数理解析研究所講究録
1039巻 1998年 64-80

量子コンピュータの計算量

名古屋大学　小澤正直　(Masanao Ozawa)*
名古屋大学　西村治道　(Harumichi Nishimura)†

アブストラクト

量子計算の研究は，1980年頃，Feynmanによって，量子力学系を古典力学的計算機で模倣することの計算量的複雑性から，量子力学の原理を利用した，より効率の高い計算の可能性が示唆されたことから始まった．1980年代後半にDeutschは量子Turing機械と量子回路の2種類の計算モデルを定式化し，現在，量子アルゴリズムは，これら2種類のモデルを通して表現される．本論文では，量子Turing機械と量子回路の厳密な数学的定式化を与え，量子回路族に対する一様性の概念を導入することで，この2種類の計算モデルの計算能力が多項式計算量の観点から同等であることを示す．

1. はじめに

Turing機械を始めとする従来の計算モデルは古典力学に基づいたものである．ところが計算素子のミクロ化をどんどん押し進めていけば，電子や原子などの微視的物理系の量子力学的振舞いの影響が現れてくる．Feynman [10] は古典力学的計算機を用いて量子力学的現象を模倣すると非常に多くの計算時間が必要となることを指摘し，量子力学的原理に基づく計算機は古典力学的計算機よりも効率的に計算が行なえるのではないかという示唆を与えた．

この量子計算機のモデルとしてDeustchはTuring型（量子Turing機械）[6] と回路型（量子回路）[7] の計算モデルを考案した．それは次の量子力学的原理を満たすものであった: (1) その時間発展はユニタリ作用素によって特徴付けられる．(2) 計算機内では1度に複数の計算（量子並列計算）が実行され得る．(3) 測定によって得られる結果は複数の計算結果のうち1つだけであり，どの計算結果を観測するかは各計算結果の量子振幅によって特徴付けられる．このDeustchの考案したモデルにもとづき，量子計算機の計算効率に関して，幾つかの成果が得られた [1,3,4,8,11,17]．とりわけ，量子計算機の利用によって高確率で効率的に整数の因数分解問題及び離散対数問題が解けるというShor [15,16] の結果は大きな影響を与えた．これらの問題を効率的に解くことのできる古典的計算機上のアルゴリズムはまだ発見されていないし，また，従来の計算量の観点からは存在しないであろうといういうのが，大方の見方であった．また，こうした計算量的困難が公開鍵暗号の理論の基になっている点からも，このことは非常に意義のあるものであった．これにより量子計算機は一躍脚光を浴びることになり，その実現へ向けて多くの研究がなされることとなった．

量子Turing機械と量子回路は二つの基本モデルであるが，量子計算の研究において異なった役割を担っている．量子Turing機械は量子計算の能力を研究するうえでの純数学的モデルとしての側面が強く，一方，量子回路はその実現へ向けて研究されている物理的モデルとしての側面が強い．そのため，2つのモデルの計算能力の関係を調べることは重要な問題である．本論文では数学的に厳密な方法により，量子Turing機械と量子回路の計算能力の関係を研究する．とりわけ，従来，あいまいな取り扱いがされてきた，量子Turing機械の停止問題と量子回路族の一様性の概念に関する厳密な定式化を与え，量子Turing機械と一様量子回路族の計算能力の同等性を証明することを目的とする．

*情報文化学部・大学院人間情報学研究科
†大学院人間情報学研究科

2. 古典 Turing 機械

古典 Turing 機械[1] (CTM) は両側無限のテープとそのテープ上の記号を読み書きする決定性かつ離散時間の力学系である. その状況 (configuration) は機械の内部状況 q, テープ上の記号列 T, そしてテープ上のヘッドの位置 x によって決定される. 任意の整数 n に対して, テープ上の位置 n にあるマス目の記号は $T(n)$ によって表される. C が CTM の状況を表すとき, 状況 C の内部状況, テープ記号列, ヘッドの位置はそれぞれ q_C, T_C, x_C によって表すものとする. テープ記号列の変化を述べるため T_C^τ は位置 x_C における記号をτ に置き換えることで T_C から得られるテープ記号列を表すものとする. CTM の時間発展は遷移関数 $\delta(p,\sigma)=(q,\tau,d)$ によって決定され, これは内部状況が p, ヘッドが指しているマス目の記号が σ のとき, ヘッドがそのマス目を τ に書き換え, 内部状況は q に変わり, そしてヘッドが方向 d に移動する, という 1 ステップの状況の変化を表す. 但し, $d\in\{0,\pm1\}$ で $d=1$ (-1) は右 (左) 方向に 1 マスの移動, $d=0$ はヘッドが移動しないことを表す. これにより $\delta(q_C,T_C(x_C))=(q,\tau,d)$ なら状況 $C=(q_C,T_C,x_C)$ は状況 (q,T_C^τ,x_C+d) へ変化する.

以下で CTM の形式的な定義を与えることにする. 本論文において, 任意の整数 n,m $(n<m)$ に対して $[n,m]_{\mathbf{Z}}$ は $\{n,n+1,\ldots,m-1,m\}$ を表すものとする. **内部状況集合**とは, q_0 と q_f という特別な元を含む有限集合で q_0 は**初期内部状況**, q_f は**終了内部状況**を表す. **記号集合**は, 空白を表す B という特別な元を含む有限集合である. ある記号集合 Σ に対する**テープ記号列** T とは, 有限個の $i\in\mathbf{Z}$ を除いて $T(i)=B$ なる $\mathbf{Z}$ から Σ への関数である. 特に

$$T(i)=\sigma_i\ \ (i\in[0,k-1]_{\mathbf{Z}}),\ \ B\ \ (\text{otherwise})$$

のとき, テープ記号列 T と長さ k の Σ-列 ($\Sigma\setminus\{B\}$ の有限列) $\sigma_0\cdots\sigma_{k-1}$ は 1 対 1 に対応するので, しばしば $T\sim x$ と書いて T を長さ k のテープ記号列という. Σ からのテープ記号列の集合を $\Sigma^{\#}$ と表すことにする. **Turing フレーム**とは, 内部状況集合 Q と記号集合 Σ の組 (Q,Σ) のことを指す. ある Turing フレーム (Q,Σ) の**状況空間**とは, $\mathcal{C}(Q,\Sigma)=Q\times\Sigma^{\#}\times\mathbf{Z}$ のことであり, その元 $C=(q_C,T_C,x_C)$ を (Q,Σ) の**状況**という. この状況は, 機械の内部状況が q_C で, テープ記号列 T_C がテープ上に書かれていて, ヘッドの位置が x_C であることを表す. (Q,Σ) の任意の状況 $C=(q_C,T_C,x_C)$ に対して T_C^τ は次の関係によって定義されるテープ記号列である.

$$T_C^\tau(n)=T_C(n)\ \ (n\neq x_C),\ \ \tau\ \ (n=x_C)$$

(Q,Σ) に対する**遷移関数**とは $Q\times\Sigma$ から $Q\times\Sigma\times[-1,1]_{\mathbf{Z}}$ への関数である. **古典 Turing 機械**は Turing フレーム (Q,Σ) と (Q,Σ) に対する遷移関数 δ からなる 3 つ組 $M=(Q,\Sigma,\delta)$ である.

$M=(Q,\Sigma,\delta)$ を CTM とする. Q の元は M の**内部状況**, 集合 Σ は M の**アルファベット**, 関数 δ は M の**遷移関数**, そして (Q,Σ) の状況は M の**状況**と呼ばれる. M の**初期状況**とは $q_C=q_0$, $x_C=0$ なる状況 C のことを指す. 任意のテープ記号列 T に対して, **入力テープ記号列** T_{in} を持つ M の**計算**とは, 次の条件を満たす状況の (有限, または無限の) 列 $\{C(n)|n\in I\}$; $I=\{0,1,\ldots,N\}$ または $I=\{0,1,\ldots\}$ のことである.

(1) $C(0)$ は $T_{C(0)}=T_{in}$ なる初期状況である.

(2) $C(n+1)$ は $C(n)$ と δ から次のように決定される: $\delta(q_{C(n)},T_{C(n)}(x_{C(n)}))=(q,\tau,d)$ のとき

$$C(n+1)=(q,T_{C(n)}^\tau,x_{C(n)}+d).$$

特に Σ-列 x に対して $T_{in}\sim x$ のとき, **入力** x を持つ M の計算という. 計算 $\{C(n)|n\in I\}$ は $q_{C(n)}=q_f$ なるある n が存在して $T_{C(m)}=T_{out}$, $m=\min\{n\in I|q_{C(n)}=q_f\}$ のとき, **出力テープ記号列** T_{out} で**停**

[1] これは通常計算量の分野では, 決定性 Turing 機械と呼ばれるものである. この論文では古典と量子の対応を与えるためこのような呼び方をしている.

止するという. やはり特に $T_{out} \sim y$ のとき, M は Σ-列 y を**出力**するという. m を入力テープ記号列 T_{in} に対する M の**計算時間**という. 任意の $n \in \mathbf{N}$ に対し, 長さ n の入力を持つ M の計算時間が高々 $t(n)$ であるとき, M を $t(n)$ **時間限定** CTM といい, 関数 t が多項式のとき, **多項式時間限定** CTM という.

CTM M のアルファベットが $\Sigma_1 \times \cdots \times \Sigma_k$ と書けるとき, M を k **トラック CTM** と呼ぶ. これは物理的には M のテープが k 個のトラックに分割されていることを意味する. このとき Σ_i によって表されるトラックを第 i トラックという. 形式的には, 第 i トラックは $T(j) = (Tr_1(j), \ldots, Tr_k(j))$ となるような関数 Tr_i によって表される. これは**第 i トラック記号列**と呼ぶことにする. $T = (Tr_1, \ldots, Tr_k)$ とも書くことにする. x を長さ n の Σ_1-列 とする. 第 1 トラックに入力 x を持つ M の計算とは, 入力 $(x, B^n, \ldots, B^n)$ を持つ M の計算のことである. 同様にして, 第 i トラックに入力 x を持つ M の計算, M は第 i トラックに x を出力するといった概念が定義できる. $x_1, \ldots, x_j$ をそれぞれ長さが n 以下の Σ-列とし, $x_1 B^{n_1}, \ldots, x_j B^{n_j}$ をそれぞれ, それらのあとに空白記号列が続く長さが n の Σ-列とする. このとき, $T \sim (x_1 B^{n_1}, \ldots, x_j B^{n_j}, B^n, \ldots, B^n)$ を $T \sim (x_1, \ldots, x_j)$ と略すことにする.

3. 量子 Turing 機械

量子 Turing 機械 (QTM) は CTM の量子化である. その状態は, 計算基底と呼ばれる CTM の状況の集合と 1 対 1 対応を持つ完備直交系によって張られる Hilbert 空間内のベクトルによって表現される. つまり計算基底は CTM の任意の状況 C に対して, $|C\rangle = |q_C, T_C, x_C\rangle$ によって表現される. QTM の時間発展は, 1 ステップ後の状況の遷移の振幅を与える量子遷移関数によって決定されるユニタリ作用素 U によって述べられる. 量子遷移関数とは, 複素関数 $\delta(p, \sigma, q, \tau, d) = c$ のことで, 古典的遷移 $\delta(p, \sigma) = (q, \tau, d)$ が振幅 c で生じることを表す. これにより時間発展作用素 U は,

$$U\,|q_C, T_C, x_C\rangle = \sum_{q,\tau,d} \delta(q_C, T_C(x_C), q, \tau, d)\,|q, T_C^{\tau}, x_C + d\rangle$$

によって決定される. QTM の形式的な定義は次のようになる.

(Q, Σ) を Turing フレームとする. (Q, Σ) の**状態空間**とは, 状況空間 $\mathcal{C}(Q, \Sigma)$ によって生成される Hilbert 空間 $\mathcal{H}(Q, \Sigma)$ である. $\mathcal{C}(Q, \Sigma)$ と 1 対 1 対応を持つ基底 $\{|q_C, T_C, x_C\rangle \,|(q_C, T_C, x_C) \in \mathcal{C}(Q, \Sigma)\}$ は $\mathcal{H}(Q, \Sigma)$ の**計算基底**と呼ばれる. それゆえ空間 $\mathcal{H}(Q, \Sigma)$ は $\sum_{C \in \mathcal{C}(Q,\Sigma)} |f(C)|^2 < \infty$ であるような $\mathcal{C}(Q, \Sigma)$ 上の複素関数の空間によって表現される; この表現において, 全ての $f, g \in \mathcal{H}(Q, \Sigma)$ に対し, 内積は $\langle f|g\rangle = \sum_{C \in \mathcal{C}(Q,\Sigma)} f(C)^* g(C)$ によって定義され, その計算基底状態 $|q_C, T_C, x_C\rangle$ は $\delta_C(C') = 1$ if $C' = C$, $\delta_C(C') = 0$ otherwise, となるような関数δ_C と同一視される. (Q, Σ) に対する C **値遷移関数**とは, $Q \times \Sigma \times Q \times \Sigma \times [-1, 1]_{\mathbf{Z}}$ から複素数体 $\mathbf{C}$ への関数である. プレ量子 Turing 機械 (プレ QTM) は, Turing フレーム (Q, Σ) と (Q, Σ) に対する $\mathbf{C}$ 値遷移関数からなる 3 つ組 $M = (Q, \Sigma, \delta)$ として定義される.

$M = (Q, \Sigma, \delta)$ をあるプレ QTM とする. Q の元は M の**内部状況**, 集合 Σ は M の**アルファベット**, 関数 δ は M の**量子遷移関数**, (Q, Σ) の状況は M の**状況**, そして $\mathcal{H}(Q, \Sigma)$ の元は M の**状態**と呼ばれる. M の**時間発展作用素**とは,

$$M_\delta = \sum_{q \in Q, \tau \in \Sigma, d \in [-1,1]_{\mathbf{Z}}, C \in \mathcal{C}(Q,\Sigma)} \delta(q_C, T_C(x_C), q, \tau, d)\,|q, T_C^{\tau}, x_C + d\rangle\,\langle q_C, T_C, x_C|$$

によって定義される $\mathcal{H}(Q, \Sigma)$ 上の作用素 M_δ である. 以下では記号 $\sum_{q,\tau,d}$ によって q は Q 上, τ は Σ 上, そして d は $[-1, 1]_{\mathbf{Z}}$ 上を変化するものとする.

プレ QTM はその時間発展作用素がユニタリであるとき, 量子 Turing 機械 (QTM) と呼ばれる. プレ QTM が QTM であるための, その量子遷移関数がみたすべき必要十分条件は, 以下の定理に述べられるようなものであることがわかっている [13].

定理 3.1 プレ量子 Turing 機械が量子 Turing 機械であるための必要十分条件は以下の条件が成り立つことである.

(a) 任意の $(p,\sigma)\in Q\times\Sigma$ に対して

$$\sum_{q,\tau,d}|\delta(p,\sigma,q,\tau,d)|^2=1$$

(b) 任意の異なる $(p,\sigma),(p',\sigma')\in Q\times\Sigma$ に対して

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

(c) 任意の (p,σ,τ), $(p',\sigma',\tau')\in Q\times\Sigma^2$ に対して

$$\sum_{q}\delta(p,\sigma,q,\tau,-1)\delta(p',\sigma',q,\tau',1)^*=0$$

(d) 任意の (p,σ,τ), $(p',\sigma',\tau')\in Q\times\Sigma^2$ に対して

$$\sum_{q,d=0,1}\delta(p,\sigma,q,\tau,d)\delta(p',\sigma',q,\tau',d-1)^*=0$$

4. 停止型量子 Turing 機械と定終型量子 Turing 機械

QTM M のテープ記号列の個数は可算なので, それらは $\{T_1,T_2,\ldots\}$ と番号付されているものとする. $\mathcal{I}(Q,\Sigma)$ 及び $\mathcal{O}(Q,\Sigma)$ を各々, 基底 $\{|q_0,T_i,0\rangle\}$ 及び $\{|q_f,T_i,0\rangle\}$ によって張られる $\mathcal{H}(Q,\Sigma)$ の部分空間とする. $\mathcal{I}(Q,\Sigma)$ 及び $\mathcal{O}(Q,\Sigma)$ の元は各々**初期状態**, **終了状態**といい, $\mathcal{I}(Q,\Sigma)$ に属する計算基底状態は**初期状況**, $\mathcal{O}(Q,\Sigma)$ に属する計算基底状態は**終了状況**という. 任意の初期状態 ψ に対して, M の状態の無限列,

$$\psi,M_\delta\psi,M_\delta^2\psi,\ldots$$

を M の初期状態 ψ に対する**時間発展**という. ユニタリ作用素 M_δ は量子 Turing 機械の**計算ステップ**と呼ばれる一定時間 τ の時間発展を表わす. このとき M の状態 $M_\delta^t\psi$ を**入力状態** ψ に対する t **ステップ**後の M の**状態**という.

我々は QTM の停止及び計算時間について考える. [6, 12] において QTM は次のようなスキームによって測定結果を得るものと定義されている. このスキームは, **停止スキーム**と呼ばれる.

(I) 物理量 $\hat{n}_0=|q_f\rangle\langle q_f|\otimes I\otimes I$ は, **停止フラグ**と呼ばれ, 各ステップ後に測定される.

(II) 一度, QTM の内部状況が q_f になれば, QTM はその後, 内部状況とテープ記号列を書き換えることはしない. すなわち, QTM $M=(Q,\Sigma,\delta)$ の場合, 量子遷移関数 δ が次の条件をみたす: 任意の $T\in\Sigma^{\#}$ に対し,

$$M_\delta|q_f,T,x\rangle=\sum_d\alpha_d|q_f,T,x+d\rangle \quad (4.1)$$

となる.

(III) $\hat{n}_0$ の測定結果が 1 となったとき, その QTM のテープ記号列が測定され, その測定結果がその計算の**出力テープ記号列**と定義される.

量子 Turing 機械を初期状態に準備した後, 以上のスキームに従って出力テープの記号列を得るまでの過程を**計算**と呼び, $\hat{n}_0$ の測定結果が 1 となるまでのステップ数をその計算の**計算時間**という.

停止スキームにおける条件 (4.1) は全ての数学的に定義された QTM がみたすわけではない. そこで条件 (4.1) をみたす QTM を**停止型量子 Turing 機械** (HQTM) という. 停止スキームをみたさない QTM は

停止フラグの測定によって一般にその計算を乱すことになるが，停止型量子 Turing 機械に対しては，任意の計算ステップの後に停止フラグを測定しても，計算結果の確率分布が変化しないことが [12] で証明されている．

次に QTM の計算量理論を展開するとき便利な QTM を述べることにする．P を $\hat{n}_0$ の固有値 1 に対応する射影作用素，S をヘッドの位置 $x \in \mathbf{Z}$ を表す物理量 $\hat{x}$ の固有値 0 に対応する射影作用素 $I \otimes I \otimes |0\rangle\langle 0|$ とする．任意の初期状況 $|C\rangle$ に対して，次の条件をみたすような t が存在するとき，QTM $M = (Q, \Sigma, \delta)$ を**定終型**であるという: 全ての $s < t$ に対して，

$$||PM_\delta^s |C\rangle||^2 = 0, \text{ かつ } ||SPM_\delta^t |C\rangle||^2 = 1.$$

このときこのような t に対して有限列 $|C\rangle, M_\delta |C\rangle, \ldots, M_\delta^t |C\rangle$ を**初期状況** $|C\rangle$ に対する**定終型** QTM M の**計算**，t をその**計算時間**という．また $|C\rangle = |q_0, T_{in}, 0\rangle$，$T_{in} \sim x$ のときは各々**入力** x に対する M の**計算**及びその**計算時間**という．$\{x_i\}$ を長さの等しい任意の Σ-列の集合とし，ϕ を

$$\phi = \sum_i \alpha_i |q_0, T_i, 0\rangle \quad (T_i \sim x_i)$$

をみたす初期状態とする．すべての入力 x_i に対してその計算時間が t のとき，有限列

$$\phi, M_\delta \phi, \ldots, M_\delta^t \phi$$

を**入力状態** ϕ に対する M の**計算**といい，t をその**計算時間**，$M_\delta^t \phi$ をその**出力状態**という．任意の n に対し，長さ n の任意の入力に対する M の計算時間が高々 $f(n)$ のとき M は $f(n)$ **時間限定**定終型 QTM といい，f が多項式のとき，**多項式時間限定**定終型 QTM という．テープ記号列を表す物理量 $\hat{T}$ は，

$$\hat{T} = \sum_{j=1}^{\infty} \lambda_j I \otimes |T_j\rangle\langle T_j| \otimes I$$

と表現される．但し，$\{\lambda_1, \lambda_2, \ldots\}$ は $\{T_1, T_2, \ldots\}$ と多項式時間計算可能関数により 1 対 1 に対応する正数の可算集合である．Q_j を物理量 $\hat{T}$ の固有値 λ_j に対応する射影作用素 $I \otimes |T_j\rangle\langle T_j| \otimes I$ とする．t を入力 x に対する M の計算時間とするとき

$$||Q_j M_\delta^t |q_0, T_{in}, 0\rangle||^2 = p, \quad T_{in} \sim x$$

のとき，M は**確率** p でテープ記号列 T_j を**出力する**といい，$T_j \sim y$ のときは，確率 p で Σ-列 y を出力するという．

注意. トラックの概念は古典同様の方法で QTM にも定義できる．また k トラック QTM $M = (Q, \Sigma_1 \times \Sigma', \delta)$ $(\Sigma' = \Sigma_2 \times \cdots \times \Sigma_k)$ の停止スキームは条件 (4.1) が以下の条件 (4.2) に代わることを除いて同様に定義される:

$$M_\delta |q_f, T, x\rangle = \sum_{\tau \in \Sigma', d} \alpha_{\tau,d} \left| q_f, T^{(T\tau_1(x),\tau)}, x + d \right\rangle \quad (4.2)$$

一般に，定終型 QTM M は HQTM の条件をみたしていないが，その計算時間が t のとき，t ステップ後の M の状態に対して，M のテープ記号列に対応する物理量が測定されたときの確率分布に対応づけ可能な確率分布を t ステップ以降，常に得ることのできる多トラック HQTM M' が存在することは確認できる．さらに HQTM の与えられたステップ後における出力の確率分布を任意の精度で効率的に模倣するような定終型 QTM が存在することも示すことができる [13]．よってあるアルゴリズムを実行する HQTM が作りたいとき，我々は定終型 QTM を作れば十分である．

QTM $M = (Q, \Sigma, \delta)$ の量子遷移関数が任意の $\sigma \in \Sigma$ に対して $\delta(q_f, \sigma, q_0, \sigma, 1) = 1$ となるとき，M を**標準型**という．特に定終型かつ標準型 QTM は第 6 章の補題により，QTM の計算の一部として使用できるのでアルゴリズムを作るには有用である．以後，定終型かつ標準型 QTM を SNQTM (stationary, normal form quantum Turing machine の略) と表す．

5. 可逆性 Turing 機械と二方向量子 Turing 機械

QTM の時間発展作用素はユニタリなので QTM は可逆性を有している. その一方で CTM は一般には非可逆であるが, Bennett [2] は任意の CTM が可逆性を持った CTM によって効率的に模倣できることを示した. そのような CTM は, **可逆性 Turing 機械** (RTM) と呼ばれている. 我々は RTM $M = (Q, \Sigma, \delta)$ を任意の状況 C に対して, $\delta(q_{C'}, T_{C'}(x_C - d)) = (q_C, T_C(x_C - d), d)$ となるような状況 C' と方向 d の組が丁度 1 組存在するような CTM である, と定義することができる. 後に, Deuscth [6] は RTM の時間発展作用素の計算基底に関する行列表現が, 成分として 0 と 1 しか持たない直交行列であることから, 次の意味で RTM が QTM の一種であることを述べた: RTM $M = (Q, \Sigma, \delta)$ と QTM $M' = (Q, \Sigma, \delta')$ は任意の $(p, \sigma, q, \tau, d) \in Q \times \Sigma \times Q \times \Sigma \times [-1, 1]_{\mathbf{Z}}$ に対して $\delta'(p, \sigma, q, \tau, d) = 1$ のとき, そしてそのときのみ $\delta(p, \sigma) = (q, \tau, d)$, という対応のもとで同一視できる. 以後, M' のような QTM も RTM ということにする. Bennett の証明で用いられた RTM は多テープ Turing 機械であったが, [4] では 1 テープ二方向 RTM によって模倣できることが示された. 但し, **二方向**(古典または量子) Turing 機械とは, head の動きを表す d を ± 1 に制限した Turing 機械のことである. 以下では, RTM に関しては二方向 RTM のみを考えることにする. また定終型かつ標準型 RTM を SNRTM と略す.

定理 5.1 (同時化定理) [4] $f : \Sigma^* \to \Sigma^*$ が多項式時間限定 CTM によって計算可能な関数で, 入力 x に対して $|f(x)|$ が $|x|$ のみに依るならば, x に対して $(x, f(x))$ を出力する二方向定終型かつ標準型 RTM が存在して, その計算時間は $|x|$ の多項式時間である. さらに f が全単射で f^{-1} が多項式時間限定 CTM によって計算可能な関数とすると x に対して $f(x)$ を出力する二方向定終型かつ標準型 RTM が存在して, その計算時間は $|x|$ の多項式時間である.

これまで Turing-型 の量子コンピュータのモデルとしては [3], [6] などで, 二方向 QTM が使用されてきた. その理由は, プレ QTM が QTM になるための条件の扱いやすさにある. 具体的には, 二方向プレ量子 Turing 機械 $M = (Q, \Sigma, \delta)$ が二方向 QTM となるための必要十分条件は, 定理 3.1 の条件 (a),(b),(c) が成り立つだけでよくなる [3]. さらに δ が次の条件をみたす二方向 QTM は, 条件 (c) が自然と成立しているものであり, **一方向** QTM と呼ばれる [3]: 任意の $q \in Q$ 及び任意の $(p, \sigma, \tau, d), (p', \sigma', \tau', d') \in Q \times \Sigma^2 \times \{-1, 1\}$ に対し, $\delta(p, \sigma, q, \tau, d)$ 及び $\delta(p', \sigma', q, \tau', d')$ がともに 0 でないなら $d = d'$. 一方向 QTM のヘッドは, 新しい内部状況 q によって決定される方向 d に移動するので, その時間発展は (p, σ) 列 (q, τ) 行の成分が $\delta(p, \sigma, q, \tau, d)$ となるような, 有限次元ユニタリ行列 L_δ によって表現できる. 実は, 任意の QTM は一方向 QTM によって模倣できる [4].

補題 5.2 (完成補題) $Q \times \Sigma \times Q \times \Sigma \times \{-1, 1\}$ 内の部分集合上で, 定理 3.1 の条件 (a),(b),(c) を満たす関数 δ' に対して, δ' の定義域では δ' と同じ値を取る量子遷移関数 δ を持つような二方向 QTM $M = (Q, \Sigma, \delta)$ が存在する.

この補題は二方向 QTM のもう 1 つの利点である. これにより, 我々はある二方向 QTM に実行させたいアルゴリズムを容易に構築することができる. なぜならアルゴリズムの中で使用される全ての内部状況と記号の組に対して, 定理 3.1 の条件 (a),(b),(c) を満たす部分関数を定義すれば十分だからである.

6. QTM のプログラムのための補題

この章では, 8 章の定理を証明するために必要な [4] の補題を記す. これらの証明は [4] を参照されたい.

任意の QTM $M = (Q, \Sigma, \delta)$ と任意のアルファベットΣ' が与えられたとき, 次の 2 トラック QTM $M(\Sigma') = (Q, \Sigma \times \Sigma', \delta')$ は, (M へのアルファベット Σ' を持つ) トラックの**付加**により構成されたという: 任意の $(p, (\sigma, \sigma'), q, (\tau, \tau'), d) \in (Q \times (\Sigma \times \Sigma'))^2 \times [-1, 1]_{\mathbf{Z}}$ に対して

$$\delta'(p, (\sigma, \sigma'), q, (\tau, \tau'), d) = \delta(p, \sigma, q, \tau, d), \quad (\sigma' = \tau'), \quad 0 \quad (\text{otherwise})$$

また k トラック QTM $M=(Q,\Sigma_1\times\cdots\times\Sigma_k,\delta)$ と置換 $\pi:[1,k]_{\mathbf{Z}}\to[1,k]_{\mathbf{Z}}$ が与えられたとき, 次の k トラック QTM $M'=(Q,\Sigma_{\pi(1)}\times\cdots\times\Sigma_{\pi(k)},\delta')$ は（M に対する）トラックの**置換** π によって構成されたという: 任意の $(p,(\sigma_1,\ldots,\sigma_k),q,(\tau_1,\ldots,\tau_k),d)\in(Q\times(\Sigma_{\pi(1)}\times\cdots\times\Sigma_{\pi(k)}))^2\times[-1,1]_{\mathbf{Z}}$ に対して,

$$\delta'(p,(\sigma_1,\ldots,\sigma_k),q,(\tau_1,\ldots,\tau_k),d)=\delta(p,(\sigma_{\pi(1)},\ldots,\sigma_{\pi(k)}),q,(\tau_{\pi(1)},\ldots,\tau_{\pi(k)}),d).$$

多トラック QTM において, あるトラックであるアルゴリズムを実行したいときは, そのアルゴリズムを実行する QTM を構成してから, トラックの付加及び置換を用いればよい. 8章の定理の証明では, トラックの付加及び置換を頻繁に利用しているので, その使用を一つ一つ断わることはしないものとする. 次に QTM のアルゴリズム設計に必要な補題を与えておく.

補題 6.1（接続補題） M_1,M_2 が同じアルファベットを持ち, M_1 が SNQTM なら M_1 の行う計算の実行後, M_2 の計算を実行する QTM M が存在する. このような M を M_1 と M_2 を接続して構成された QTM という.

注意. 各ステップ後のヘッドの位置が入力の長さにのみ依存する（古典または量子）Turing 機械を忘却 (oblivious) Turing 機械という. 一般にたとえ M_2 が定終型でも M が定終型であるとは限らない. M が定終型であるには, 次の条件を満たせば十分である: M_1 の終了状態が $\sum_{i:\alpha_i\neq 0}\alpha_i|q_f,T_i,0\rangle$ ならば, 全ての i に対して長さの等しい x_i が存在して $T_i\sim x_i$ であり, M_2 が定終型忘却 QTM である. この条件を接続条件という.

補題 6.2（分岐補題） M_1,M_2 が同じアルファベットを持つSNQTM なら次のようなSNQTM M が存在する “第2トラックが空白なら, M は第1トラックで M_1 の計算を実行し, マス目 0 に 1 を持つなら M_2 の計算を実行する. いずれも第2トラックは書き換えない”. M の計算時間は実行される QTM M_i ($i=1$ or 2) の計算時間より4ステップ余分にかかる.

補題 6.3（ループ補題） 次のようなSNRTM M と定数 c が存在する. “正整数 k の2進表示を入力としたとき M は $O(k\log^c k)$ 時間で終了状況に入り, そのテープ記号列は初期状況のものと同じである. さらに M はある特定の内部状況 q^* にマス目 0 でちょうど k 回入る”.

注意. この q^* に SNQTM M' を “挿入” する, すなわち, M の内部状況が q^* になるごとに M' の計算を実行することにより, M' によって行われる計算を k 回実行する SNQTM が構成できることになる.

M と M' はSNQTM であり, また同じアルファベットを持つものとする. そのとき M' が M を**逆行する**とは, M の初期内部状況と M' の最終内部状況, M' の初期内部状況と M の最終内部状況を同一視することで次のことが成り立つことをいう: もし $|C\rangle$ と $|\phi\rangle$ がそれぞれ M の初期状況と終了状態なら M' の初期状態 $|\phi\rangle$ に対する終了状態は $|C\rangle$ である.

補題 6.4（逆行補題） $M=(Q,\Sigma,\delta)$ が一方向 SNQTM（二方向標準型 RTM）なら, M の計算を逆行する一方向 SNQTM（二方向標準型 RTM）M' が存在して, M の計算時間を t ステップとすると M' の計算時間は $t+2$ ステップである.

7. 量子回路

以下, 我々は $\{0,1\}$ の元をビット, $\{0,1\}^m$ の元を長さ m のビット列と呼ぶことにする. また長さ m のビット列 $x=x_1\cdots x_m$ に対して, x_i を x の第 i ビットという. m 入力 n 出力の**古典ゲート** G とは, 長さ m のビット列に長さ n のビット列を対応させる関数である. $G(x_1\cdots x_m)=y_1\cdots y_n$ のとき, $y_1\cdots y_n$ を入力 $x_1\cdots x_m$ に対する G の出力という. G が全単射のとき G は可逆性ゲートという. G の入力の長さが n のとき, G を n ビット可逆性ゲートと呼ぶ. 例えば入力 xy に対して $x(x\oplus y)$ を出力する古典ゲート $M_2(N)$ は 2 ビット可逆性ゲートであり, **制御否定ゲート**と呼ばれる. 第1ビットは制御ビット, 第2ビットは標的ビットと呼ばれている [1].

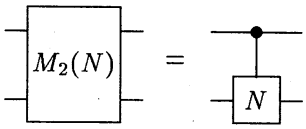

図 1：制御否定ゲート $M_2(N)$

次に量子ゲートの定義を与える．そのため，まず可算無限個の 2 状態系の集まりを考える．この集合に属する各々の 2 状態系を**ワイヤ**と呼ぶ．各ワイヤには，指標 $j = 1, 2, \ldots$ が与えられており，この指標を**ビット番号**と呼ぶ．形式的には，指標 j をもつワイヤは，ビットに一対一対応を与える正規直交系 $\{|0\rangle_j, |1\rangle_j\}$ を基底とする Hilbert 空間 $\mathcal{H}_j \cong \mathbf{C}^2$ で記述される．Hilbert 空間 $\mathcal{H}_j$ の物理量 $\hat{n}_j = |1\rangle_j \langle 1|_j$ を**第 j ビット物理量**と呼ぶ．$\Lambda = \{j_1, \ldots, j_n\}$ $(j_1 < \cdots < j_n)$ を大きさ n の指標の集合とする．指標 $j \in \Lambda$ をもつ n 個のワイヤの合成系は，Hilbert 空間 $\mathcal{H}_\Lambda = \bigotimes_{j\in\Lambda} \mathcal{H}_j$ で記述される．Hilbert 空間 $\mathcal{H}_\Lambda$ において，長さ n のビット列の集合 $\{0,1\}^n$ に一対一対応を与える正規直交基底

$$\{|x_1\rangle_{j_1} \cdots |x_n\rangle_{j_n} \mid x_1 \cdots x_n \in \{0,1\}^n\}$$

を Λ 上の**計算基底**という．以後，$|x_1 \cdots x_n\rangle = |x_1\rangle_{j_1} \cdots |x_n\rangle_{j_n}$ と略記する．このとき

$$1 \otimes \cdots 1 \otimes \hat{n}_{j_k} \otimes 1 \cdots \otimes 1 \, |x_1 \cdots x_k \cdots x_n\rangle = x_k \, |x_1 \cdots x_k \cdots x_n\rangle$$

となる．$\mathcal{H}_\Lambda$ の単位ベクトルは**長さ n の状態**と呼ばれる．

以下では，指標の集合 $\{1, \ldots, n\}$ を $\Lambda^{(n)}$ と表すことにする．n ビット量子ゲートとは，n 個のワイヤが相互作用していて，入力状態から出力状態への状態変化がそれら n 個のワイヤの合成系の時間発展により得られるものである．形式的には，ワイヤの指標の集合 Λ に対して，Hilbert 空間 $\mathcal{H}_\Lambda$ 上のユニタリ作用素を**Λ-量子ゲート**と定義する．特に $\Lambda^{(n)}$-量子ゲートは，n **ビット量子ゲート**と呼ばれる．Λ-量子ゲートの計算基底に関する行列を **S-行列**という．Λ-量子ゲート G に対して，$\mathcal{H}_\Lambda$ の単位ベクトル ψ, ϕ が $G\psi = \phi$ という関係をみたすとき，ϕ を**入力状態** ψ に対する G の**出力状態**という．特に，入力状態が $\psi = |x_1 \cdots x_n\rangle$ のとき，ビット列 $x_1 \cdots x_n$ を G の**入力**と呼ぶ．

n ビット可逆性ゲートは S-行列が，各行各列に 1 つだけ 1 をもち，他は 0 であるような $2^n \times 2^n$ 直交行列であるユニタリ作用素とみなせるので，n ビット量子ゲートの一種である．以下では，このような S-行列を持つ量子ゲートをも可逆性ゲートと呼ぶことにする．

$\Lambda^{(n)}$ 上の置換を P とする．このとき長さ n の状態 $|x_1 \cdots x_n\rangle$ を $|x_{P(1)} \cdots x_{P(n)}\rangle$ に変換する $\mathcal{H}_{\Lambda^{(n)}}$ 上の作用素 V_P を $\Lambda^{(n)}$ 上の**置換作用素**という．また $m \leq n$ のとき，$\Lambda^{(m)}$-量子ゲート G に対して，$\Lambda^{(n)}$-量子ゲート $G \otimes I_{\Lambda^{(n)} \setminus \Lambda^{(m)}}$ [2] を G の（n ビットへの）**拡大**といって $\tilde{G}$ と表す．このとき n ビット量子ゲート G が量子ゲートの**集合 $\mathcal{G}$ によって分解可能である**とは，n_i $(\leq n)$ ビット量子ゲート $G_i \in \mathcal{G}$ $(i = 1, \ldots, k)$ 及び $\Lambda^{(n)}$ 上の置換作用素 V_{P_i} $(i = 1, \ldots, k)$ が存在して，

$$G = U_1 \cdots U_m, \quad (U_i = V_{P_i}^\dagger \tilde{G}_i V_{P_i})$$

と書けることを指し，このとき量子ゲート G は $\mathcal{G}$ **に属する** m 個の量子ゲートに分解可能であるという．このような m の最小数を G の $\mathcal{G}$ **に対するサイズ**という．また $\|G - U_1 \cdots U_m\| \leq \epsilon$ と書けるとき G は $\mathcal{G}$ によって**精度** ϵ 以内で分解可能であるという．

任意の量子ゲートを任意の精度で分解可能であるような量子ゲートの集合を**万能集合**，その元を**基本ゲート**という．$R_{1,\theta}, R_{2,\theta}, R_{3,\theta}$ をその S-行列が

$$R_{1,\theta} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad R_{2,\theta} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix}, \quad R_{3,\theta} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

[2] 有限集合 Λ に対して I_Λ は $\mathcal{H}_\Lambda = \otimes_{\lambda\in\Lambda} \mathcal{H}_\lambda$ 上の恒等作用素である．

となるような1ビット量子ゲートであるとする. このとき無限集合

$$\mathcal{G}_u = \{R_{1,\theta}, R_{2,\theta}, R_{3,\theta}, M_2(N) | \theta \in [0, 2\pi]\}$$

によって, 任意の量子ゲートが分解可能であることが [1] において示されている.

定理 7.1 任意の n ビット量子ゲート G は, 高々$O(n^3 2^{2n})$ 個の $\mathcal{G}_u$ 内の量子ゲートによって分解可能である.

よって無限集合 $\mathcal{G}_u$ は万能集合である. 以下では, $\mathcal{G}_u$ に対するサイズを特に **u-サイズ**という.

次に我々は有限の万能集合を考える. そのためにまず "効率的に計算可能な数" の概念を与える. 実数 x が多項式時間計算可能であるとは, 任意の $n \in \mathbf{N}$ に対して $|\phi(1^n) - x| \leq 2^{-n}$ かつ $\phi(1^n) \in \{m/2^n; m \in \mathbf{Z}\}$ なる多項式時間限定 CTM T によって計算可能な関数 ϕ が存在することを意味する. 多項式時間計算可能な実数の集合を $P\mathbf{R}$ と表す. また実部及び虚部が多項式時間計算可能な複素数を多項式時間計算可能な複素数といってその集合を $P\mathbf{C}$ と表す. 以下, 本論文では $\mathcal{R} = 2\pi \sum_{i=1}^{\infty} 2^{-2^i}$ と表すことにする. このとき次の補題が成り立つ.

補題 7.2 [4] 実数$\theta \in [0, 2\pi]$, $\epsilon > 0$ に対して $|k\mathcal{R} - \theta| \ (mod\ 2\pi) \leq \epsilon$ となる最小の非負整数 $k \leq O(1/\epsilon^2)$ が存在する. また入力としてθ, $\epsilon \in P\mathbf{R}$ を与えたとき[3] 上のような k を出力する入力の長さの多項式時間限定 CTM が存在する.

補題 7.2 より $\mathcal{G}_{\mathcal{R}} = \{R_{1,\mathcal{R}}, R_{2,\mathcal{R}}, R_{3,\mathcal{R}}, M_2(N) | \mathcal{R} = 2\pi \sum_{i=1}^{\infty} 2^{-2^i}\}$ とすると $\mathcal{G}_u$ の 1 ビット量子ゲートは $\mathcal{G}_{\mathcal{R}}$ の 1 ビット量子ゲートによって任意の精度で分解可能なので有限集合 $\mathcal{G}_{\mathcal{R}}$ は万能集合である. 以下, $\mathcal{G}_{\mathcal{R}}$ に対するサイズのことを単に**サイズ**ということにする.

任意の古典ゲートは論理積, 論理和, そして否定の合成によって得られるので, 古典の場合これらのゲートをもとに古典回路が考えられている. 形式的には, 古典回路は非循環有向グラフとして定義され, その各頂点が古典ゲート, 各辺が古典ゲートを接続するワイヤに対応する [14].

一方, n ビット量子回路とは, 複数の量子ゲートが各々 n 個のワイヤのうち, 決められた幾つかのワイヤにつながれている様を表すものである. 形式的には次のように定義される. $\mathcal{G}$ を量子ゲートの集合とする. $\mathcal{G}$ **を基底とする** n ビット**量子回路** K とは, 次の条件を満たす 2 つ組 (G_i, P_i) の有限列 $(G_1, P_1), \ldots, (G_m, P_m)$ である.

(1) G_i は $\mathcal{G}$ に属する n_i $(\leq n)$ ビット量子ゲートである.

(2) P_i は $\Lambda^{(n)}$ 上の置換作用素である.

このとき G_i の j **番ピン**には, ビット番号 $P_i(j)$ のワイヤが**接続されている**という. また K は $G_1, \ldots, G_m$ **の連結によって構成されている**という. m を K の $\mathcal{G}$ **に対するサイズ**という. 特に $\mathcal{G}_u$ に対するサイズのことを u-サイズ, $\mathcal{G}_{\mathcal{R}}$ に対するサイズを単にサイズということにする. ユニタリ作用素 $U_1 \cdots U_m$, $(U_i = V_{P_i}^{\dagger} \tilde{G}_i V_{P_i},\ G_i \in \mathcal{G})$ を K **で定まる** n ビット量子ゲートといって, 以下これを記号 G_K で表すことにする. 定義より G_K の $\mathcal{G}$ に対するサイズは K の $\mathcal{G}$ に対するサイズ以下である. また $K_1 = (G_1^{(1)}, P_1^{(1)}), \ldots, (G_m^{(1)}, P_m^{(1)})$ 及び $K_2 = (G_1^{(2)}, P_1^{(2)}), \ldots, (G_l^{(2)}, P_l^{(2)})$ を $\mathcal{G}$ を基底とする n ビット量子回路とするとき, $K_1 + K_2 = (G_1^{(1)}, P_1^{(1)}), \ldots, (G_m^{(1)}, P_m^{(1)}), (G_1^{(2)}, P_1^{(2)}), \ldots, (G_l^{(2)}, P_l^{(2)})$ は K_1 と K_2 の連結によって構成された量子回路といい, $nK_1 = \underbrace{K_1 + \cdots + K_1}_{n}$ は n 個の K_1 の連結によって構成された量子回路という.

次に, k 入力 m 出力の量子回路の物理的定義を与える. k 入力 m 出力の n ビット量子回路とは, 量子ゲートの集合を基底とする n ビット量子回路（で定まる n ビット量子ゲート）に長さ k のビット列及び長さ $n-k$ の一定のビット列を入力して, このゲートによるユニタリ変換を受けた後, ある決められた m 個のワイヤのビット物理量を測定して, 長さ m のビット列を出力として得るもののことである.

[3] 入力として多項式時間計算可能な実数 θ を与えるということは, θ の有理数による近似値を計算する CTM T_θ のコードと必要な精度ϵ_0 の組を与えることを意味する.

形式的には，**k 入力 m 出力の n ビット量子回路 $\mathbf{K}$** とは，次の条件をみたす4つ組 $(K, \Lambda_1, \Lambda_2, S)$ である．

(1) K は n ビット量子回路である．

(2) Λ_1, Λ_2 は $\Lambda^{(n)}$ の部分集合で $|\Lambda_1| = k$, $|\Lambda_2| = m$ である．

(3) S は $\Lambda^{(n)} \setminus \Lambda_1$ を添字集合とするビットの族である．つまり，$S = \{b_j | \, j \in \Lambda^{(n)} \setminus \Lambda_1\}$ $(b_j \in \{0,1\})$.

$\mathbf{K} = (K, \Lambda_1, \Lambda_2, S)$ を k 入力 m 出力の n ビット量子回路とし，$\Lambda_1 = \{j_1, \ldots, j_k\}$，$\Lambda_2 = \{i_1, \ldots, i_m\}$ とする．k ビット列 $x_1 \cdots x_k$ に対して，$u_{j_1} = x_1, \ldots, u_{j_k} = x_k$，かつ $j \in \Lambda^{(n)} \setminus \Lambda_1$ に対して，$u_j = b_j \in S$ となるように，n ビット列 $u_1 \cdots u_n$ を定める．入力 $u_1 \cdots u_n$ に対する G_K の出力状態を ϕ とし，状態 ϕ でビット物理量 $\hat{n}_{i_1}, \ldots, \hat{n}_{i_m}$ を同時測定して，測定値 $y_1, \ldots, y_m$ が得られるとき，ビット列 $y_1 \cdots y_m$ は**入力** $x_1 \cdots x_k$ に対する $\mathbf{K}$ の**出力**であるという．入力が x であるという条件のもとで，出力として $y = y_1 \cdots y_m$ を得る確率 $\rho^K(y|x)$ は量子力学の統計公式から次のように書ける．

$$\rho^K(y|x) = \left\langle u_1 \cdots u_n \left| {G_K}^\dagger E_{i_1}(y_1) \cdots E_{i_m}(y_m) G_K \right| u_1 \cdots u_n \right\rangle$$

但し，$E_{i_p}(y_p)$ は $\hat{n}_{i_p}$ の固有値 y_p に対応する射影作用素である．$\mathbf{K}$ は各入力 $x = x_{i_1} \cdots x_{i_k} \in \{0,1\}^k$ を $\{0,1\}^m$ 上の確率分布 $\rho^K(x)$ に対応させていると考えられる．このとき $\rho^K(x)$ を $\mathbf{K}$ **によって定まる** x **に対する分布**という．以後，特に混同しないときは $\mathbf{K}$ と K を同一視して扱う．

関数 $e : \Sigma \to \{0,1\}^{l_0}$ $(l_0 = \lceil \log |\Sigma| \rceil)$ を単射，$d : \{0,1\}^{l_0} \to \Sigma$ を $d \cdot e = \mathrm{id}|_{\Sigma \setminus \{B\}}$ かつ $d(x) = B$ $(x \notin \mathrm{range}(e))$ をみたす関数とする．また Σ-列 $x = x_1 \cdots x_k$ 及びビット列 $z = z_1 \cdots z_k$ $(z_i \in \{0,1\}^{l_0})$ に対して $e_k(x_1 \cdots x_k) = e(x_1) \cdots e(x_k)$，$d_k(z_1 \cdots z_k) = d(z_1) \cdots d(z_k)$ とする．このとき（kl_0 入力 $(t + \tilde{t} + 1)l_0$ 出力）量子回路 K が QTM $M = (Q, \Sigma, \delta)$ を（符号化関数 e, 復号化関数 d のもと）**精度** ϵ **で** (k,t)**−模倣する**（$\epsilon = 0$ の場合，単に (k,t)−模倣するという）とは，長さ k の任意の Σ-列 x に対し，M に x を入力して t ステップ後にテープのマス目 $-t$ からマス目 $\tilde{t} = \max(t, k)$ を測定したときの測定値の確率分布と K に $e_k(x)$ を入力したときの出力を z としたときの $d_{t+\tilde{t}+1}(z)$ の確率分布の TVD [4] が ϵ 以内となる，すなわち

$$\sum_{y \in \Sigma^{t+\tilde{t}+1}} \left| \rho_t^M(y|x) - \tilde{\rho}^K(y|x) \right| \leq \epsilon$$

をみたすような kl_0 入力 $(t + \tilde{t} + 1)l_0$ 出力の量子回路 K が存在することである．但し，

$$\begin{aligned} \tilde{\rho}^K(y|x) &= \sum_{z_{-t} \cdots z_{\tilde{t}} \in d_{t+\tilde{t}+1}^{-1}(y)} \rho^K(z_{-t} \cdots z_{\tilde{t}} | e_k(x)) \\ \rho_t^M(y|x) &= \left\langle q_0, T_{in}, 0 \left| {M_\delta^t}^\dagger E_{-t}(y_{-t}) \cdots E_{\tilde{t}}(y_{\tilde{t}}) M_\delta^t \right| q_0, T_{in}, 0 \right\rangle, \quad (T_{in} \sim x) \end{aligned}$$

である．但し，マス目 i の記号を表す物理量の $y_i \in \Sigma \setminus B$ に対応する固有値を λ_i とすれば，$E_i(y_i)$ は λ_i に対応する射影作用素である．

Yao は [17] で任意の QTM M, 入力 x, そして時間 t に対して，M を $(|x|, t)$-模倣する量子回路 $K(M, |x|, t)$ が存在して，その “サイズ”（“サイズ” は Deustch ゲート [7] の個数である）は高々 t の多項式以下であることを示した．我々はこの Yao の証明で使われた量子回路を少し変形することで多テープ QTM にも定理が成立するようにしておく．また後でこの証明を利用するために “サイズ” として u-サイズを用いることにする．

定理 7.3 $M = (Q, \Sigma, \delta)$ をある QTM, $t > k$ とすると，M を (k,t)-模倣するような u-サイズ $O(t^2)$ の量子回路が存在する．

証明 $l = O(2 + \lceil \log(|Q| + 1) \rceil + \lceil \log |\Sigma| \rceil)$ とする．QTM M を (k,t)-模倣するような量子回路 $K_\mathcal{G}$ で定まる量子ゲート $G_{K_\mathcal{G}}$ は $(2t+4)l$ 本のワイヤが接続されている．そのワイヤは l 個ごとに分けて考える

[4] 同じ定義域上の分布 $\mathcal{D}$, $\mathcal{D}'$ の全変動距離 (TVD) とは，$\sum_{i \in I} |\mathcal{D} - \mathcal{D}'|$ のことである．TVD と Euclid 距離の関係として，Euclid 距離が ϵ 以内なら TVD は 4ϵ 以内となることがわかっている [4].

ことにする. ビット番号 $jl+1,\ldots,jl+l$ $(0\leq j\leq 2t)$ のワイヤは M のマス目 $j-t$ を表現していて, このワイヤの集合を $K_{\mathcal{G}}$ のマス目 $j-t$ と呼ぶことにする. $K_{\mathcal{G}}$ のマス目 i $(-t\leq i\leq t)$ の状態は計算基底

$$\{|q_i a_i s_i b_i\rangle\},\quad q_i a_i s_i b_i\in\{0,1\}^l$$

によって張られる Hilbert 空間内の単位ベクトルによって表現される（b_i は一定のビット列であり, 以下では省略する）. q_i は M のヘッドがマス目 i にあるときは M の内部状況, マス目 i にないときは $\emptyset=0^{\lceil\log(|Q|+1)\rceil}$ を表す $\lceil\log(|Q|+1)\rceil$ ビット列, a_i は M のマス目 i の記号を表す $\lceil\log|\Sigma|\rceil$ ビット列, そして s_i は M のヘッドがマス目 i にあるとき 1 または 2, ないときは 0 を表す 2 ビット列 である. ビット番号 $(2t+1)l+1,\ldots,(2t+4)l$ の $3l$ 本のワイヤは M の量子遷移関数に対応する操作を行うため使用して, ビット番号が小さい順に l 個づつのワイヤの集合をマス目 L, N, R または, マス目 $2t+2,2t+3,2t+4$ と呼ぶことにする.

次に $K_{\mathcal{G}}$ を構成する量子ゲート G_1,G_2,G_3 を与えることにする. 以下において $p,q,\ldots$ は Q の元, $\sigma,\tau,\ldots$ は Σ の元を表すものとする. G_1 は次の条件をみたす $4l$ ビット可逆性ゲートである:

$$G_1\,|p\sigma 1;\emptyset B0;\emptyset B0;\emptyset B0\rangle=|\emptyset B2;\emptyset B0;p\sigma 1;\emptyset B0\rangle\,,\quad G_1\,|\emptyset B0;\emptyset B0;\emptyset B0;\emptyset B0\rangle=|\emptyset B0;\emptyset B0;\emptyset B0;\emptyset B0\rangle\,.$$

G_2 は次の条件 (A) をみたす $3l$ ビット量子ゲートである: (A)

$$\begin{aligned}|w_{p,\sigma}\rangle &= |\emptyset B0;p\sigma 1;\emptyset B0\rangle\,,\\ |v_{p,\sigma}\rangle &= \sum_{q,\tau}\delta(p,\sigma,q,\tau,-1)\,|qB2;\emptyset\tau 0;\emptyset B0\rangle+\sum_{q,\tau}\delta(p,\sigma,q,\tau,0)\,|\emptyset B0;q\tau 2;\emptyset B0\rangle\\ &\quad+\sum_{q,\tau}\delta(p,\sigma,q,\tau,1)\,|\emptyset B0;\emptyset B0;q\tau 2\rangle\end{aligned}$$

とするとき $G_2\,|w_{p,\sigma}\rangle=|v_{p,\sigma}\rangle$. 最後に G_3 は次の条件をみたす $6l$ ビット可逆性ゲートである:

(a) $G_3\,|\emptyset\sigma_1 0;\emptyset B2;\emptyset\sigma_2 0;qB2;\emptyset\tau 0;\emptyset B0\rangle=|q\sigma_1 1;\emptyset\tau 0;\emptyset\sigma_2 0;\emptyset B0;\emptyset B0;\emptyset B0\rangle$
(b) $G_3\,|\emptyset\sigma_1 0;\emptyset B2;\emptyset\sigma_2 0;\emptyset B0;q\tau 2;\emptyset B0\rangle=|\emptyset\sigma_1 0;q\tau 1;\emptyset\sigma_2 0;\emptyset B0;\emptyset B0;\emptyset B0\rangle$
(c) $G_3\,|\emptyset\sigma_1 0;\emptyset B2;\emptyset\sigma_2 0;\emptyset B0;\emptyset\tau 0;qB2\rangle=|\emptyset\sigma_1 0;\emptyset\tau 0;q\sigma_2 1;\emptyset B0;\emptyset B0;\emptyset B0\rangle$
(d) $G_3\,|\phi\rangle=|\phi\rangle$

但し, $|\phi\rangle$ は次の 9 種類の計算基底状態からなる任意の状態を表す.

(1) $|\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset B2;qB2;\emptyset\tau 0;\emptyset B0\rangle$,
(2) $|\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset B2;\emptyset B0;q\tau 2;\emptyset B0\rangle$
(3) $|\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset B2;\emptyset B0;\emptyset\tau 0;qB2\rangle$,
(4) $|\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset\sigma_3 0;qB2;\emptyset\tau 0;\emptyset B0\rangle$
(5) $|\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset\sigma_3 0;\emptyset B0;q\tau 2;\emptyset B0\rangle$,
(6) $|\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset\sigma_3 0;\emptyset B0;\emptyset\tau 0;qB2\rangle$
(7) $|q\tau 1;\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset B0;\emptyset B0;\emptyset B0\rangle$,
(8) $|\emptyset\sigma_1 0;q\tau 1;\emptyset\sigma_2 0;\emptyset B0;\emptyset B0;\emptyset B0\rangle$
(9) $|\emptyset\sigma_1 0;\emptyset\sigma_2 0;\emptyset\sigma_3 0;\emptyset B0;\emptyset B0;\emptyset B0\rangle$

今, $K_{\mathcal{G}}$ を $\mathcal{G}=\{G_1,G_2,G_3\}$ を基底として, 以下のように構成される量子回路とする. 以下で, ml ビット量子ゲート G $(m=1,2,\ldots,2t+4)$ がマス目 $i_1,\ldots,i_m$ $(i_1<\cdots<i_m)$ に接続されるとは, G の $(j-1)l+k$ 番ピン $(j=1,\ldots,m,\ k=1,\ldots,l)$ がビット番号 $(i_j+t)l+k$ のワイヤに接続されることを表す: $2t+1$ 個の G_1 を順に接続する. このとき j 番目 $(1\leq j\leq 2t+1)$ の G_1 はマス目 $j-t-1,L,N,R$ に接続する. この $2t+1$ 個の G_1 から構成される $(2t+4)l$ ビット量子回路を K_1 と呼ぶ. 次に G_2 をマス目 L,N,R に接続する. この G_2 から構成される $(2t+4)l$ ビット量子回路を K_2 と呼ぶ. 最後に $2t-1$ 個の G_3 を順に接続する. このとき j 番目 $(1\leq j\leq 2t-1)$ の G_3 はマス目 $j-t-1,j-t,j-t+1,L,N,R$ に接続する. この $2t-1$ 個の G_3 から構成される $(2t+4)l$ ビット量子回路を K_3 と呼ぶ. そして $K_{\mathcal{G}}=t(K_1+K_2+K_3)$ とする. $K_1+K_2+K_3$ は図 2 に表されるような量子回路であり, これが M の 1 ステップに対応する操作を実行することは G_1,G_2,G_3 の定義から確認することができる.

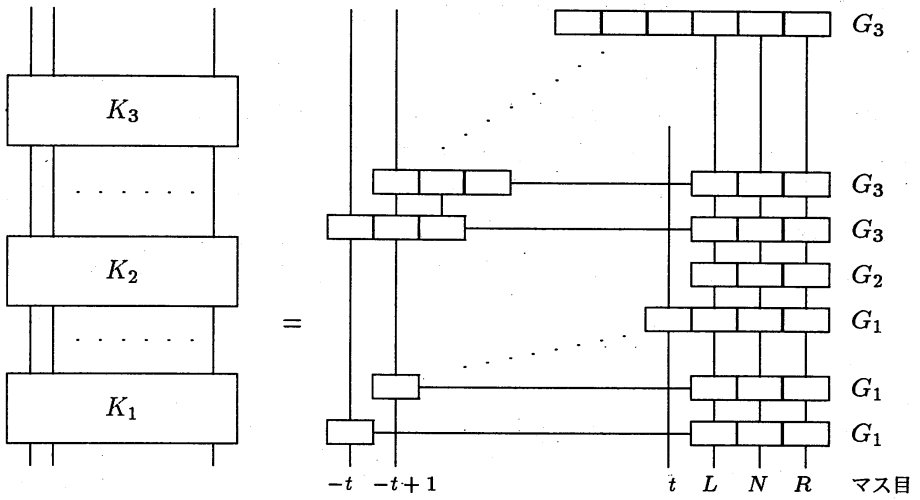

図 2 : $\mathcal{G}$ を基底とする量子回路 $K_1 + K_2 + K_3$

実際, t' ステップ後 $(0 \leq t' < t)$ における M の状態が $|p, T, i\rangle ; T(i) = \sigma$ のとき, $t'+1$ 個目の $K_1+K_2+K_3$ の入力状態は, 計算基底状態

$$|\emptyset T(-t)0; \cdots ; \emptyset T(i-1)0; pT(i)1; \emptyset T(i+1)0; \cdots ; \emptyset T(t)0; \emptyset B0; \emptyset B0; \emptyset B0\rangle$$

であり, G_1 の定義からこの計算基底状態が G_{K_1} によって

$$|\emptyset T(-t)0; \cdots ; \emptyset T(i-1)0; \emptyset B2; \emptyset T(i+1)0; \cdots ; \emptyset T(t)0; \emptyset B0; pT(i)1; \emptyset B0\rangle$$

に決定的に変換される. G_2 の定義からこの状態は G_{K_2} によって,

$$|\emptyset T(-t)0; \cdots ; \emptyset T(i-1)0; \emptyset B2; \emptyset T(i+1)0; \cdots ; \emptyset T(t)0\rangle \otimes |v_{p,\sigma}\rangle$$

に変換される. つまり K_2 はマス目 L, N, R 上で M の "振幅 $\delta(p, \sigma, q, \tau, d)$ でヘッドが指すマス目の記号 σ をτ に書換え, 内部状況を p から q にして, ヘッドを d 方向に移動する" に対応する操作を実行することになる. 最後に G_3 の定義から G_{K_2} 通過後の状態は G_{K_3} によって,

$$\begin{aligned}
&\textstyle\sum_{q,\tau} \delta(p, \sigma, q, \tau, -1) \, |\emptyset T(-t)0; \cdots ; qT(i-1)1; \emptyset\tau 0; \emptyset T(i+1)0; \cdots ; \emptyset T(t)0; \emptyset B0; \emptyset B0; \emptyset B0\rangle \\
&+ \textstyle\sum_{q,\tau} \delta(p, \sigma, q, \tau, 0) \, |\emptyset T(-t)0; \cdots ; \emptyset T(i-1)0; q\tau 1; \emptyset T(i+1)0; \cdots ; \emptyset T(t)0; \emptyset B0; \emptyset B0; \emptyset B0\rangle \\
&+ \textstyle\sum_{q,\tau} \delta(p, \sigma, q, \tau, 1) \, |\emptyset T(-t)0; \cdots ; \emptyset T(i-1)0; \emptyset\tau 0; qT(i+1)1; \cdots ; \emptyset T(t)0; \emptyset B0; \emptyset B0; \emptyset B0\rangle
\end{aligned}$$

に変換される. 以上により $K_1 + K_2 + K_3$ によって, "t' ステップ後にマス目 i にヘッドを持ち, マス目 i の記号 σ, 内部状況 p の M の状況は振幅 $\delta(p, \sigma, q, \tau, d)$ でマス目 $i+d$ にヘッドを持ち, マス目 i の記号 τ, 内部状況 q の状況に変換される" という操作に対応する変換が $K_{\mathcal{G}}$ のマス目 i, $i+d$ 上でなされたことになる.

G_1, G_2, G_3 はいずれも定理 7.1 より $\mathcal{G}_u$ に属する (t に依存しない) 定数個の量子ゲートに分解可能なので u-サイズが定数で, 定まる量子ゲートが各々 G_1, G_2, G_3 である $\mathcal{G}_u$ を基底とする $4l$ ビット量子回路 $K_{u,1}$, $3l$ ビット量子回路 $K_{u,2}$, そして $6l$ ビット量子回路 $K_{u,3}$ が存在する. さらに各々 u-サイズが $O(2t+1)$, $O(1)$, $O(2t-1)$ で, 定まる量子ゲートが $G_{K_1}, G_{K_2}, G_{K_3}$ であるような $(2t+4)l$ ビット量子回路 K_a, K_b, K_c が存在する. $K = t(K_a + K_b + K_c)$ とすると, K は M を (k,t)-模倣する u-サイズ $O(t^2)$ の量子回路である. $Q.E.D$

8. 一様量子回路族と QTM の計算量に関する同等性

量子回路に対する一様性の概念は Shor [16], Ekert と Jozsa [9] などによって触れられてはいるが, 基本ゲートなど一様性の厳密な数学的定義を与えるのに必要な概念が述べられていない. そこで我々は万能集合として $\mathcal{G}_{\mathcal{R}}$ 及び $\mathcal{G}_u$ を考え, それらをもとに一様性の概念を導入する.

量子ゲートの有限集合が $\mathcal{G} = \{G_1, \ldots, G_l\}$ (G_i は n_i ビット量子ゲート) と番号付が行われているものと仮定する. このとき $\mathcal{G}$ を基底とする量子回路 K のコードは量子回路の定義から自然に定義できて, $K = (G_{i_1}, P_1), \ldots, (G_{i_m}, P_m)$ のとき, その**標準コード** $c(K)$ とは, 自然数の有限列 $\langle\langle i_1, P_1(1), \ldots, P_1(n_{i_1})\rangle, \ldots, \langle i_m, P_m(1), \ldots, P_m(n_{i_m})\rangle\rangle$ であると定義する. $\mathcal{G}_{\mathcal{R}}$ の場合 $R_{1,\mathcal{R}}, R_{2,\mathcal{R}}, R_{3,\mathcal{R}}, M_2(N)$ の順に $1, 2, 3, 4$ と番号付することで $\mathcal{G}_{\mathcal{R}}$ を基底とする量子回路 K に対する標準コード $c(K)$ が定義できる.

一方, 任意の量子回路 K で定まる量子ゲート G_K は, 定理 7.1 より $\mathcal{G}_u$ によって分解可能なので, 以下では $\mathcal{G}_u$ (またはその有限部分集合) を基底とする量子回路のみを考えることにする. $\mathcal{G}_u$ を基底とするサイズ s の n ビット量子回路 $K = (G_1, P_1), \ldots, (G_s, P_s)$ の **ϵ-近似**とは, K を構成する各 1 ビット量子ゲート $R_{j,\theta}$ $(j = 1, 2, 3)$ に対して, $||R_{j,\theta} - R^m_{j,\mathcal{R}}|| \leq \epsilon/s$ となるような最小の $m = m_{j,\theta}$ を取り, $R_{j,\theta}$ を m 個の 1 ビット量子ゲート $R_{j,\mathcal{R}}$ の積によって置き換えることで得られる, $\mathcal{G}_{\mathcal{R}}$ を基底とする量子回路のことであり, 以下これを K_ϵ と表すことにする. 但し, 量子回路 $K = (G_1, P_1), \ldots, (G_i, P_i), \ldots, (G_l, P_l)$ 内の 1 ビット量子ゲート G_i を m 個の 1 ビット量子ゲート G'_i の積によって置き換えることで得られる量子回路とは, $(G_1, P_1), \ldots, \underbrace{(G'_i, P_i), \ldots, (G'_i, P_i)}_{m}, \ldots, (G_l, P_l)$ のことである. このとき K の**精度 ϵ での標準コード**を K_ϵ の標準コード $c(K_\epsilon)$ であると定義する. そしてこれを $\bar{K}_\epsilon$ と表すことにする.

$\mathcal{G} = \{G_1, \ldots, G_l\}$ を基底とする **k 入力 m 出力の n ビット量子回路 $\mathbf{K} = (K, \Lambda_1, \Lambda_2, S)$ の標準コード** $c(\mathbf{K})$ は $\Lambda^{(n)} \setminus \Lambda_1 = \{i_1, \ldots, i_{n-k}\}$, $\Lambda_2 = \{j_1, \ldots, j_m\}$, $S = \{b_j |\ j \in \Lambda^{(n)} \setminus \Lambda_1\}$ とすると次のような有限列で定義される.

$$c(\mathbf{K}) = \langle \langle i_1, b_{i_1} \rangle, \ldots, \langle i_{n-k}, b_{i_{n-k}} \rangle, c(K), j_1, \ldots, j_m \rangle$$

量子回路族とは, n 入力 ($f(n)$ 出力の $g(n)$ ビット) 量子回路 $\mathbf{K}_n$ からなる無限列 $\mathcal{K} = \{\mathbf{K}_n\}_{n\geq 1}$ であり, 全ての $\mathbf{K}_n$ が $\mathcal{G}$ を基底としているとき, $\mathcal{K}$ は**$\mathcal{G}$ を基底とする量子回路族**という. さらに $\mathbf{K}_n$ の $\mathcal{G}$ に対するサイズが関数 s によって $s(n)$ で押さえられるとき, $\mathcal{K}$ を **$\mathcal{G}$ を基底とするサイズ関数 s の量子回路族**といい, 特に s が多項式のとき **$\mathcal{G}$ を基底とする多項式サイズ量子回路族**という. また $\mathcal{G} = \mathcal{G}_u$ のとき $\mathcal{K}$ を **u-多項式サイズ量子回路族**, $\mathcal{G} = \mathcal{G}_{\mathcal{R}}$ のときは単に**多項式サイズ量子回路族**という. $\mathcal{K} = \{\mathbf{K}_n\}_{n\geq 1}$ を $\mathcal{G}_u$ を基底とするサイズ関数 s の量子回路族とする. このとき $\mathbf{K}_n = (K_n, \Lambda_1, \Lambda_2, S)$ の**精度 ϵ での標準コード**は n 入力量子回路 $\mathbf{K}_{n,\epsilon} = ((K_n)_\epsilon, \Lambda_1, \Lambda_2, S)$ の標準コード $c(\mathbf{K}_{n,\epsilon})$ と定義して, これを $\bar{\mathbf{K}}_{n,\epsilon}$ と表すことにする. $\mathbf{K}_{n,\epsilon}$ は $\mathbf{K}$ の **ϵ-近似**と呼ぶ. 以下では $(K_n)_\epsilon$ を $K_{n,\epsilon}$ と書くことにする. 関数 $c:\ (1^n, \epsilon) \to \bar{\mathbf{K}}_{n,\epsilon}$ を $\mathrm{poly}(s(n) \log 1/\epsilon)$ 時間で計算可能な CTM が存在するとき $\mathcal{K}$ は**一様である**という.

次に $\mathcal{G}_u$ の有限部分集合を基底とする量子回路に対する一様性の概念を与えることにする. 有限集合 $\mathcal{B} \subseteq \mathcal{G}_u$ は $\{R_1, \cdots, R_k, R_{k+1}\}$, $(R_{k+1} = M_2(N))$ と番号付がされているものとする. $\mathcal{B}$ を基底とするサイズ関数 s の量子回路族 $\mathcal{K} = \{\mathbf{K}_n\}_{n\geq 1}$ に対して, 関数 $c : 1^n \to c(\mathbf{K}_n)$ を $\mathrm{poly}(s(n))$ 時間で計算可能な CTM が存在するとき $\mathcal{K}$ は**入力長一様量子回路族**という.

定義からサイズ関数 s の一様量子回路族 $\mathcal{K}$ とは, 任意の精度ϵ 及び $\mathbf{K}_n \in \mathcal{K}$ に対して $||G_{K_n} - G_{K_{n,\epsilon}}|| \leq \epsilon$ となり, K_n の精度 ϵ での標準コードを $\mathrm{poly}(s(n) \log 1/\epsilon)$ 時間で計算できることを意味している. このときさらに $\{\mathbf{K}_{n,\epsilon}\}_{n\geq 1}$ が入力長一様量子回路族となることがわかる. $\{\mathbf{K}_{n,\epsilon}\}_{n\geq 1}$ は $\mathcal{K}$ の **ϵ-近似**であるといって, $\mathcal{K}_\epsilon$ と表すことにする. 以後, 特に混同しない限り K_n と $\mathbf{K}_n$ は同一視して扱うことにする.

離散フーリエ変換を行う u-多項式サイズ量子回路族 $\mathcal{K} = \{K_n\}_{n\geq 1}$ は図 3 及び図 4 のように構成される (図 3 は K_4 を表している). 但し $A = R_{\pi/4}$ であり, B_k は $\mathcal{G}_u$ を基底とする, 図 4 のような量子回路 K_B で定まり, 次のような作用を施す 2 ビット量子回路である: $x, y \in \{0, 1\}$ に対して, $B_k |xy\rangle = \exp(\frac{2x \cdot y\pi i}{2^k}) |xy\rangle$.

([9], [16] では, 離散フーリエ変換を行う量子回路族は無限集合 $\{A, B_1, B_2, \ldots\}$ を基底として "一様" とされている.)

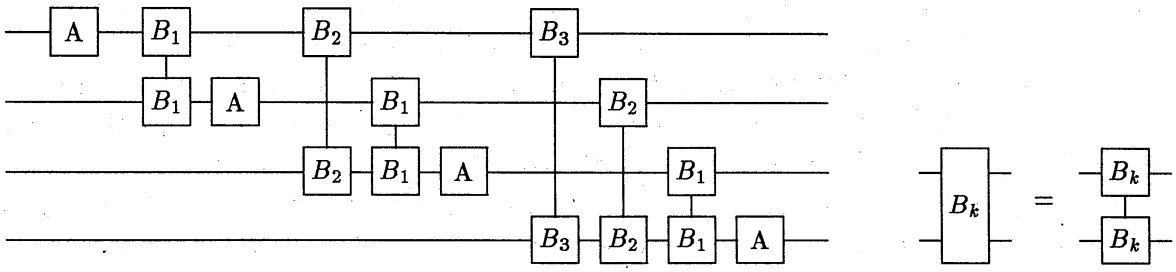

図 3 : 量子回路 K_4

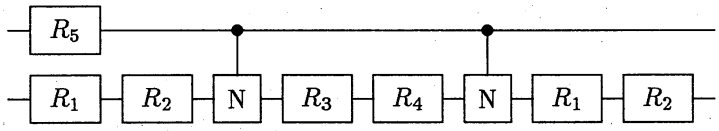

図 4 : 量子回路 K_B

但し, $R_1 = R_{2,-\pi/2^{k+2}}$, $R_2 = R_{3,\pi/2^{k+2}}$, $R_3 = R_{2,-\pi/2^{k+1}}$, $R_4 = R_{3,\pi/2^{k+1}}$, $R_5 = R_{3,\pi/2^k}$

以下は入力 $1^n, \epsilon > 0$ が与えられたとき, K_n の精度 ϵ での標準コードを計算するアルゴリズムである.

(1) $||A - R^m_{1,\mathcal{R}}|| \leq \epsilon/s(n)$ となる最小の m を補題 7.2 に従って求める. 但し, $s(n) \leq n + 9 \times \frac{1}{2}n(n-1)$ は K_n の $\mathcal{G}_u$ に対するサイズを表す.

(2) $k = 1$ から n に対して, $||R_i - R^{m(k,i)}_{a(i),\mathcal{R}}|| \leq \epsilon/s(n)$ となる最小の $m(k,i)$ $(i = 1 \sim 5)$ を求める. 但し, $a(i) = 2$ $(i = 1, 3)$, 3 $(i = 2, 4, 5)$ である.

(3) 図 3 及び図 4 のような入力の長さの多項式時間で計算可能な構成に基づいた K_n に対して, (1),(2) で求めた m 及び $m(k,i)$ をもとに A 及び B_k を各々 m 個の $R_{1,\mathcal{R}}$ 及び $m(k,i)$ 個の $R_{a(i),\mathcal{R}}$ で置き換えて, その結果得られる量子回路 $K_{n,\epsilon}$ の標準コードを計算する.

このアルゴリズムの実行時間は高々 n と $\log 1/\epsilon$ の多項式時間であることは容易に確認できる. ゆえに $\mathcal{K}$ は本論文で定義した意味での一様になっている.

計算量理論において通常, 問題の難しさを考えるときよく使用されるのが有限ビット列の集合 (言語) である. 我々は QTM 及び量子回路によって認識可能な言語のクラスの中で効率的に認識可能と考えられるものを与えることにする. なお従来の計算量理論に関しては例えば [14] を参照せよ. まず QTM であるが, QTM M が**確率** p で $x \in \{0,1\}^*$ を**受理 (拒否) する**とは, 入力 x に対する M の出力が確率 p で $x1$ (x) であることをいう. そして M が確率 p 以上で**言語** L を**認識する**とは, 任意の $x \in \{0,1\}^*$ に対して $x \in L$ のとき p 以上の確率で M は x を受理, $x \notin L$ のとき p 以上の確率で M は x を拒否する, ことをいう.

このとき [4] において定義されている BQP は次のような言語クラスである. 以下では, $0 < \eta \leq 1/2$ は入力によらない定数として扱う. $A \subseteq \mathbf{C}$ のとき, ある**言語** L **が** $BQP[A]$ **に属する**とは, 量子遷移関数の値域 range(δ) が A に含まれ, L を確率 $1/2 + \eta$ 以上で認識する多項式時間限定 QTM $M = (Q, \Sigma, \delta)$ が存在することをいう. 特に $BQP[P\mathbf{C}]$ を単に BQP と表すことにする. 確率 $1/2 + \eta$ はループ補題を用いて M を効率的な回数だけ繰り返して多数決を取ることで, 幾らでも確率 1 に近付けられる [5].

量子回路による言語判定に関する定義は次のように与えられる. n 入力 1 出力の量子回路 K によって定まる分布は, 各入力 $x \in \{0,1\}^n$ に対して 1 を出力する確率 $p_x = \rho^K(1|x)$ によって特徴づけられる. $p_x = p$ のとき, K は**確率** p で x を**受理する** (または確率 $1-p$ で x を拒否する) という. そして任意の $x \in \{0,1\}^n$

に対して $x \in L_n$ のとき, K は p 以上の確率で x を受理, $x \notin L_n$ のとき, K は $1-p$ 以下の確率で x を受理するとき, K は言語 L_n を**確率 p 以上で認識する**という.

異なる長さを持つビット列を含むような言語を認識するためには, 回路族を考える必要がある. 以下では, 任意の言語 L に対して $L_n = L \cap \{0,1\}^n$ と表すことにする. 量子回路族 $\mathcal{K} = \{K_n\}_{n\geq 1}$ が (確率 $1/2+\eta$ 以上で) 言語 L を**認識する**とは, 全ての n に対して K_n が確率 $1/2+\eta$ 以上で言語 L_n を認識することをいう. このとき言語 L が**多項式サイズ量子回路を持つ**とは, L を認識するような多項式サイズ量子回路族 $\mathcal{K} = \{K_n\}_{n\geq 1}$ が存在することをいう. 特に $\mathcal{K}$ が入力長一様であるとき, L は**入力長一様多項式サイズ量子回路を持つ**という. 同様に L が **u-多項式サイズ量子回路を持つ**とは, L を認識するような u-多項式サイズ量子回路族 $\mathcal{K} = \{K_n\}_{n\geq 1}$ が存在することをいう. 特に $\mathcal{K}$ が入力長一様であるき, L は**入力長一様 u-多項式サイズ量子回路を持つ**という. また, L を認識するような, u-多項式サイズ量子回路族 $\mathcal{K} = \{K_n\}_{n\geq 1}$ が一様であるとき, L は **一様 u-多項式サイズ量子回路を持つ**という.

以上の定義のもとで次の補題が成り立つ.

補題 8.1 (1) 言語 L が多項式サイズ量子回路を持つ $\Leftrightarrow$ L が u-多項式サイズ量子回路を持つ

(2) 言語 L が入力長一様多項式サイズ量子回路を持つ$\Leftrightarrow$ L が一様 u-多項式サイズ量子回路を持つ

証明 (1) は (2) と同様に示されるので (2) のみ証明する.

($\Rightarrow$) 仮定より任意の n に対して, L_n を $1/2+\eta$ 以上の確率で認識する $\mathcal{G}_{\mathcal{R}}$ を基底とするサイズ $p(n)$ (p は多項式) の量子回路 K_n が存在して, 関数 $1^n \to c(K_n)$ を計算する多項式時間限定 CTM M_0 が存在する. このとき $\mathcal{K} = \{K_n\}_{n\geq 1}$ は L を認識する $\mathcal{G}_u$ を基底とする量子回路族であり, $K_{n,\epsilon} = K_n$ より, 関数 $(1^n, \epsilon) \to \bar{K}_{n,\epsilon} = c(K_n)$ を計算する多項式時間限定 CTM は M_0 から容易に構成できる.

($\Leftarrow$) 仮定より任意の n に対して, L_n を $1/2+\eta$ 以上の確率で認識する $\mathcal{G}_u$ を基底とする u-サイズ $p(n)$ (p は多項式) の量子回路 K_n が存在して, 関数 $(1^n, \epsilon) \to K_{n,\epsilon}$ を計算する $\mathrm{poly}(n \log 1/\epsilon)$ 時間限定 CTM M_0 が存在する. このとき $K_{n,\epsilon}$ の定義から $x \in L$ のとき $K_{n,\epsilon}$ は $1/2+(\eta-\epsilon)$ 以上の確率で L を受理し, $x \notin L$ のとき $1/2-(\eta-\epsilon)$ 以下の確率で L を受理する. よって $\epsilon < \eta/2$ を満たすある ϵ に対して, $\mathcal{K}_\epsilon = \{K_{n,\epsilon}\}_{n\geq 1}$ は L を認識する $\mathcal{G}_{\mathcal{R}}$ を基底とする量子回路族であり, 関数 $1^n \to c(K_{n,\epsilon})$ を $\mathrm{poly}(n)$ 時間で計算する CTM は M_0 から構成できる. 次に $K_{n,\epsilon}$ のサイズを考える. K_n を構成する各 1 ビット量子ゲート $R_{j,\theta}$ $(j=1,2,3,\ \theta \in [0,2\pi])$ に対して $\|R_{j,\theta} - R^m_{j,\mathcal{R}}\| \leq \epsilon/p(n)$ となるような最小の m は, 補題 7.2 から高々 $O(p^2(n)/\epsilon^2)$ なので, $\epsilon \leq \eta/2$ を満たすある ϵ に対して, $K_{n,\epsilon}$ のサイズは $O(p^2(n)/(\frac{\eta}{2})^2) \times p(n) = O(p^3(n))$. 以上から L は入力長一様多項式サイズ量子回路をもつ. $Q.E.D$

Turing 機械と回路の計算量に関する対応において, 計算量理論では次のことがわかっている. これは CTM と一様古典回路族の計算量に関する同等性を示している [14].

定理 8.2 $L \in P \Leftrightarrow L$ が一様多項式サイズ古典回路を持つ.

これに対応する QTM と量子回路族の関係は次の定理に示される.

定理 8.3 $L \in BQP \Leftrightarrow L$ が一様 u-多項式サイズ量子回路を持つ.

証明 ($\Rightarrow$) $L \in BQP$ なら L を $1/2+\eta$ 以上の確率で認識する $p(n)$ 時間限定 QTM $M = (Q, \{0,1\}, \delta)$ (p は多項式) [5] が存在する. この M は定理 7.3 の証明のように構築した u-サイズ $O(p^2(n))$ の量子回路 K_n によって $(n, p(n))$-模倣できる. 定理 7.3 の構成法より有限列 K_n は n の多項式時間で計算でき, また $\mathrm{range}(\delta) \subseteq \boldsymbol{PC}$ 及び補題 7.2 より入力 $(1^n, \epsilon)$ に対して, K_n の精度 ϵ での標準コード $\bar{K}_{n,\epsilon}$ を出力するような n および $\log 1/\epsilon$ の多項式時間限定 CTM M_0 が存在するので $\mathcal{K} = \{K_n\}_{n\geq 1}$ は一様である. 以上から L は一様 u-多項式サイズ量子回路を持つ.

($\Leftarrow$) 補題 8.1 より L が入力長一様多項式サイズ量子回路を持つ, としてよい. この仮定より L_n を認

[5] 任意の一方向 QTM $M = (Q, \Sigma, \delta)$ はアルファベットが $\{0,1\}$ からなるある一方向 QTM $M' = (Q', \{0,1\}, \delta')$ によって効率的に模倣できることが容易にわかる. 5 章で述べたように任意の QTM は一方向 QTM で効率的に模倣できたので, L を $1/2+\eta$ 以上の確率で認識する QTM として, アルファベットが $\{0,1\}$ からなるものを考えても問題はない. 但しこのとき空白を表す B は 0 であるとみなすことにする.

識する $\mathcal{G}_{\mathcal{R}}$ を基底とする量子回路 K_n が存在して, そのサイズは $p(n)$ (p は多項式) である. また, 関数 $1^n \to c(K_n)$ を計算する多項式時間限定 CTM M_0 が存在する. 今, G_{K_n} を実行するような SNQTM $M=(Q,\Sigma,\delta)$ を構築できたとすると, 長さ n の任意の入力 x に対して, $c(K_n)$ を計算した後, $(x,c(K_n))$ を入力として G_{K_n} を実行するような QTM が接続補題から構成できて, それは $1/2+\eta$ 以上の確率で L を認識する. 但し, QTM M が n ビットユニタリ変換 U を実行するとは, 任意の入力状態 $|q_0,T,0\rangle$, $T\sim(x,c(U))$ $(|x|=n)$ に対して, M の出力状態が

$$\sum_i c_i\,|q_f,T_i,0\rangle\ ,\ T_i\sim(y_i,c(U))\text{such that}\ \ \sum_i c_i\,|y_i\rangle = U\,|x\rangle$$

となることをいう. 但し, $c(U)$ は U のコードである. よって n の多項式時間で G_{K_n} を実行して, range(δ)$\subseteq PC$ を満たす M を構成すれば証明は終了する.

M は 3 トラック QTM でその入力は $(x,c(K_n))$ である. M は以下のように G_{K_n} を実行する.

(1) $l=1$ から $p(n)$ まで (2)~(3) の操作を反復する. 但し, (3) とは (3.1),(3.2) のどちらかである.

(2) 第 2 トラックにおいて, 標準コード $c(K_n)$ の第 l 成分 $\langle k,i\rangle$ (または $\langle k,i,j\rangle$) を走査する. つまり, k は K_n の l 番目の量子ゲートの $\mathcal{G}_{\mathcal{R}}$ における番号で, i (及び j) は接続されるワイヤの番号である.

(3.1) $k=4$ のとき (a) 第 1 トラックにある x の i,j 番目のビット x_i,x_j を第 3 トラックのマス目 0,1 に書き移して, その一方で第 1 トラックの x_i,x_j のあったマス目には特定の記号 s_1,s_2 を書き込む. (b) 第 3 トラックにおいて $M_2(N)$ を実行する. (c) その結果, 得られた値 x_i,y_j を s_1,s_2 の書かれたマス目に書き込む一方で第 3 トラックを空白にする.

(3.2) $k=1,2,3$ のとき (a) x の第 i ビット x_i を第 3 トラックのマス目 0 に書き移して, その一方で x_i のあったマス目には特定の記号 s を書き込む. (b) 第 3 トラックにおいて $R_{k,\mathcal{R}}$ を実行する. (c) その結果得られた y_i を第 1 トラックの s の書かれたマス目に書き込む一方で, 第 3 トラックを空白にする.

(3.1) の場合, (a) の操作は決定的なので, 同時化定理によってこれを行う SNRTM M_a が存在する. また (c) の操作は M_a を逆行すればよいので, 逆行補題よりこれを行う SNRTM M_c が存在する. (b) に関しては次の 2 つの SNQTM $M_{4,m}=(\{q_0,q_1,q_f\},\{0,1,B\},\delta_m$[6]$)$ $(m=0,1)$

$$\delta_m(q_0,0,q_1,0,-1)=\delta_m(q_0,1,q_1,1,-1)=1-m,$$
$$\delta_m(q_0,0,q_1,1,-1)=\delta_m(q_0,1,q_1,0,-1)=m,\qquad \delta_m(q_1,B,q_f,B,1)=1$$

に分岐補題を適用すれば, (b) を行う SNQTM M_b が構成できる. δ_m が定理 3.1 の条件を満たすことは容易に確認できる. M_a, M_b, M_c を接続すれば, (3.1) を実行する SNQTM が構成できることになる. (3.2) の場合も同様に考えることができる. よって (3.1),(3.2) とも SNQTM によって実行でき, また (2) は決定性なので同時化定理によってこれを行う SNRTM は存在する. k の値によって (2) の後, (3.1),(3.2) のいずれかを実行する SNQTM M' は分岐補題及び接続補題によって構成できる. 最後にループ補題を用いて M' を $p(n)$ 回繰り返すような SNQTM を構成すれば, それが M である. M の量子遷移振幅は $\mathcal{R}$ の定義から明らかに PC に属する. G_l を通過したときの操作は (3) において行なわれるので, SNQTM M は G_{K_n} を実行する. M の計算時間は各 l に対して $O(|x|+|c(K_n)|)=O(p(n)\log n)$ なので $n=|x|$ の多項式時間である. $Q.E.D$

一方, $\mathcal{G}_u$ の有限部分集合を基底として与えると次の関係が成り立ち, これは 2 つのモデルに関する計算量の拡張された対応関係を与えている.

系 8.4 [13] $L\in BQP[\mathbf{C}] \Leftrightarrow L$ が入力長一様 u-多項式サイズ量子回路を持つ.

参考文献

[1] A. Barenco, C. H. Bennett, R. Cleve, D. DiVicenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin

[6] ここで δ_m は部分的にしか定義していないが, $M_{4,m}$ が 2 方向 QTM であることより, 完成補題によって全域関数にできる.

and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[2] C. H. Bennett, IBM J. Res. Develop. **17**, 525 (1973).

[3] E. Bernstein and U. Vazirani, in Proceedings of the 25th Annual ACM Symposium on Theory of Computing, 11 (1993).

[4] E. Bernstein and U. Vazirani, preprint (1996).

[5] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, quant-ph/9701001 (1997).

[6] D. Deustch, Proc. Roy. Soc. London Ser. A **400**, 96 (1985).

[7] D. Deustch, Proc. Roy. Soc. London Ser. A **425**, 73 (1989).

[8] D. Deustch and R. Jozsa, Proc. Roy. Soc. London Ser. A **439**, 553 (1992).

[9] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).

[10] R. Feynman, Internat. J. Theoret. Phys. **21**, 467 (1982).

[11] L. Grover, in Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212 (1996).

[12] M. Ozawa, quant-ph/9704028 (1997).

[13] M. Ozawa and H. Nishimura, in preparation.

[14] C. H. Papadimitriou. *Computational Complexity*, Addison-Wesley (1994).

[15] P. W. Shor, Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, 124 (1994).

[16] P. W. Shor, quant-ph/9508027 (1995).

[17] A. Yao, Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, 352 (1993).