2009－MPS－73 (28)
2009／3／5

一般化量子チューリング機械の数理モデルとNP完全問題の量子アルゴリズム

入山 聖史† 大矢 雅則†

† 東京理科大学理工学部情報科学科

概要: 量子力学を原理とした計算機の数理モデルとして，一般化量子チューリング機械が提案されている．本講演では，その定義と言語クラスを説明し，NP完全問題に対する量子アルゴリズムを示し，その計算の複雑さを議論する．

On Generalized Quantum Turing Machine and Quantum Algorithm for NP Complete Problem

Satosh Iriyama† Masanori Ohya†

†Department of Information Sciences, Tokyo University of Science

Abstract: Ohya and Volovich proposed a quantum algorithm for SAT problem which belongs to NP compelte. We defined a mathematical model of quantum computation called a generalised quantum Turing machine and discussed a computational complexity of it. In this talk, we explain the definition of it and language classes. Moreover, we show the quantum algorithm for the NP complete problem.

1 序

我々はヒルベルト空間上の量子チャネルと密度作用素を用いて，一般化量子チューリング機械（GQTM）を定義した [7, 9]．これは，量子アルゴリズムとして，観測過程やその他の物理過程を含む形での一般化であり，これにより，量子力学を原理とした計算モデルを記述できることになる．さらに，このGQTMを考えることにより，量子計算における計算の複雑さを定義することができ，厳密な計算量を導出することができる．これを用いて，OMV-SATアルゴリズムの計算量が求められており，量子アルゴリズムと，ある増幅過程を用いれば，NP完全問題が多項式解けるということが示されている [1, 2, 3, 8]．

本講演では，まずGQTMの定義と，計算過程を説明し．言語クラスとその包含関係を説明する．そして，NP完全問題の一つであるSAT問題について説明し，SAT問題を多項式時間で解く量子アルゴリズムのGQTMでの記述を示し，その計算の複雑さを議論する．

2 一般化量子チューリング機械

GQTM M_{gq} は，次の4つ組 $(Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ で与えられる．ここで，Λ_δ は様相（configuration）から様相への量子遷移関数，Q と Σ はそれぞれ標準的な基底 $\{|q\rangle\,; q \in Q\}$ と $\{|a\rangle\,; a \in \Sigma\}$ によって張られるヒルベルト空間 $\mathcal{H}_Q$ と $\mathcal{H}_\Sigma$ 上の密度作用素の集合である．テープ状態 A は，Σ の要素からなる配列で標準的な基底 $\{|A\rangle\,; A \in \Sigma^*\}$ によって張られるヒルベルト空間 $\mathcal{H}_\Sigma$ 上の密度作用素で表される．ここで Σ^* はアルファベット Σ の要素のすべての配列である．テープの位置は標準的な基底 $\{|i\rangle\,; i \in \mathbb{Z}\}$ によって張られるヒルベルト空間 $\mathcal{H}_Z$ 上の密度作用素で表される．GQTM M_{gq} の様相 ρ はヒルベルト空間 $\mathcal{H} \equiv \mathcal{H}_Q \otimes \mathcal{H}_\Sigma \otimes \mathcal{H}_Z$ 上の密度

作用素で表される．ここで，$\mathfrak{S}(\mathcal{H})$ を $\mathcal{H}$ 上のすべての密度作用素の集合とする．

次の遷移関数 δ_1 を考える．

$$\delta_1 : \mathbb{R} \times Q \times \Sigma \times Q \times \Sigma \times Q \times \Sigma \times \{0, \pm 1\} \times Q \times \Sigma \times \{0, \pm 1\} \to \mathbb{C}.$$

量子遷移関数は次の準線形完全正チャネルで与えられる．

$$\Lambda_\delta : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\mathcal{H}),$$

これは，次の条件を満たす．

定義 1

すべての様相 $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|, |\psi_k\rangle = \sum_l \alpha_{k,l} |q_{k,l}, A_{k,l}, i_{k,l}\rangle, \sum_k \lambda_k = 1, \forall \lambda_k \geq 0, \sum_l |\alpha_{k,l}|^2 = 1, \forall \alpha_{k,l} \in \mathbb{C}$ に対して，遷移関数 δ_1 が存在して，Λ_δ が次のように書け，RHS が状態となるとき，Λ_δ は量子遷移関数と呼ばれる．

$$\Lambda_\delta(\rho) = \sum_{k,l,m,n,p,b,d,p',b',d'} \delta_1(\lambda_k, q_{k,l}, A_{k,l}(i_{k,l}), , q_{m,n}, A_{m,n}(i_{m,n}), p, b, d, p', b', d') \times |p, B, i_{k,l} + d\rangle\langle p', B', i_{m,n} + d'|$$

$$B(j) = \begin{cases} b & j = i_{k,l} \\ A_{k,l}(j) & \text{otherwise} \end{cases}$$

$$B'(j) = \begin{cases} b' & j = i_{m,n} \\ A_{m,n}(j) & \text{otherwise} \end{cases}$$

定義 2

すべての様相 ρ_k に対して，遷移関数

$$\delta_2 : Q \times \Sigma \times Q \times \Sigma \times Q \times \Sigma \times \{0, \pm 1\} \times Q \times \Sigma \times \{0, \pm 1\} \to \mathbb{C}$$

が存在して，Λ_δ が次のように書け，

$$\Lambda_\delta(\rho_k) = \sum_{k,l,m,n,p,b,d,p',b',d'} \delta_2(q_{k,l}, A_{k,l}(i_{k,l}), , q_{m,n}, A_{m,n}(i_{m,n}), p, b, d, p', b', d') \times |p, B, i_{k,l} + d\rangle\langle p', B', i_{m,n} + d'|$$

RHS が状態であるとき，$M_{gq} = (Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ は LQTM と呼ばれる．すべての様相 $\sum_k \lambda_k \rho_k$ に対して，Λ_δ は次のアフィン性をもつ;

$$\Lambda_\delta\left(\sum_k \lambda_k \rho_k\right) = \sum_k \lambda_k \Lambda_\delta(\rho_k)$$

定義 3

Λ_δ がユニタリーチャネル：$\Lambda_\delta = Ad_{U_\delta}$ であるとき，GQTM M_{gq} は UQTM と呼ばれる．ここで，$|\psi\rangle = |q, A, i\rangle$ に対して U_δ は次のようになる．

$$U_\delta |\psi\rangle = U_\delta |q, A, i\rangle = \sum_{p,b,r} \delta_3(q, A(i), p, b, d) |p, B, i + d\rangle$$

ここで

$$\delta_3 : Q \times \Sigma \times Q \times \Sigma \times \{0, 1\} \to \mathbb{C}$$

はすべての $q \in Q, a \in \Sigma$, $q'(\neq q) \in Q, a'(\neq a) \in \Sigma$ に対して次を満たす．

$$\sum_{p,b,d} |\delta_3(q, a, p, b, d)|^2 = 1.$$

$$\sum_{p,b,d,d'} \delta_3(q', a', p, b, d')^* \delta_3(q, a, p, b, d) = 0.$$

[1, 2] において，SAT 問題を多項式時間で解くために用いられるカオス増幅器は，非線形チャネルであり，[7] で GQTM による表現がなされている．

2.1 GQTM の計算過程

$M = (Q, \Sigma, \mathcal{H}, \Lambda_\delta)$, $\rho_0 = |\psi_0\rangle\langle\psi_0|$, $|\psi_0\rangle = |q_0, A, 0\rangle$ とする．A の初期状態を M の入力と呼ぶ．GQTM における計算過程は Λ_δ を初期様相 ρ_0 に及ぼすことにより進行し，プロセッサ状態が終状態の集合 $\{q_F\}$ に入るまで繰り返され，停止する．この過程は，Λ_δ を用いて次のように記述される．

$$\Lambda_\delta \circ \cdots \circ \Lambda_\delta(\rho_0) = \rho_f$$

ρ_f は終状態で，次のように表される．

$$\rho_f = \sum_k \lambda_k \rho_k + \sum_l \mu_l \sigma_l$$

$$\sum_k \lambda_k + \sum_l \mu_l = 1, \quad \forall \lambda_k, \mu_l \geq 0$$

ここで，$\sigma_l \uparrow H_Q \in \{q_F\}$ である．$p = \sum_l \mu_l$ は停止確率とよばれる．

2.2 GQTMにおける言語クラス

本節では，GQTMを用いて定義される言語クラスを説明する．L をアルファベット列とする．$x \in L$ で停止し，$x \notin L$ で停止しないTM（またはGQTM）が存在するとき，L を言語といい，M は L を認識するという．

定義 4
言語 L に対しあるGQTM（UQTM, LQTM）M_{gq} が存在し，M_{qg} は L を多項式時間で確率 $p \geq \frac{1}{2}$ で停止するとき，L はクラスBGQPP（BUQPP = BPP，BLQPP）に属する．

LQTMはCTMを含むことから，次の包含関係が成り立つ．

$$BPP \subseteq BLQPPL \subseteq BGQPP.$$

3 OMV SATアルゴリズムのGQTMにおける計算の複雑さ

SAT問題はNP完全問題の一つであり，Ohya, Masuda,Volovichは量子アルゴリズムとある増幅過程を用いて，多項式時間でSAT問題を解くアルゴリズム（OMV-SATアルゴリズム）を提案した[1, 2, 4]．さらにOhya，SIは与えられた問題に対し，時間計算量，領域計算量を厳密に導出した[8]．本節では，SAT問題を説明し，OMV-SATアルゴリズムのGQTMでの記述を説明する．

$X^+ = \{x_1, \cdots, x_n\}$ を論理変数の集合とし，$X^- = \{\bar{x}_1, \cdots, \bar{x}_n\}$ をその否定とする．$X = X^+ \cup X^-$ をリテラルといい，すべてのリテラルの部分集合を $F(X)$ とする．関数 $t : F(X) \to \{0,1\}$ を割り当てといい，

$$t(x) = 1 - t(\bar{x})$$

を満たす．$C_k \in F(X)$ を節（closure）といい，$\mathcal{C}$ を節の集合とする．いま，$\mathcal{C} = \{C_1, \cdots, C_m\}$ に対して論理式

$$f(\mathcal{C}) \equiv \wedge_{i=1}^{m} \vee_{x_j \in C_i} t(x_j)$$

を定め，次の問題を考える．

問題 5 (SAT問題)
$f(\mathcal{C}) = 1$ となる割り当て t は存在するか（satisfiable）．

あるリテラル X に対し，t の取り方は $2^{card(X)}$ 個あるため，SAT問題はNPに属し，他のNP問題に帰着される（Cook-Levin）ため，NP完全問題である．

定理 6
SAT問題を多項式時間で判定する3マルチトラックGQTMが存在する[9]．

$M_{SAT} = \left(Q, \Sigma^3, \mathcal{H}, \Lambda_{SAT}\right)$ を3マルチトラックGQTMとする．$\rho_0 \equiv |v_0\rangle \langle v_0|, |v_0\rangle = |q_0, A, 0\rangle$ を初期状態，$A = (A_1, A_2, A_3), A_1, A_2, A_3 \in \Sigma^*$ を3マルチトラックテープとする．Λ_{SAT} は次の3つの量子遷移関数で表される．

$$\Lambda_{SAT} = \Lambda_{CA}^{k} \circ \Lambda_T \circ \Lambda_C$$

ここで，Λ_C はすべての割り当てについて $f(\mathcal{C})$ を計算するユニタリーチャネル，Λ_T は線形チャネル，Λ_{CA}^{k} はOMV-SATアルゴリズムにおけるカオス増幅器と同じ動作を行う非線形量子チャネルである．

$\Lambda_T \circ \Lambda_C$ を初期状態に及ぼし，次の ρ_6 を得る．

$$\begin{aligned}
&\Lambda_T \circ \Lambda_C(\rho_0) \\
&= q^2 |q_f, (A_1, A_2, A_3), 0\rangle \langle q_f, (A_1, A_2, A_3), 0| \\
&+ \left(1 - q^2\right) |q_6, (B_1, B_2, B_3), 0\rangle \langle q_6, (B_1, B_2, B_3), 0| \\
&= \rho_6
\end{aligned}$$

ここで，すべての $i \in \mathbb{Z}$ について，

$$\begin{aligned}
A_1(i) &= A_2(i) = \# \\
B_1(i) &= B_2(i) = \#
\end{aligned}$$

であり，

$$A_3(i) = \begin{cases} 1 & i = 0 \\ \# & \text{otherwise} \end{cases} \quad \text{(satisffiable)}$$

$$B_3(i) = \begin{cases} 0 & i = 0 \\ \# & \text{otherwise} \end{cases} \quad \text{.(not satisffiable)}$$

である．

Λ_{CA} は δ_1 により次のように定義される.

$$\delta_1\left(1-q^2,q_6,0,q_6,0,q_6,0,0,q_6,0,0\right)\equiv 1-g\left(q^2\right)$$
$$\delta_1\left(q^2,q_f,1,q_f,1,q_f,1,0,q_f,1,0\right)\equiv g\left(q^2\right).$$

ここで, g は

$$g(x)=3.71x(1-x)$$

である.

定理 7
任意の

$$q^2\in\left\{\frac{1}{2^n},\frac{2}{2^n},\cdots,\frac{2^n-1}{2^n},1\right\}$$

に対して

$$\Lambda_{CA}^k\left(q^2\right)\geq\frac{1}{2}$$

となる k が存在し,

$$k\leq\left[\frac{5}{4}(n-1)\right]$$

である [8, 9].

定理 8
次の包含関係が存在する [7, 9].

$$NP\subseteq BGQPP$$

参考文献

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

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

[5] L. Accardi and M.Ohya, A Stochastic limit approach to the SAT problem, Open systems and Information Dynamics, 11-3, 219-233, 2004

[6] E.Bernstein and U.Vazirani, *Quantum Complexity Theory*, In Proc. 25th ACM Symp. on Theory of Computation, 11–20, 1993.

[7] S.Iriyama, M.Ohya and I.V.Volovich (2006) Generalized Quantum Turing Machine and its Application to the SAT Chaos Algorithm, QP-PQ:Quantum Prob. White Noise Anal., Quantum Information and Computing, 19, World Sci. Publishing, 204-225

[8] S.Iriyama and M.Ohya, Rigorous Estimate for OMV SAT Algorithm, Open System and Information Dynamics, 15, 2, 173-187

[9] S.Iriyama and M.Ohya(2008), Language Classes Defined by Generalised Quantum Turing Machine, to appear in OSID 15:4.

[10] S.Iriyama and M.Ohya, The problem to construct Unitary Quantum Turing Machine for compute partial recursive function, to be submitted.