数理解析研究所講究録
第1561巻 2007年 54-60

一般化量子チューリング機械とその言語クラスについて

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

本研究は，アルゴリズムの数学的モデルであるチューリング機械を，非可換代数系で定式化し，ブール代数で表現される言語のクラス分類を目的とする．定式化はチューリング機械の様相を量子系の状態，遷移函数を量子チャネルとして記述し，遷移函数が，状態に依存して定まる内部函数を仲介して定義される．本講演では，まず一般化量子チューリング機械の定式化と，いくつかのタイプの分類，そしてそれらを元に定義される各言語クラスを説明する．

1 はじめに

P問題がNP問題であるかという問いは，計算の複雑さの研究分野において未解決の問題である．NP完全問題の一つであるSAT問題について，様々な古典計算機におけるアルゴリズムが開発されているが，未だ多項式時間で確率1で解くアルゴリズムは見つかっていない．OhyaとVolovichは，量子計算とカオス力学を組み合わせたアルゴリズムで，量子計算機をもちいれば，多項式時間で確率1/2以上で解けることを示した[2, 3]．また，OhyaとAccardiはStochastic Limitというものを用いて，SATアルゴリズムをユニタリー作用素で記述した[5, 6].

本稿では，量子計算機の数学的モデルである一般化量子チューリング機械(GQTM)の定義と，それを用いて定義される各言語クラスを説明する．まず，数学的モデルであるチューリング機械を説明し，決定性チューリング機械，非決定性チューリング機械，確率的チューリング機械を説明する．次に，GQTMを，Hilbert空間上の状態と完全正チャネルを用いて定義する．そして，その完全正チャネルの性質により，GQTMがいくつかのタイプに分けられるということを説明する．また，それらを用いて言語クラスの分類を行い，SAT問題がどのような言語クラスに属するかを説明する．

2 一般化量子チューリング機械

この節では，本稿で用いられるいくつかの記号について説明し，古典チューリング機械 (CTM)，決定性チューリング機械，非決定性チューリング機械についておおまかに説明する．

2.1 古典チューリング機械

CTM M_{cl} は，次の三つ組 (Q, Σ, δ) で表される．ここで，Σ は（有限な）アルファベットの集合で，ブランク記号 $\#$ を含む．Q はプロセッサ状態の集合で，初期状態 q_0 と，終状態の集合 $\{q_F\}$ を持つ．古典チューリング機械は，プロセッサ，テープと呼ばれるアルファベット列 $\Sigma^* = \Sigma \times \cdots \times \Sigma$，テープを読むテープヘッドの三つの装置を持っている．テープヘッドがテープのアルファベットを読み，プロセッサの状態を参照し，必用ならテープのアルファベットを書き換えながら計算が進行する．また，現在の装置全体の状態を様相とよび，$(q, A, i) \in Q \times \Sigma^* \times \mathbb{Z}$ であらわす．また，ある位置 j のテープに記述されているアルファベットを $A(j)$ であらわす．

写像 $\delta : Q \times \Sigma \to 2^{Q \times \Sigma \times \{0, \pm 1\}}$ を，遷移関数と呼ぶ．$\{0, \pm 1\}$ は，テープヘッドの移動する方向を意味し，-1 なら左，1 なら右，0 は動かないことを表す．決定性チューリング機械は，遷移関数 δ が，$\delta : Q \times \Sigma \to Q \times \Sigma \times \{0, \pm 1\}$ であるものをいい，枝分かれのない写像である．いい替えると，任意の $(q, a) \in Q \times \Sigma$ に対して，δ の値が一意に決まっているものをいう．また，決定性チューリング機械でないものを非決定性チューリング機械という．

非決定性チューリング機械を，遷移を確率的にどれかの枝を取るものとした計算モデルを確率的チューリング機械という．つまり遷移を行う時に，サイコロを振るなどして，出た目に対応する枝を採用する計算モデルである．

2.2 一般化量子チューリング機械

量子チューリング機械に関する議論は Deutsch [8] によりはじめられ，それ以降，関連したさまざまな研究が行われている．Bernstein と Vazirani は，いくつかの CTM における定理を QTM に拡張し，また，万能チューリング機械が構成可能であることを示した [9]．

我々は，GQTM をこれらの議論を含む形で定義する，すなわち，完全正写像で遷移関数を記述することで，今までの議論はそのチャネルがユニタリーチャネルであるときに成立する．

GQTM M_{gq} はつぎの 4 つ組 $(Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ で与えられ，ここで，Λ_δ は様相を様相へ移す完全正チャネルで，量子遷移チャネルと呼ぶ．Q と Σ は CTM と同様である．$\mathcal{H}$ はある Hilbert 空間で，$\mathcal{H} = \mathcal{H}_Q \times \mathcal{H}_\Sigma \times \mathcal{H}_Z$ とかかれ，ここで

$\mathcal{H}_Q$, $\mathcal{H}_\Sigma$, $\mathcal{H}_Z$ は，それぞれ次の標準的な基底 $\{|q\rangle ; q \in Q\}$, $\{|A\rangle ; A \in \Sigma^*\}$, $\{|i\rangle ; i \in \mathbb{Z}\}$ により張られる Hilbert 空間である．様相 ρ は $\mathcal{H}$ 上の密度作用素で表され，$\mathfrak{S}(\mathcal{H})$ を $\mathcal{H}$ 上の全ての密度作用素の集合とする．

ここで，次の遷移関数を定義する．

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

量子遷移チャネル

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

は，次の条件を満たすものとして定義される．

定義 1 次の条件を満たす Λ_δ を量子遷移チャネルと呼ぶ．任意の様相 $\rho = \sum_k \lambda_k |\psi_k\rangle \langle\psi_k|$, $|\psi_k\rangle = \sum_l \alpha_{k,l} |q_{k,l}, A_{k,l}, i_{k,l}\rangle$, $\sum_k \lambda_k = 1$, $\forall \lambda_k \geq 0$, $\sum_l |\alpha_{k,l}|^2 = 1$, $\forall \alpha_{k,l} \in \mathbb{C}$ に対して，量子遷移関数 δ が存在して，

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

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

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

を満たす．ここで，右辺は状態となる．

定義 2 次の条件を満たす $M_{gq} = (Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ を *LQTM(Linear Quantum Turing Machine)* とよぶ．全ての ρ_k に対して

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

が存在し Λ_δ が

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

とかける．ここで *RHS* は状態となる．ここで，全ての状態 $\sum_k \lambda_k \rho_k$ に対して，Λ_δ は次の *Affine* 性を満たす；

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

定義 3 次の条件を満たす *GQTM* M_{gq} を *Unitary QTM(UQTM)* とよぶ. Λ_δ がユニタリーチャネル: $\Lambda_\delta = Ad_{U_\delta}$. U_δ であり，状態ベクトル $|\psi\rangle = |q, A, i\rangle$ に対して，

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

を満たす．ここで

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

は任意の $q \in Q, a \in \Sigma$, $q' (\neq q) \in Q, a' (\neq a) \in \Sigma$ に対して

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

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

を満たす.

次のテーブルに上の GQTM の各タイプで用いられている δ を纏めた.

Classes of GQTM	Transition function
GQTM	$\mathbb{R} \times Q \times \Sigma \times Q \times \Sigma \times Q \times \Sigma \times \{0, \pm 1\} \times Q \times \Sigma \times \{0, \pm 1\} \to \mathbb{C}$
LQTM	$Q \times \Sigma \times Q \times \Sigma \times Q \times \Sigma \times \{0, \pm 1\} \times Q \times \Sigma \times \{0, \pm 1\} \to \mathbb{C}$
UQTM	$Q \times \Sigma \times Q \times \Sigma \times \{0, \pm 1\} \to \mathbb{C}$.

記事 4 任意の $q, p \in Q, a, b \in \Sigma, d \in \{0, \pm 1\}$ に対して，$\delta(q, a, p, b, d) = 0$ または 1 とすると *UQTM* は可逆 *CTM* となる.

OMV-SAT アルゴリズム [2, 3] で用いられているカオス増幅過程は，非線形チャネルで記述できる [?].

2.3 · GQTM における計算過程

この節では，GQTM における計算過程を説明する．$M = (Q, \Sigma, \mathcal{H}, \Lambda_\delta)$ を GQTM とし，$\rho_0 = |\psi_0\rangle\langle\psi_0|$，ここで $|\psi_0\rangle = |q_0, A, 0\rangle$ とする．この ρ_0 を初期状態とよび，A を M の入力とよぶ．GQTM の計算過程は Λ_δ を ρ_0 に作用させ，プロセッサ状態が終状態 $q_f \in \{q_F\}$ になるまで続けられ，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 は終状態と呼ばれ

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

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

を満たす．ここで各 σ_l は $q_f \in \{q_F\}$ を含む．$\sum_l \mu_l$ を停止確率という．

2.4 GQTMにおける言語クラス

この節では，GQTMにより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の集合とする．$x \in L$ では停止し，$x \notin L$ では停止ないようなTMM が存在するとき，L を言語といい，またそのとき M を L を認識するTM と呼ぶ．

CTM が認識する言語に，次の代表的なクラスがある．

定義 5 入力サイズの多項式時間で認識する決定性 *TM* が存在するとき，その言語はクラス P に属すると言う．

定義 6 入力サイズの多項式時間で認識する非決定性 *TM* が存在するとき，その言語はクラス P に属すると言う．さらに，言語 $L_1 \in NP$ が，$L_2 \in NP$ に多項式時間帰着するとき，L_1 を *NP* 完全という．

定義 7 入力サイズの多項式時間で確率 p で認識する確率的 *TM* が存在するとき，その言語はクラス *BPP(Bounded Probalility Polynomial)* に属すると言う．

NP 完全問題は，その定義から，属する言語の一つに対して多項式時間で解けるアルゴリズムが存在すれば，P=NP がいえる．SAT 問題に関しての量子回路とカオス増幅器を組み合わせて多項式時間で解くアルゴリズムは [2, 3] で示されている．

ここで，GQTM における認識を定義する．

定義 8 *GQTM* M_{gq} と言語 L に対して，あるステップ N が存在して，そのとき，状態が終状態を確率 p で含むとき，*GQTM*M_{gq} は L を確率 p で認識し，計算時間は N であるという．

次に GQTM で定義される以下の言語クラスを定義する．

定義 9 言語 L に対して，多項式時間で確率 p で認識する *GQTM* が存在するとき，L は *BGQPP(Bounded Generalized Quantum Probability Polynomial)* に属するという．

同様に,

定義 10 言語 L に対して，多項式時間で確率 p で認識する $LQTM$ が存在するとき，L は *BLQPP(Bounded Linear Quantum Probability Polynomial)* に属するという.

定義 11 言語 L に対して，多項式時間で確率 p で認識する $UQTM$ が存在するとき，L は *BLQPP(Bounded Unitary Quantum Probability Polynomial)* に属するという.

LQTM は CTM を含むため，次の包含関係がいえる [11].

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

さらに，OMV-SAT アルゴリズムを実装する GQTM が存在することから，次がいえる [11].

$$NP \subseteq BGQPP$$

参考文献

[1] J.Gu, P.W.Purdom, J.Franco, and B.W.Wah, "Algorithms for the Satisfiability (SAT) Problem: a Survey," Preliminary version, 1996. http://citeseer.nj.nec.com/56722.html

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

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

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

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

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

[7] L.Accardi and M.Ohya (2004) A Stochastic Limit Approach to the SAT Problem,Open Systems and Information dynamics, 11,1-16.

[8] D.Deutsch, Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, Proc. Roy. Soc, A, **400** 97-117, 1985.

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

[10] M.Ohya and I.V.Volovich, Mathematical Foundation of *Quantum Information and Quantum Computation,* to be published.

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