一般化量子チューリング機械について

入山 聖史，大矢 雅則
Satoshi Iriyama and Masanori Ohya
東京理科大学 情報科学科
Tokyo University of Science
Depertment of Information Science

Abstract

Ohya and Volovich have proposed a new quantum computation model with chaotic amplification to solve the SAT problem, which went beyond usual quantum algorithm. In this paper, we generalize quantum Turing machine by rewriting usual quantum Turing machine in terms of channel transformation. Moreover, we define some computational classes of generalized quantum Turing machine and show that we can treat the Ohya-Volovich (OV) SAT algorithm.

1 Introduction

The problem whether NP-complete problems can be P problem has been considered as one of the most important problems in theory of computational complexity. Various studies have been done for many years. Ohya and Volovich [1, 2] proposed a new quantum computation model with chaotic amplification process to solve the SAT problem, which went beyond usual quantum algorithm. This quantum chaos algorithm enabled to solve the SAT problem in a polynomial time [1, 2, 3].

In this paper we generalize quantum Turing machine so that it enables to describe non-unitary evolution of states, we show GQTM for the OV SAT algorithm referring to the paper [9] and calculate the computational complexity of GQTM for the OV SAT algorithm. This study is based on mathematical studies of quantum communication channels [4, 5].

2 Generalized Quantum Turing Machine

Classical Turing machine(TM or CTM) M_{cl} is defined by a triplet (Q, Σ, δ), where Σ is a finite alphabets with an identified blank symbol #, Q is a finite set of states (with an initial state q_0 and a set of final states q_f) and $\delta : Q \times \Sigma \rightarrow Q \times \Sigma \times \{-1, 0, 1\}$ is a transition function. Note that $\{-1, 0, 1\}$ indicates moving direction of the tape head of TM. The deterministic TM has a deterministic transition function $\delta : Q \times \Sigma \rightarrow 2^{Q} \times \Sigma \times \{-1, 0, 1\}$, that is, δ is a non-branching map, in other words, the range of δ for each $(q, a) \in Q \times \Sigma$ is unique. A TM M is called non-deterministic if it is not deterministic.

In this section, we introduce a generalized quantum Turing machine (GQTM), which contains QTM as a special case.

Definition 1 *Usual Quantum Turing machine M_q is defined by a quadruplet $M_q = (Q, \Sigma, \mathcal{H}, U)$, where $\mathcal{H}$ is a Hilbert space described below in (2.1)and U is a unitary operator on the space $\mathcal{H}$ of the special form described below in (2.2).*

Let $\mathcal{C} = Q \times \Sigma \times \mathbb{Z}$ be the set of all classical configurations of the Turing machine M_{cl}, where $\mathbb{Z}$ is the set of all integers. It is a countable set and one has

$$\mathcal{H} = \left\{ \varphi \mid \varphi : \mathcal{C} \rightarrow \mathbb{C}; \sum_{C \in \mathcal{C}} |\varphi(C)|^2 < \infty \right\}. \tag{2.1}$$

Since the configuration of TM can be written as $C = (q, A, i)$ one can say that the set of functions $\{| \, q, A, i >\}$ is a basis in the Hilbert space $\mathcal{H}$. Here $q \in Q$, $i \in \mathbb{Z}$ and A is a function $A : \mathbb{Z} \rightarrow \not\prec$. We will call this basis the *computational basis.*

By using the computational basis we now state the conditions to the unitary operator U. We denote the set $\Gamma \equiv \{1, 0, -1\}$. One requires that there is a function $\delta : Q \times \Sigma \times Q \times \Sigma \times \Gamma \rightarrow \widetilde{\mathbb{C}}$ which takes values in the field of computable numbers $\widetilde{\mathbb{C}}$ and such that the following relation is satisfied:

$$U \left| q, A, i \right\rangle = \sum_{p,b,\sigma} \delta(q, A(i), p, b, \sigma) \left| p, A_i^b, i + \sigma \right\rangle . \tag{2.2}$$

Here the sum runs over the states $p \in Q$, the symbols $b \in \Sigma$ and the elements $\sigma \in \Gamma$. Actually this is a finite sum. The function $A_i^b : \mathbb{Z} \to \nless$ is defined as

$$A_i^b(j) = \begin{cases} b \text{ if } j = i, \\ A(j) \text{ if } j \neq i. \end{cases}$$

Note that if, for some integer $t \in \mathbb{N} \equiv \{1, 2, ...\}$, the quantum state $U^t |q_0, A, 0\rangle$ is a final quantum state, i.e. $\|E_Q(q_F)U^s |q_0, A, 0\rangle\| = 1$ and for any $s < t$, $s \in \mathbb{N}$ one has $\|E_Q(q_F)U^s |q_0, A, 0\rangle\| = 0$, then one says that the quantum Turing machine *halts with running time* t on input A.

Now we define the generalized quantum Turing machine (GQTM) by using of a channel Λ (see below) instead of a unitary operator U.

Definition 2 *Generalized Quantum Turing machine M_{gq} (GQTM) is defined by a quadruplet $M_{gq} = (Q, \Sigma, \mathcal{H}, \Lambda)$, where Q and Σ are two alphabets, $\mathcal{H}$ is a Hilbert space and Λ is a channel on the space of states on $\mathcal{H}$ of the special form described below.*

Q and Σ are represented by a density operator on Hilbert space $\mathcal{H}_Q$ and $\mathcal{H}_\Sigma$,which are spanned by canonical basis $\{|q\rangle \,; q \in Q\}$ and $\{|a\rangle \,; a \in \Sigma\}$, respectively. A tape configuration A is a sequence of elements of Σ represented by a density operator on Hilbert space $\mathcal{H}_\Sigma$ spanned by a canonical basis $\{|A\rangle \,; A \in \Sigma^*\}$, where Σ^* is the set of sequences of alphabets in Σ. A position of tape head is represented by a density operator on Hilbert space $\mathcal{H}_Z$ spanned by a canonical basis $\{|i\rangle \,; i \in \mathbf{Z}\}$. Then a configuration ρ of GQTM M_{gq} is described by a density operator on $\mathcal{H} \equiv \mathcal{H}_Q \otimes \mathcal{H}_\Sigma \otimes \mathcal{H}_Z$. Let $\mathfrak{S}(\mathcal{H})$ be the set of all density operator on Hilbert space $\mathcal{H}$. A quantum transition function Λ is given by a completely positive (CP) channel

$$\Lambda : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\mathcal{H}).$$

For instance, given a configuration $\rho \equiv \sum_k \lambda_k |\psi_k\rangle \langle\psi_k|$, where $\sum \lambda_k = 1, \lambda_k \geq 0$ and $\psi_k = |q_k\rangle \otimes |A_k\rangle \otimes |i_k\rangle$ $(q_k \in Q, A_k \in \Sigma^*, i_k \in \mathbf{Z})$ is a vector in a basis of $\mathcal{H}$. This configuration changes to a new configuration ρ' by one step transition as $\rho' = \Lambda(\rho) = \sum_k \mu_k |\psi_k\rangle \langle\psi_k|$ with $\sum \mu_k = 1, \mu_k \geq 0$.

For any configuration ρ, GQTM M_{gq} is called UQTM M_{uq} if the quantum transition function δ of GQTM M_{gq} is given by

$$\Lambda_\delta(\rho) = U_\delta \rho U_\delta^*,$$

where U_δ is a unitary operator in $\mathcal{H}$. Obviously $M_{uq} = M_q$. Several studies have been done on QTM whose transition function is represented by unitary operator.

A transition of GQTM is regarded as a transition of amplitude of each configuration vector. We categorize GQTMs by a property of CP channel Λ as below.

Definition 3 *A GQTM M_{gq} is called unitary QTM (UQTM, i.e., usual QTM), if all of quantum transition function Λ in M are unitary CP channel.*

For all configuration $\rho = \sum_n \lambda_n \rho_n$ $(\Sigma_n \lambda_n = 1, \lambda_n \geq 0)$, a GQTM M_{gq} is called LQTM M_{lq} if Λ is affine ; $\Lambda\left(\sum_n \lambda_n \rho_n\right) = \sum_n \lambda_n \Lambda\left(\rho_n\right)$. Since a measurement defined by $\Lambda_M \rho = \sum\limits_k P_k \rho P_k$ with a PVM $\{P_k\}$ on $\mathcal{H}$ is a linear CP channel, LQTM may include a measurement process.

For a more general channel the state change is expressed as

$$\begin{aligned}\Lambda(\left|q, A\left(i\right), i\right\rangle \left\langle q, A\left(i\right), i\right|) = &\sum_{p,b,\sigma,p',b',\sigma'} \delta(q, A(i), p, b, \sigma, p', b', \sigma') \\ &\left|p, A_i^b, i+\sigma\right\rangle \left\langle p, A_i^{b'}, i+\sigma\right|\end{aligned}$$

with some function $\delta(q, A(i), p, b, \sigma, p', b', \sigma')$ such that the RHS of this relation is a state.

Thus we define two more classes of GQTM for non-unitary CP channels.

Definition 4 *A GQTM M_{gq} is called a linear QTM(LQTM) if its quantum transition function Λ is a linear quantum channel.*

Unitary operator is linear, hence UQTM is a sub-class of LQTM. moreover, classical TM is a special class of LQTM.

Definition 5 *A GQTM M_{gq} is called non-linearQTM(NLQTM) if its quantum transition function Λ contains non-linear CP channel.*

A chaos amplifier used in [1, 2] is a non-linear CP channel, the details of this channel and its application to the SAT problem will be discussed in the sequel.

2.1 Computational class for GQTM

Given a GQTM $M_{gq} = (Q, \Sigma, \delta)$ and an input configuration $\rho_0 = |v_{in}\rangle \langle v_{in}|$, $(|v_{in}\rangle = |q_0\rangle \otimes |T\rangle \otimes |0\rangle)$, a computation process is described as the following product of channels

$$\Lambda_1 \circ \cdots \circ \Lambda_t (\rho_0) = \rho_f \equiv |v_f\rangle \langle v_f|$$

where $\Lambda_1, \cdots, \Lambda_t$ are CP channels. Applying the CP channels to an initial state, we obtain a final state ρ_f and we measure this state by a projection (or PVM)

$$P_f = |q_f\rangle \langle q_f| \otimes I_\Sigma \otimes I_Z,$$

where I_Σ, I_Z are identity operators on $\mathcal{H}_\Sigma, \mathcal{H}_Z$, respectively. Let $p \geq 0$ be a halting probability such that

$$tr_{\mathcal{H}_\Sigma \otimes \mathcal{H}_Z} (P_f \rho_f) = p |q_f\rangle \langle q_f| .$$

Then, we define the *acceptance (rejection)* of GQTM and some classes of languages.

Definition 6 *Given GQTM M_{gq} and a language L, if there exists t steps when we obtain the configuration of acceptance (or rejection)by the probability p, we say that the GQTM M_{gq} accepts (or rejects)L by the probability p, and its computational complexity is t.*

Definition 7 *A language L is bounded quantum probability polynomial time GQTM(BGQPP) if there is a polynomial time GQTM M_{gq} which accepts L with probability $p \geq \frac{1}{2}$.*

If NLQTM accepts the SAT OV algorithm in polynomial time with probability $p \geq \frac{1}{2}$, then we may have the inclusion

$$NP \subseteq BGQPP.$$

where NP is a language class that a deterministic Turing machine, which recognize with some informations in polynomial time of input size exists.

3 SAT Problem

Let $X \equiv \{x_1, \ldots, x_n\}, n \in \mathbf{N}$ be a set. x_k and its negation $\overline{x}_k\,(k = 1, \ldots, n)$ are called literals Let $\overline{X} \equiv \{\overline{x_1}, \ldots, \overline{x_n}\}$ be a set, then the set of all literals is denoted by $X' \equiv X \cup \overline{X} = \{x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n}\}$. 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 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, that of $C$ is false. Take 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 $\wedge$, 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 $C_j\,(j = 1, 2, \cdots, m)$ 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 8 *SAT Problem: Given a Boolean set $X \equiv \{x_1, \cdots, x_n\}$and a set $\mathcal{C} = \{C_1, \cdots, C_m\}$ of clauses, determine whether $\mathcal{C}$ is satisfiable or not.*

4 SAT algorithm in GQTM

In this section, we construct a GQTM for the OV SAT algorithm. OV SAT algorithm is a quantum algorithm with the chaos amplifier explained in the paper [1, 2, 6]. The GQTM with the chaos amplifier belongs to NLQTM because the chaos amplifier is represented by non-linear CP channel. The OV algorithm runs from an initial state $\rho_0 \equiv |v_0\rangle \langle v_0|$ to $\overline{\rho}_k$ through $\rho \equiv |v_f\rangle \langle v_f|$. The computation from $\rho_0 \equiv |v_0\rangle \langle v_0|$ to $\rho \equiv |v_f\rangle \langle v_f|$ is due to unitary channel $\Lambda_C \equiv U_C \bullet U_C$, and that from $\rho \equiv |v_f\rangle \langle v_f|$ to $\overline{\rho}_f$ is due to a non-unitary channel $\Lambda_{CA}^k \circ \Lambda_I$, so that all computation can be done by $\Lambda_{CA}^k \circ \Lambda_I \circ \Lambda_C$, which is a completely positive, so the whole computation process is deterministic (see [9]). It is a multi-track (actually 4 tracks) GQTM that represents this whole computation process.

A multi-track GQTM has some workspaces for calculation, whose tracks are independent each other. This independence means that the TM can operate only one track at one step and all tracks do not affect each other. Let us explain our computation by a multi-track GQTM. The first track stores the input data and the second track stores the value of literals. The third track is used for the computation of $t(C_i), (i = 1, \cdots, m)$ described by unitary operators. The fourth track is used for the computation of $t(\mathcal{C})$ denoting the result. The work of GQTM is represented by the following 8 steps:

- Step 1 : Store the counter $c = 0$ in Track 1. Calculate $\left[\frac{5}{4}(n-1)\right] + 1$, we take this value as the maximum value of the counter. Then, store it in Track 4.
- Step 2 : Calculate $c + 1$ and store it in Track 4.
- Step 3 : Apply the Hadamard transform to Track 2.
- Step 4 : Calculate $t(C_1), \cdots t(C_m)$ and store them in Track 3.
- Step 5 : Calculate $t(\mathcal{C})$ by using the value of the third track, and store $t(\mathcal{C})$ in Track 4.
- Step 6 : Empty the first, second and third Tracks.
- Step 7 : Apply the chaos amplifier to the result state obtained up to the step 6.
- Step 8 : If $c = \left[\frac{5}{4}(n-1)\right] + 1$ or GQTM is in the final state, GQTM halts. If GQTM is not in the final state, GQTM runs the step 2 to the step 8 again.

The detail of this quantum algorithm is explained in the paper [9].

4.1 Computational complexity of the SAT algorithm

We define the computational complexity of the OV SAT algorithm as the product of $T_Q\left(U_{\mathcal{C}}^{(n)}\right)$ and $T_{CA}(n)$,where $T_Q\left(U_{\mathcal{C}}^{(n)}\right)$ is the complexity of unitary computation and $T_{CA}(n)$ is that of chaos amplification.

The following theorem is essentially discussed in [7, 2, 3].

Theorem 9 *For a set of clauses $\mathcal{C}$ and n Boolean variables, the computational complexity of the OV SAT algorithm including the chaos amplifier, denoted by $T(\mathcal{C}, n)$, is obtained as follows.*

$$T_{GQTM}(\mathcal{C}, n) = T_Q\left(U_{\mathcal{C}}^{(n)}\right) T_{CA}(n) = O(poly(n)),$$

where $poly(n)$ denotes a polynomial of n.

The computational complexity of quantum computer is determined by the total number of logical quantum gates. This inequality implies that the computational complexity of SAT algorithm is bounded by $\mathcal{O}(n)$ for the size of input n while a classical algorithm is bounded by $\mathcal{O}(2^n)$.

References

[1] M.Ohya and I.V.Volovich, *Quantum computing and chaotic amplification*, J. opt. B, **5**,No.6 639-642, 2003.

[2] M.Ohya and I.V.Volovich, *New quantum algorithm for studying NP-complete problems*, Rep.Math.Phys., **52**, No.1,25-33 2003.

[3] M.Ohya and N.Masuda, *NP problem in Quantum Algorithm,* Open Systems and Information Dynamics, 7 No.1 33-39, 2000.

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

[5] L.Accardi and M.Ohya, Compound channels, transition expectations, and liftings, Appl. Math. Optim., Vol.39, 33-59, 1999.

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

[7] S.Akashi and S.Iriyama, Estimation of Complexity for the Ohya-Masuda-Volovich SAT Algorithm (to appear).

[8] C.H.Bennett, E.Bernstein, G.Brassard, U.Vazirani, *Strengths and Weaknesses of Quantum Computing*, SICOMP Vol. 26 Number 5 pp. 1510-1523. 1997.

[9] S.Iriyama, M.Ohya and I.V.Volovich, Generalized Quantum Turing Machine and its Application to the SAT Chaos Algorithm, TUS preprint.