of all subsets of X' is denoted by $\mathcal{F}(X')$ and an element $C \in \mathcal{F}(X')$ is called a clause. We take a truth assignment to all Boolean variables x_k. If we can assign the truth value to at least one element of C, then C is called satisfiable. When C is satisfiable, the truth value $t(C)$ of C is regarded as true, otherwise, it is is false. Taking the truth values as "true ↔1, false ↔0". Then C is satisfiable iff $t(C) = 1$.

Let $L = \{0, 1\}$ be a Boolean lattice with usual join $\vee$ and meet $\wedge$ operations, and $t(x)$ be the truth value of a literal x in X. Then the truth value of a clause C is written as $t(C) \equiv \vee_{x \in C} t(x)$.

Moreover the set $\mathcal{C}$ of all clauses C_j $(j = 1, 2, \ldots, m)$ is called satisfiable iff the meet of all truth values of C_j is 1; $t(\mathcal{C}) \equiv \wedge_{j=1}^{m} t(C_j) = 1$. Thus the SAT problem is written as follows:

DEFINITION 3 *SAT Problem: Given a Boolean set* $X \equiv \{x_1, \ldots, x_n\}$ *and a set* $\mathcal{C} = \{\mathcal{C}_1, \ldots, \mathcal{C}_m\}$ *of clauses, determine whether* $\mathcal{C}$ *is satisfiable or not.*

That is, this problem is to ask whether there exists a truth assignment which makes $\mathcal{C}$ satisfiable. It is known that one needs polynomial time to check the satisfiability when a specific truth assignment is given, but we cannot determine the satisfiability in polynomial time when an assignment is not specified.

In [10] we have discussed the quantum algorithm of the SAT problem, which was rewritten in [18] and we have showed that OM SAT-algorithm is combinatoric. In [12, 13] it is shown that the chaotic quantum algorithm can solve the SAT problem in polynomial time.

Ohya and Masuda pointed out [10] that the SAT problem, and hence all other NP problems, can be solved in polynomial time by a quantum computer if the superposition of two orthogonal vectors $|0\rangle$ and $|1\rangle$ can be physically detected. However this detection is considered impossible with the present day technology. The problem to be overcome is how to distinguish the pure vector $|0\rangle$ from the superposed one $\alpha|0\rangle + \beta|1\rangle$, obtained by the OM SAT-quantum algorithm, if β is not zero but very small. If such a distinction is possible, then we can solve the NPC problem in the polynomial time. In [12, 13] it is shown that it can be possible by combining nonlinear chaos amplifier with the quantum algorithm, which would imply the existence of a mathematical algorithm solving NP = P. It is not known if the algorithm of Ohya and Volovich lies in the framework of quantum Turing algorithms or not. So the next question is (1) whether there exists a physical realization combining the SAT quantum algorithm with chaos dynamics, or (2) whether there exists another method to achieve the above distinction of two vectors by a suitable unitary evolution so that all process can be modeled by a certain quantum Turing machine (circuits).

In this paper, we argue that the stochastic limit, recently extensively studied by Accardi and coworkers [1], can be used to find another method of (2) above. In Sect. 2, we review mathematical frame of quantum algorithm and the OM SAT-algorithm following the representation of Accardi and Sabaddini [18] with a quick review of OV-chaos algorithm in Sect. 3. In Sect. 4, a new concept — quantum adaptive stochastic system — is proposed, and in Sect. 5, we show that it can be used to solve the problem NP = P.

2. Quantum Algorithm

The quantum algorithms discussed so far are rather idealized because computation is represented by unitary operations. A unitary operation is rather difficult to realize in physical processes, a more realistic operation is the one allowing some dissipation like semigroup dynamics. However such dissipative dynamics destroys the entanglement and hence they essentially reduce the ability of quantum computation to preserve the entanglement of states. In order to keep the power of quantum computation and good entanglement, it will be necessary to introduce some kind of amplification in the course of real physical processes in physical devices, which will be similar to the amplication processes in quantum communication. In this section, to look for more realistic operations in a quantum computer, the channel expression will be used, at least, in the sense of mathematical scheme of quantum computation because a channel is not always unitary and represents many different types of dynamics.

Let $\mathcal{H}$ be a Hilbert space describing the input, computation and the output (result). As usual, the Hilbert space is $\mathcal{H} = \otimes_1^N \mathbb{C}^2$, and let the basis of $\mathcal{H} = \otimes_1^N \mathbb{C}^2$ be:

$$\begin{array}{rcl} e_0 & \equiv & |0\rangle \; = \; |0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle \ , \\ e_1 & \equiv & |1\rangle \; = \; |0\rangle \otimes \cdots \otimes |0\rangle \otimes |1\rangle \ , \\ \cdots & & \cdots \\ e_{2^N-1} & \equiv & \left|2^N-1\right\rangle \; = \; |1\rangle \otimes \cdots \otimes |1\rangle \otimes |1\rangle \, . \end{array}$$

Any number $t \in \{0, \ldots, 2^N - 1\}$ can be expressed by

$$t \; = \; \sum_{k=1}^{N} a_t^{(k)} 2^{k-1},$$

$a_t^{(k)} = 0$ or $a_t^{(k)} = 1$, so that the associated vector is written by

$$|t\rangle \, (= e_t) \; = \; \bigotimes_{k=1}^{N} \left| a_t^{(k)} \right\rangle .$$

Applying n-tuples of the Hadamard matrix $A \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to the vacuum vector $|0\rangle$, we get

$$A\,|0\rangle\,(\,=\xi\,(0))\;\equiv\;\bigotimes_{1}^{N}\frac{1}{\sqrt{2}}\,(|0\rangle+|1\rangle)\,.$$

Put

$$W\,(t)\;\equiv\;\bigotimes_{j=1}^{N}\begin{pmatrix} 1 & 0 \\ 0 & \exp(\frac{2\pi it}{2^N}2^{j-1}) \end{pmatrix}.$$

Then we have

$$\xi\,(t)\;\equiv\;W\,(t)\,\xi\,(0)\;=\;\frac{1}{\sqrt{2^N}}\sum_{k=0}^{2^N-1}\exp\Big(\frac{2\pi itk}{2^N}\Big)\,|k\rangle\,,$$

which is called Discrete Fourier Transformation. The combination of the above operations gives a unitary operator $U_F\,(t)\equiv W\,(t)\,A$ and the vector $\xi\,(t)=U_F\,(t)\,|0\rangle$.

2.1. Channel expression of conventional unitary algorithm

All conventional unitary algorithms can be written as a combination of the following three steps:

(1) Preparation of state: Take a state ρ (e.g., $\rho=|0\rangle\,\langle 0|$) and apply the unitary channel defined by the above $U_F\,(t):\Lambda_F^*=\mathrm{Ad}_{U_F(t)}$

$$\Lambda_F^*\;=\;\mathrm{Ad}_{U_F}\quad\Longrightarrow\quad\Lambda_F^*\rho\;=\;U_F\rho U_F^*.$$

(2) Computation: Let U be a unitary operator on $\mathcal{H}$ representing the computation followed by a suitable programming of a certain problem, then the computation is described by a channel $\Lambda_U^*=\mathrm{Ad}_U$ (unitary channel). After the computation, the final state ρ_f will be

$$\rho_f\;=\;\Lambda_U^*\Lambda_F^*\rho\,.$$

(3) Registration and Measurement: For the registration of the computed result and its measurement we may need an additional system $\mathcal{K}$ (e.g., register), so that the lifting $\mathcal{E}_m^*$ from $\mathcal{S}\,(\mathcal{H})$ to $\mathcal{S}\,(\mathcal{H}\otimes\mathcal{K})$ in the sense of [2] is useful to describe this stage. Thus the whole process is wrtten as

$$\rho_f\;=\;\mathcal{E}_m^*\,(\Lambda_U^*\Lambda_F^*\rho)\,.$$

Finally, we measure the state in $\mathcal{K}$: For instance, let $\{P_k;k\in J\}$ be a projection valued measure (PVM) on $\mathcal{K}$

$$\Lambda_m^*\rho_f\;=\;\sum_{k\in J}I\otimes P_k\rho_f I\otimes P_k\,,$$

after which we can get a desired result by observations in finite times if the size of the set J is small.

2.2. Channel expression of the general quantum algorithm

When dissipation is involved the above three steps have to be generalized. Such a generalization can be expressed by means of suitable channel, not necessarily unitary.

(1) Preparation of state: We may use the same channel $\Lambda_F^* = \mathrm{Ad}_{U_F}$ in this first step, but if the number of qubits N is large so that it will not be built physically, then Λ_F^* should be modified; let us denote it by Λ_P^*.

(2) Computation: This stage is certainly modified to a channel Λ_C^* reflecting a physical device realizing it.

(3) Registration and Measurement: This stage is the the same as above. Thus the whole process is written as

$$\rho_f \;=\; \mathcal{E}_m^* \left(\Lambda_C^* \Lambda_P^* \rho\right).$$

3. Quantum Algorithm of SAT

Let 0 and 1 of the Boolean lattice L be denoted by the vectors $|0\rangle \equiv \binom{1}{0}$ and $|1\rangle \equiv \binom{0}{1}$ in the Hilbert space $\mathbb{C}^2$, respectively. That is, the vector $|0\rangle$ represents false and $|1\rangle$ truth. This section is based on [10, 18, 3].

As we explained in the previous section, an element $x \in X$ can be denoted by 0 or 1, i.e. by $|0\rangle$ or $|1\rangle$ in the present context. In order to describe a clause C of length at most n by a quantum state, we need the n-tuple tensor product Hilbert space $\mathcal{H} \equiv \otimes_1^n \mathbb{C}^2$. For instance, in the case of $n = 2$, given $C = \{x_1, x_2\}$ with an assignment $x_1 = 0$ and $x_2 = 1$, the corresponding quantum state vector is $|0\rangle \otimes |1\rangle$, so that the quantum state vector describing C is generally written as $|C\rangle = |x_1\rangle \otimes |x_2\rangle \in \mathcal{H}$ with $x_k = 0$ or 1 $(k = 1, 2)$.

The quantum computation is performed by a unitary gate constructed from several fundamental gates such as "Not" gate, "Controlled-Not" gate, "Controlled-Controlled" Not gate [22, 11]. Once $X \equiv \{x_1, \ldots, x_n\}$ and $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$ are given, the SAT is to find the vector

$$|t\left(\mathcal{C}\right)\rangle \;\equiv\; \bigwedge_{j=1}^{m} \bigvee_{x \in C_j} t(x)\,,$$

where $t(x)$ is $|0\rangle$ or $|1\rangle$ when $x = 0$ or 1, respectively, and $t(x) \wedge t(y) \equiv t(x \wedge y)$, $t(x) \vee t(y) \equiv t(x \vee y)$.

3.1. Logical negation

DEFINITION 4 Let X be a set. A *negation* on X is an involution without fixed points, i.e. a map $X \ni x \mapsto x' \in X$ such that $(x')' = x\,;\; x \neq x' \;\forall x \in X$. x' is called the *negation* of x.

PROPOSITION 1 *Given a nonempty set X with a negation $(x \mapsto x')$ and denoting*

$$I' := \{x' \in X : x \in I\},$$

for $I \subseteq X$, there exists a set $I \subseteq X$ such that $X = I \cup I'$.

Thus a finite set with a negation must be even. Let X be a finite set with $2n$ elements and with a negation $(x \mapsto x')$. A partition $X = I \cup I'$, $|I| = n$ can be constructed with an n-step algorithm. Not all n-step algorithms are equivalent.

DEFINITION 5 Given a set X with a negation $x \mapsto x'$, a "clause" is a subset of X. A minimal clause is a subset $I \subseteq X$ such that $I \cap I' = \emptyset$ (i.e. if I contains x, it does not contain the negation of x).

In any set X of cardinality $2n$ there are 2^n minimal clauses. Given a set $\widehat{\mathcal{C}}_0$ of clauses, if there are non-minimal clauses in it, then we can eliminate them from $\hat{\mathcal{C}}_0$ because any truth function must be identically zero on a non-minimal clause.

However, to eliminate the non-minimal clauses from $\widehat{\mathcal{C}}_0$, one has to "read" all its elements. Their number can be of order 2^n.

3.2. Truth functions

The set $\{0, 1\}$ is a Boolean algebra with the operations

$$\varepsilon \vee \varepsilon' := \max\{\varepsilon, \varepsilon'\}, \qquad \varepsilon \wedge \varepsilon' := \min\{\varepsilon, \varepsilon'\}, \quad \varepsilon, \varepsilon' \in \{0, 1\}.$$

A clause truth function on the clauses on the set $X = \{x_1, \dots, x_n, x'_1, \dots, x'_n\}$ is a boolean algebra homomorphism

$$t : X \to \{0, 1\}$$

with the property (*principle of the excluded third*):

$$t(x_j) \vee t(x'_j) = 1, \quad \forall\, j = 1, \dots, n. \tag{1}$$

Because of (1), such a function is uniquely determined by values $\{t(x_1), \dots, t(x_n)\}$, hence the number of such functions is 2^n. For this reason, in the following we will simply say *truth function on* $\{x_1, \dots, x_n\}$ meaning by this a truth function on the clauses of the set $\{x_1, \dots, x_n, x'_1, \dots, x'_n\}$. Conversely given any n-tuple $\varepsilon = (\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1\}^n$, there exists only one truth function on $\{x_1, \dots, x_n\}$, with the property that

$$t(x_j) = \varepsilon_j, \quad \forall\, j = 1, \dots, n.$$

In what follows, given a truth function t, we denote the string in $\{t(x_1), \dots, t(x_n)\}$ uniquely associated to that function by ε_t.

Let $\mathcal{T}$ be the set of truth functions on $\{x_1, \dots, x_n\}$. The function

$$t \in \mathcal{T} \mapsto |t(x_1), \dots, t(x_n)\rangle \in \otimes^n \mathbb{C}^2$$

defines a one-to-one correspondence between $\mathcal{T}$ and the set $\{0, 1\}$, that is, a one-to-one correspondence between truth functions and vectors of the computational basis of $\otimes^n \mathbb{C}^2$

PROPOSITION 2 *Let $C \subseteq X$ be a clause and I, I' the sets associated to it through the procedure explained in Sect. 1. Let t be a truth function on $\{x_1, \ldots, x_n\}$. Then*

$$t(C) \;=\; \left[\bigvee_{i\in I} t(x_i)\right] \vee \left[\bigvee_{j\in I'} (1 - t(x_j))\right].$$

Therefore, as stated in Introduction, a set of clauses $\mathcal{C}_0$ is said to be SAT if there exists a truth function t, on $\{x_1, \ldots, x_n\}$ such that

$$t(\mathcal{C}_0) \;:=\; t\Big(\bigwedge_{C\in\mathcal{C}_0} C\Big) = \prod_{C\in\mathcal{C}_0} t(C) = 1\,.$$

3.3. Quantum algorithm for the SAT Problem

We review here a technique developed in [10], which shows that the SAT problem can be solved in polynomial time by a quantum computer.

Given a set of clauses $\mathcal{C}_0 = \{C_1, \ldots, C_m\}$ on X, Ohya and Masuda constructed a Hilbert space $\mathcal{H} = \otimes^{n+\mu}\mathbb{C}^2$, where μ is a number that can be chosen linear in mn, and a unitary operator $U_{\mathcal{C}_0} : \mathcal{H} \to \mathcal{H}$ with the property that, for any truth function t,

$$U_{\mathcal{C}_0}|\varepsilon_t, 0_\mu\rangle \;=\; |\varepsilon_t, x^{\varepsilon_t}_{\mu-1}, t(\mathcal{C}_0)\rangle\,,$$

where ε_t is the vector of the computational basis of $\otimes^n\mathbb{C}^2$ corresponding to t, and 0_μ (resp. $x^{\varepsilon}_{\mu-1}$) is a string of μ zeros (resp. a string of $(\mu - 1)$ binary symbols depending on ε).

Furthermore $U_{\mathcal{C}_0}$ is a product of *gates*, namely of unitary operators that act at most on two qubits at a time.

Let $\mathcal{C}_0$ and $U_{\mathcal{C}_0}$ be as above and, for every $\varepsilon \in \{0,1\}^n$, let t_ε be the corresponding truth function. Applying the unitary operator $U_{\mathcal{C}_0}$ to the vector

$$|v\rangle \;:=\; \frac{1}{2^{n/2}} \sum_{\varepsilon\in\{0,1\}^n} |\varepsilon, 0_\mu\rangle$$

one obtains the final state vector

$$|v_f\rangle \;:=\; U_{\mathcal{C}_0}\,|v\rangle \;=\; \frac{1}{2^{n/2}} \sum_{\varepsilon\in\{0,1\}^n} |\varepsilon, x^{\varepsilon}_{\mu-1}, t_\varepsilon(\mathcal{C}_0)\rangle\,.$$

THEOREM 1 *$\mathcal{C}_0$ is satisfiable if and only if*

$$P_{n+\mu,1} U_{\mathcal{C}_0}\,|v\rangle \;\neq\; 0\,,$$

where $P_{n+\mu,1}$ denotes the projector

$$P_{n+\mu,1} \;:=\; 1_{n+\mu-1} \otimes |1\rangle\langle 1|$$

on the subspace of $\mathcal{H}$ spanned by the vectors

$$|\varepsilon_n, \varepsilon_{\mu-1}, 1\rangle\,.$$

According to the standard theory of quantum measurement, after a measurement of the event $P_{n+\mu,1}$, the state $\rho = |v_f\rangle\langle v_f|$ becomes

$$\rho \;\to\; \frac{P_{n+\mu,1}\rho P_{n+\mu,1}}{\operatorname{Tr}\rho' P_{n+\mu,1}} \;=:\; \rho' \,.$$

Thus the solvability of the SAT problem is reduced to check that $\rho' \neq 0$. The difficulty is that the probability of $P_{n+\mu,1}$ is

$$\operatorname{Tr}\rho' P_{n+\mu,1} \;=\; \|P_{n+\mu,1}\psi\|^2 \;=\; \frac{|T(\mathcal{C}_0)|}{2^n}\,,$$

where $|T(\mathcal{C}_0)|$ is the cardinality of the set $T(\mathcal{C}_0)$, of all the truth functions t such that $t(\mathcal{C}_0) = 1$.

We put $q := \sqrt{r/2^n}$ with $r := |T(\mathcal{C}_0)|$ in the sequel. Then if r is suitably large to detect it, then the SAT problem is solved in polynomial 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 $t(C_0) = 1$, so that in such a case we need further deliberation.

Let us simplify our notations. After the quantum computation, 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 [16] that 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 then is exponentially small. And one could claim that amplification of this distinguishability is not possible.

At this point we emphasized [13] that we do not propose to make a measurement which will be overwhelmingly likely to fail. What we do it is a proposal 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 computations with a unitary evolution. However the idea of the paper [12, 13] is different. In [12, 13] it is proposed to combine quantum computer with a chaotic dynamics amplifier. Such a quantum chaos computer is a new model of computations and we demonstrate that the amplification is possible in the polynomial time.

One could object that we do not 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. It seems to us that the quantum chaos computer considered in [13] deserves an investigation and has a potential to be realizable.

Here we mention two works on non-linear quantum evolution to study NP-problems done by Abrams-Lloyd [8] and Czachor [9]. The former was based on the Weinberg model of nonlinear quantum mechanics and the latter was done by means of the Polchinski type description. Czachor's work looks similar to our approach (stochastic limit). Their works are very artificial and conceptually different from ours.

3.4. Chaotic dynamics

Various aspects of classical and quantum chaos have been the subject of numerous studies, see [19] and references therein. Here we will argue that chaos can play a constructive role in computations (see [12, 13] for the details).

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

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

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

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 [19]. It is important to notice that if the initial value $x_0 = 0$, then $x_n = 0$ for all n.

It is known [21] that any classical algorithm can be implemented on a quantum computer. Our quantum chaos computer will consist of two blocks. One block is an 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 $|\psi\rangle$ first be transformed into the density matrix of the form

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

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 Pauli matrix on $\mathbb{C}^2$. To find the proper value m we finally measure the value of σ_3 in the state ρ_m such that

$$M_m \ \equiv \ \mathrm{Tr} \rho_m \sigma_3 \, .$$

We obtain

THEOREM 2

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

Thus the question is whether we can find such an m in polynomial number steps in n satisfying the inequality $M_m \geq \frac{1}{2}$ 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 at most 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.

THEOREM 3 *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* $1/2^n$ *and the set* J *be* $\{0, 1, 2, \ldots, n, \ldots 2n\}$. *If* a *is* 3.71, *then there exists an integer* m *in* J *satisfying* $x_m > 1/2$.

THEOREM 4 *Let* a *and* n *be the same as in the above proposition. If there exists* m_0 *in* J *such that* $x_{m_0} > 1/2$, *then* $m_0 > (n - 1)/\log_2 3.71$.

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

The complexity of the quantum algorithm for the SAT problem was discussed in Sect. 3 to be polynomial in time. We have only to consider the number of steps in the classical algorithm for the logistic map performed on a quantum computer. It is the probabilistic part of the construction and one has to repeat computations several times to be able to distinguish the cases $q = 0$ and $q > 0$. Thus it seems that the quantum chaos computer can solve the SAT problem in polynomial time.

In conclusion of [12, 13], the quantum chaos computer combines the ordinary quantum computer with quantum chaotic dynamics amplifier. It may go beyond the usual quantum Turing algorithm, but such a device can be powerful enough to solve the NP-complete problems in the polynomial time. The detailed estimation of the complexity of the SAT algorithm is discussed in [23].

In the next two sections we will discuss the SAT problem from a different point of view, that is, we will show that the same amplification is possible by unitary dynamics defined in the stochastic limit.

4. Quantum Adaptive Systems

The idea to develop a mathematical approach to adaptive systems, i.e. those systems whose properties are in part determined as responses to an environment

[7, 25], was born in connection with some problems of quantum measurement theory and chaos dynamics.

The mathematical definition of an adaptive system is in terms of observables, namely: *an adaptive system is a composite system whose interaction depends on a fixed observable* (typically in a measurement process, this observable is the observable one wants to measure). Such systems may be called *observable-adaptive.*

In the present paper, we want to extend this point of view by introducing another natural class of adaptive systems which, in a certain sense, is the dual to the one defined above, namely the class of *state-adaptive* systems. These are defined as follows: *a state-adaptive system is a composite system whose interaction depends on the state of at least one of the sub-systems at the instant in which the interaction is switched on.*

Notice that both definitions make sense both for classical and for quantum systems. Since in this paper we will be interested in an application of adaptive systems to quantum computation, we will discuss only quantum adaptive systems, but one should keep in mind that all the considerations below apply to classical systems as well.

The difference between state-adaptive systems and nonlinear dynamical systems should be emphasized:

(i) in nonlinear dynamical systems (such as those whose evolution is described by the Boltzmann equation, or nonlinear Schrödinger equation, etc.) the interaction Hamiltonian depends on the state at each time t, i.e. $H_I = H_I(\rho_t)$ $\forall\ t$.

(ii) in state-adaptive dynamical systems (such as those considered in the present paper) the interaction Hamiltonian depends on the state only at each time $t = 0$, i.e. $H_I = H_I(\rho_0)$.

The latter class of systems describes the following physical situation: at time $t = -T$ ($T > 0$) the system S is prepared in the state ψ_{-T} and in the time interval $[-T, 0]$ it evolves according to a fixed (free) dynamics $U_{[-T,0]}$ so that its state at time 0 is $U_{[-T,0]}\psi_{-T} =: \psi_0$. At time $t = 0$ an interaction with another system R is switched on and this interaction depends on the state ψ_0, i.e. $H_I = H_I(\psi_0)$.

If we interpret the system R as *environment*, we can say that the above interaction describes the response of the environment to the state of the system S.

Now from the general theory of stochastic limit [1] one knows that, under general ergodicity conditions, an interaction with an environment drives the system to a dynamical (but not necessarily thermodynamical) equilibrium state which depends on the initial state of the environment and on the interaction Hamiltonian.

Therefore, if one is able to realize experimentally these state dependent Hamiltonians, one would be able to drive the system S to a pre-assigned dynamical equilibrium state depending on the input state ψ_0.

In the following section we will substantiate the general scheme described above with an application to the quantum computer approach to the SAT problem described in previous sections.

5. Stochastic Limit and SAT Problem

We illustrate the general scheme described in the previous section in the simplest case when the state space of the system is $\mathcal{H}_S \equiv \mathbb{C}^2$. We fix an orthonormal basis of $\mathcal{H}_S$ as $\{e_0, e_1\}$.

The unknown state (vector) of the system at time $t = 0$

$$\psi := \sum_{\varepsilon \in \{0,1\}} \alpha_\varepsilon e_\varepsilon = \alpha_0 e_0 + \alpha_1 e_1 , \quad \|\psi\| = 1 .$$

In the case of Sect. 3, α_1 corresponds to q and e_j does to $|j\rangle$ $(j = 0, 1)$. This vector is taken as input and defines the interaction Hamiltonian in an external field

$$\begin{aligned} H_I &= \lambda |\psi\rangle\langle\psi| \otimes (A_g^+ + A_g) \\ &= \sum \lambda \alpha_\varepsilon \overline{\alpha}_\varepsilon |e_\varepsilon\rangle\langle e_{\varepsilon'}| \otimes (A_g^+ + A_g) , \end{aligned}$$

where λ is a small coupling constant. Here and in the following summation over repeated indices is understood.

The free system Hamiltonian is taken to be diagonal in the e_ε-basis

$$H_S := \sum_{\varepsilon \in \{0,1\}} E_\varepsilon |e_\varepsilon\rangle\langle e_\varepsilon| = E_0 |e_0\rangle\langle e_0| + E_1 |e_1\rangle\langle e_1|$$

and the energy levels are ordered so that $E_0 < E_1$. Thus there is a single Bohr frequency $\omega_0 := E_1 - E_0 > 0$. The one-particle field Hamiltonian is

$$S_t g(k) = e^{it\omega(k)} g(k) ,$$

where $\omega(k)$ is a function satisfying the basic analytical assumption of the stochastic limit. Its second quantization is the free field evolution

$$e^{itH_0} A^\pm g e^{-itH_0} = A^\pm_{S_t g}$$

We can distinguish two cases as below, which correspond to two cases of Sect. 3, i.e., $q > 0$ and $q = 0$.

Case 1

If $\alpha_0, \alpha_1 \neq 0$, then, according to the general theory of stochastic limit (i.e., $t \to t/\lambda^2$) [1], the interaction Hamiltonian H_I is in the same universality class as

$$\widetilde{H}_I = D \otimes A_g^+ + D^+ \otimes A_g ,$$

where $D := |e_0\rangle\langle e_1|$ (this means that the two interactions have the same stochastic limit). The interaction Hamiltonian at time t is then

$$\widetilde{H}_I(t) = e^{-it\omega_0} D \otimes A^+_{S_t g} + \text{ h.c.} = D \otimes A^+(e^{it(\omega(p) - \omega_0)} g) + \text{ h.c.}$$

and the white noise ($\{b_t\}$) Hamiltonian equation associated, via the stochastic golden rule, to this interaction Hamiltonian is

$$\partial_t U_t \;=\; i(Db_t^+ + D^+ b_t)U_t \,.$$

Its causally normal ordered form is equivalent to the stochastic differential equation

$$dU_t \;=\; (iDdB_t^+ + iD^+ dB_t - \gamma_- D^+ D dt)U_t \,,$$

where $dB_t := b_t dt$.

The causally ordered inner Langevin equation is

$$\begin{aligned} dj_t(x) &= dU_t^* x U_t + U_t^* x dU_t + dU_t^* x dU_t \\ &= U_t^*(-iD^+ x dB_t - iDx dB_t^+ - \overline{\gamma}_- D^+ D x dt + ix D dB_t^+ \\ &\quad + ix D^+ dB_t - \gamma_- x D^+ D dt + \gamma_- D^+ x D dt)U_t \\ &= ij_t([x, D^+])dB_t + ij_t([x, D])dB_t^+ \\ &\quad -(\mathrm{Re}\ \gamma_-)j_t(\{D^+ D, x\})dt + i(\mathrm{Im}\,\gamma_-)j_t([D^+ D, x])dt \\ &\quad +j_t(D^+ x D)(\mathrm{Re}\ \gamma_-)dt \,, \end{aligned}$$

where $j_t(x) := U_t^* x U_t$. Therefore the master equation is

$$\begin{aligned} \frac{d}{dt} P^t(x) &= (\mathrm{Im}\,\gamma)i[D^+ D, P^t(x)] - (\mathrm{Re}\,\gamma_-)\{D^+ D, P^t(x)\} \\ &\quad + (\mathrm{Re}\ \gamma_-)D^+ P^t(x) D \,, \end{aligned}$$

where $D^+ D = |e_1\rangle\langle e_1|$ and $D^+ x D = \langle e_0, x e_0\rangle |e_1\rangle\langle e_1|$.

The dual Markovian evolution P_*^t acts on density matrices and its generator is

$$L_*\rho \;=\; (\mathrm{Im}\,\gamma_-)i[\rho, D^+ D] - (\mathrm{Re}\ \gamma_-)\{\rho, D^+ D\} + (\mathrm{Re}\ \gamma_-)D\rho D^+ \,.$$

Thus, if $\rho_0 = |e_0\rangle\langle e_0|$ one has

$$L_*\rho_0 \;=\; 0$$

so ρ_0 is an invariant measure. From the Fagnola-Rebolledo criteria [26], it is the unique invariant measure and the semigroup $\exp(tL_*)$ converges exponentially to it.

Case 2

If $\alpha_1 = 0$, then the interaction Hamiltonian H_I is

$$H_I \;=\; \lambda |e_0\rangle\langle e_0| \otimes (A_g^+ + A_g)$$

and, according to the general theory of stochastic limit, the reduced evolution has no damping and corresponds to the pure Hamiltonian

$$H_S + |e_0\rangle\langle e_0| \;=\; (E_0 + 1)|e_0\rangle\langle e_0| + E_1 |e_1\rangle\langle e_1|$$

therefore, if we choose the eigenvalues E_1, E_0 to be integers (in appropriate units), then the evolution will be periodic.

Since the eigenvalues E_1, E_0 can be chosen a priori, by fixing the system Hamiltonian H_S, it follows that the period of the evolution can be known a priori. This gives a simple criterion for the solvability of the SAT problem because, by waiting a sufficiently long time one can experimentally detect the difference between damping and an oscillatory behaviour.

The precise estimate of this time can be achieved either by theoretical methods or by computer simulation. Both methods will be analyzed in the expanded paper [3].

Czachor [9] gave an example of a nonlinear Schrödinger equation to distinguish two cases, similar to $\alpha_1 \neq 0$ and $\alpha_1 = 0$ given above, in a certain oracle computation. We used the resulting (flag) state after quantum computation of the truth function of SAT to couple the external field and took the stochastic limit, then our final evolution becomes “linear” for the state ρ described as above. The stochastic limit is historically important to realize macroscopic (time) evolution and it is now rigorously established as explained in [1], and we gave a general protocol to study the distinction of two cases $\alpha_1 \neq 0$ and $\alpha_1 = 0$ by this rigorous mathematics. The macro-time enables us to measure the behavior of the outcomes practically. Thus our approach is conceptually different from Czachor's. Moreover Czachor discussed that some expectation value is constant for the case $\alpha_1 = 0$ and oscilating for $\alpha_1 \neq 0$, and ours gives the detail behavior of the state w.r.t the macro-time; damping ($\alpha_1 \neq 0$ case) and oscilating ($\alpha_1 = 0$ case)

6. Conclusion

We showed in [10, 12, 13] that we can find an algorithm solving the SAT problems in polynomial number of steps by combining a quantum algorithm with chaotic dynamics. We used the logistic map there, however it is possible to use other chaotic maps if they can amplify one of two coefficients. In this short paper we pointed out that it is possible to distinguish two different states, $\sqrt{1-q^2}\,|0\rangle + q\,|1\rangle$ ($q \neq 0$) and $|0\rangle$ by means of an adaptive dynamics and the stochastic limit. Finally we remark that our algorithms can be described by deterministic general quantum Turing machine [24, 4], whose result is based on the general quantum algorithm mentioned in Sect. 2.

Acknowledgment

The authors thank SCAT for financial support of this joint work. We thank the referee for informing us about the paper of Czachor.

Bibliography

[1] L. Accardi, Y. G. Lu, I. Volovich, *Quantum Theory and its Stochastic Limit*, Springer Verlag 2002, Japanese translation, Tokyo-Springer, 2003.

[2] L. Accardi and M. Ohya, *Compound channels, transition expectations, and liftings*, Appl. Math. Optim. **39**, 33 (1999).

[3] L. Accardi and M. Ohya, *A stochastic limit approach to the SAT problem*, in preparation.

[4] L. Accardi and M. Ohya, *Generalized Quantum Turing machine and stochastic limit for the SAT problem*, TUS preprint.

[5] L. Accardi, R. Sabbadini, *On the Ohya-Masuda quantum SAT Algorithm*, in: Proceedings Intern.Conf. "Unconventional Models of Computations", I. Antoniou, C. S. Calude, M. Dinneen, eds., Springer 2001; Preprint Volterra, N. 432, 2000

[6] L. Accardi, R.Sabbadini, *A Generalization of Grover's Algorithm*, Proceedings Intern. Conf.: Quantum Information III, Meijo University, Nagoya, 27-31 March, 2001; World Scientific 2002; qu-phys 0012143; Preprint Volterra, N. 444, 2001.

[7] L. Accardi and K. Imafuku, *Control of Quantum States by Decoherence*, Volterra Center Preprint No. 542.

[8] D. S. Abrams and S. Lloyd, *Nonlinear quantum mechanics implies polynomial time solution for NP-complete and #P problem*, Phys. Rev. Lett. **81**, 3992 (1998).

[9] M. Czachor, *Notes on nonlinear quantum algorithm*, Acta Phys. Slov. **48**, 157 (1998).

[10] M. Ohya and N. Masuda, *NP problem in Quantum Algorithm,* Open Sys. Information Dyn. **7**, 33 (2000).

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

[12] 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 and J. Opt. B **5**, 639 (2003).

[13] M. Ohya and I. V. Volovich, *New quantum algorithm for studying NP-complete problems*, Rep. Math. Phys.**52**, 25 (2003).

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

[15] 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.

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

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

[18] 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.

[19] M. Ohya, *Complexities and Their Applications to Characterization of Chaos,* Int. Journ. of Theort. Phys. **37**, 495 (1998).

[20] M. Ohya and I. V. Volovich, *Quantum information, computation, cryptography and teleportation*, Springer, to appear.

[21] 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.

[22] A. Ekert and R. Jozsa, *Quantum computation and Shor's factoring algorithm*, Reviews of Modern Physics **68**, 733 (1996).

[23] S. Iriyama and S. Akashi, *Complexity of Ohya-Masuda-Volovich algorithm*, to appear.

[24] S. Iriyama and M. Ohya, *On generalized Turing machine*, TUS (Tokyo University of Science) preprint, 2003.

[25] A. Kossakowski, M. Ohya and Y. Togawa, *How can we observe and describe chaos?*, Open Sys. Information Dyn. **10**, 221 (2003).

[26] F. Fagnola and R. Rebolledo, *On the existence of Stationary States for Quantum Dynamical Semigroups*, to appear in J. Math. Phys., 2001.