Vol. 36 No. 4　　情　報　処　理　　Apr. 1995

解　説

量子コンピュータ†

西野　哲朗††

1. はじめに

一般に，汎用コンピュータは以下の条件を満たすような万能計算装置であることが理想である．

「汎用コンピュータは，任意の物理的計算装置を効率よく模倣できる．」

ここで，「効率よく」というのは，「たかだか多項式倍の計算時間で」という意味である．つまり，任意の計算装置 M を考え，M がサイズ n の入力に対して，たかだか $t(n)$ ステップ以内に計算を終了するとすれば，汎用コンピュータ U はそれと同じ計算を $(t(n))^k$ ステップ以内に行わなければならない（ただし k は定数）．従来の計算論においては，このような汎用コンピュータの数学的モデルが存在していた．たとえば，万能 Turing 機械という汎用コンピュータは，任意の決定性 Turing 機械を効率よく模倣できることが知られている．

ところで，人間の脳も立派な物理的計算装置であるが，上の命題を「汎用コンピュータは，人間の脳を効率よく模倣できる」としても成り立つだろうか？汎用コンピュータとして，通常の万能 Turing 機械を採用しても，この命題が成り立つか否かは明らかではない．また最近は，ニューラルネットワークが盛んに研究されているが，ニューラルネットワークを汎用コンピュータとして採用したとしても，この命題が成り立つか否かはまだ明らかにされていない．

一方，見方を変えると，通常の Turing 機械は，計算の各ステップや，テープへの情報の書き込み・読み出しが確定的に行われるから，その意味では古典力学で記述できるモデルである．そこで，量子力学を考慮に入れても，上の命題が同様に成り立つかという疑問が生じる．David Deutsch を始めとする何人かの物理学者は，量子力学的原理に基づいて動作するコンピュータのモデル（以下，**量子コンピュータ**と呼ぶ）を考案し，それらの計算論的性質を研究した．そして，

「量子コンピュータは，任意の物理的計算装置（もちろん脳も含む）を効率よく模倣できる．」

ことを示した．

物理学の分野では，電子や原子などのミクロな物理系の振舞いは古典物理学では表現できず，量子力学で表現すると実験事実とよく合致することが知られている．さらに，量子力学的世界を支配する確率法則は，マクロな世界に住んでいる私たち人間の直観には反するものである（**3.4** を参照されたい）．この確率法則のために，量子力学的現象は，私たちが慣れ親しんでいる古典物理学的現象とはまったく異なっている．このことが計算にどのような影響を持つかを最初に問題にしたのは Feynman であった[9),10)]．彼は，古典的なノイマン型コンピュータを用いて量子力学的現象を模倣すると，この確率法則の違いのために，非常に多くの計算時間が必要となる可能性があることを示唆した．彼はまた，この問題を回避するために，量子力学的原理に基づくコンピュータを利用する可能性についても述べた．つまり，彼は暗に次のような問題を提示したのである．

「量子力学的動作原理に基づくコンピュータは，古典的コンピュータよりも効率的に計算が行えるか？」

量子力学的計算に関する初期の研究としては，Benioff[3)] によるものがある．彼は，量子力学の最も基本的な枠組みである量子過程の可逆ユニタリ発展によって，古典的 Turing 機械が模倣できることを示した．しかし，彼は量子力学的動作原

† Quantum Computers by Tetsuro NISHINO (School of Information Science, Japan Advanced Institute of Science and Technology, Hokuriku. Present Address: Department of Communications and Systems, University of Electro-Communications.).

†† 北陸先端科学技術大学院大学情報科学研究科（現所属：電気通信大学電子情報学科）

理を用いることで，より大きな計算能力が得られるか否かについては考察しなかった．

量子計算の明確なモデルを最初に与えたのは，Deutsch[6),7)]であった．彼は量子 Turing 機械と量子回路の両方を定義し，それらのいくつかの性質を研究した．Deutsch によって新たに提案された量子コンピュータには，主に以下のことが期待できる．

1．任意の物理的計算装置の効率的な模倣
2．発熱量の少ない計算機の実現
3．計算速度の向上

このうち1.については，Bernstein と Vazirani[5)],および Yao[26)]の結果から，Deutsch の量子コンピュータは任意の物理的計算装置を効率的に模倣できることが分かった．2.については，量子コンピュータが可逆的計算システム☆であることから，一般に可逆的計算システムについていわれている発熱量の少ないコンピュータの実現可能性[4),18)]は，量子コンピュータも持っている．ところが，3.についてはまだ満足の行く結果が得られていない☆☆．そこで，本稿ではこの3.の問題について考えていきたいと思う．

現在のコンピュータの数学的モデルは Turing 機械であるが，決定性 Turing 機械は巡回セールスマン問題のような NP 完全問題を多項式時間で解くことはできないであろうと，多くの研究者が予想している．そこで，適当な拡張をほどこした Turing 機械上で NP 完全問題を効率よく解こうと，確率的アルゴリズムや近似アルゴリズムという方法が考案されたが，最近までの研究成果から判断すると，これら二つの方法でも，おそらく NP 完全問題は効率的に解けないだろうと思われている☆3．つまり，これはあくまでも推測であるが，現在までに提案された種々の Turing 機械には，NP 完全問題を効率よく解くための機能が不足していると考えられる．

ここで誤解のないように断っておくと，だからといって Turing 機械が悪い計算機モデルだといっているのではない．Turing 機械は非常に簡潔で，しかも理論的に安定したモデルであり，古くは計算可能性の理論から，最近の計算量理論に至るまでの理論計算機科学において，常に中心的役割を果たしてきた素晴らしい計算機モデルである．ご存じのように，1935 年には Church の提唱が行われ，

「**計算可能**とは，Turing 機械で計算できるという意味だと考えよう」

という論理学者の間での合意が得られた．これは，けっして偶然ではない．ラムダ計算等，他の多くの論理学者たちが独立に考えていた計算機モデルが，すべて Turing 機械と等価になったためである．すなわち，当時の数多くの優れた論理学者たちが，懸命に考えた末に得られた形式化がすべて等価だったということは，やはり計算可能という概念が安定したものであるということの証である．

したがって，新たな計算機モデルを考える際に，Turing 機械の考え方を完全に捨ててしまうことは，先人の努力をすべて無駄にするという意味で科学の進む方向として不自然に思えるし，実際，そのようなことはできないくらいに，Turing 機械の概念は安定した自然なものであると思われる．

そこで，Turing 機械の新たな拡張を考えようということになる．もちろん，Turing 機械にどのような機能を付加しても構わないというわけではない．すなわち，新しい機能が付加された Turing 機械が，計算機モデルとしての自然さ，妥当性等を失ってはならない．1985 年に Deutsch は，従来の Turing 機械に**量子並列化機能**を付加した，**量子 Turing 機械**という計算機モデルを提案した[6)]．実はこの量子 Turing 機械が，上で述べた量子コンピュータの数学的モデルである．そこで以下では，**量子コンピュータ**とは，量子 Turing 機械をモデルとするコンピュータのこととする．

量子 Turing 機械は，現在の量子力学に基づいて考えると自然な計算機モデルであり，電子等のミクロな物理系の量子効果を利用して，将来，ま

☆ その計算過程を，一意的に逆もどりできるような計算システムのことをいう．詳しくは文献 18) を参照されたい．

☆☆ 実はごく最近，この状況にブレイクスルーをもたらす結果が AT & T の Shor によって示された．そのことについては 5.で述べる．

☆3 少し詳しいことが知りたい読者へ：BPP ≠ NP であろうと広く信じられている．すなわち，確率的アルゴリズムによって効率よく（多項式時間で）解くことができる問題のクラスは，NP 全体を含まないであろうと信じられている．一方，代表的な NP 完全問題である最大クリーク問題が，近似することさえ非常に困難であろうという状況証拠が，ごく最近証明された．詳しくは文献 2)，20) などを参照されたい．

ったく新しい動作原理に基づくコンピュータが実現できる可能性を示唆している．そして大変興味深いことに，量子Turing機械も**計算可能**な関数しか計算できないことが，Deutsch自身によって示されている[6]．つまり，量子Turing機械も，通常のTuring機械で計算できる関数しか計算できないことが分かった☆．したがって，興味があるのは，同じ計算を行う場合に，量子Turing機械の方が従来のTuring機械よりも高速に計算が行えるかという問題である．

本稿では，主にこの問題について詳しく解説する．まず**2.**では，量子計算のイメージを直観的に説明する．続いて**3.**では，量子コンピュータの数学的モデルである量子Turing機械の定義を行う．**4.**では，量子Turing機械が古典的Turing機械よりも高速に解ける問題の例を示す．**5.**では，量子計算量のクラスを紹介し，さらに，量子Turing機械が従来のコンピュータよりも高速に解けると強く予想される，いくつかの問題を紹介する．また，**6.**では，量子Turing機械上でのNP完全問題の解法について考える．そして，NP完全問題が量子Turing機械上で効率的に解けるか否かは，実は物理学の大問題である**観測問題**と密接に関係していることを示す．最後に**7.**では，量子計算の研究の位置付けや，量子コンピュータの実現可能性等について述べる．なお，量子力学に関する教科書や啓蒙書は良書が多数出版されているが，私の個人的経験から，情報分野の研究者に理解しやすいものとして，文献13)，19)，21)，22)，24)を紹介しておく．また文献11)は，力学系の観点からの量子コンピュータの解説である．

2. 量子コンピュータとは？

Deutschによって考案された量子コンピュータが，通常のTuring機械と最も大きく異なる点は，量子コンピュータでは単一プロセッサ上で任意の並列度☆☆の並列計算が行える点である．

簡単な例で説明する．$f:\{0,1\}^n\to\{0,1\}$をn変数ブール関数とし，異なる二つの入力Xと$Y(X, Y\in\{0,1\}^n)$に対して，fの値（0または1）を求める必要があるとしよう．この場合，通常はまず$f(X)$の値を計算し，その後に$f(Y)$の値を計算しなければならないであろう．しかし，このような計算を行うと，fの値を一つの入力に対して計算するのに必要な時間の，およそ2倍の時間がかかってしまう．

量子コンピュータでは，入力XとYの両方を同時に符号化した入力を用意することができる．これは実際には，XとYをある線形空間内の点$\vec{X}, \vec{Y}$として表現し，量子コンピュータに$\vec{X}+\vec{Y}$を入力することに相当する．この形の符号化を，XとYの**量子重ね合わせ**（quantum superposition）と呼ぶ．この入力に対して，fを計算する通常のプログラムを量子コンピュータ上で走らせると☆，その結果，出力として$f(X)$と$f(Y)$の量子重ね合わせが得られる．このことを，もう少し形式的に述べよう．量子コンピュータは，実際にはfの計算に対応する線形変換（U_fと呼ぼう）を実行する．このとき，U_fの線形性から以下が成り立つ．

$$U_f(\vec{X}+\vec{Y})=U_f(\vec{X})+U_f(\vec{Y})$$

この式の右辺が$f(X)$と$f(Y)$の量子重ね合わせに相当する．この計算においては，fの計算プログラム（すなわち線形変換U_f）は1回しか実行されていないので，この計算に要する時間は，fの値を一つの入力に対して計算するのに必要な時間のみである．入力の量子重ね合わせに対して行われるこのような計算を，**量子並列計算**と呼ぶ．

さらに好都合なことには，**4.**で示すような方法を用いると，量子コンピュータは**指数個**の入力の量子重ね合わせを線形時間で用意することができる．したがって，その入力の重ね合わせに対してfのプログラムを1回実行すれば，すべての入力に対するfの値の量子重ね合わせが得られる．

ここまで読まれた読者は，あまりにも話がうま過ぎると思われたであろうが，現在の量子力学の枠組みに従う限り，ここまでのところは一応問題ない．実は，問題はその後である．上のような計算が行われた後には，たとえば，出力テープ上に2^n個のfの値$f(X_1), f(X_2), \cdots, f(X_{2^n})$が量子重ね合わせの状態で印刷されていることになる．こ

☆ 「計算可能」という概念は，何と安定した概念なのだろうと思わずにはいられない．

☆☆ 量子力学の理論的枠組みに従えば，無限の並列度も許されている．

☆ 量子コンピュータは，通常のTuring機械が実行可能なすべてのプログラムを実行できる．

こで再び，現在の量子力学の枠組みに従うと，出力テープからの値の読み出しに強い制限が課されてしまうのである．

いまの例でいえば，出力の可能な観測方法としては，たとえば，ある $i, 1\leq i\leq 2^n$ に対して，「$f(X_i)=1$ か？」($X_i\in\{0,1\}^n$) を観測することができるが，この場合，

1．実際に $f(X_i)=0$ のときは，上の観測結果は確率1で NO となり，

2．実際に $f(X_i)=1$ のときは，上の観測結果は確率 $1/2^n$ で YES となる

ことしか保証できない（**3.4** 参照）．

このことは，量子コンピュータはすべての入力値に対する計算を効率よく行ったのに，その結果を我々人間が効率よくは読み出せないというジレンマを表している．一方，**4.**で述べるように，量子コンピュータが現在のコンピュータよりも高速に解ける問題がすでに知られている．そのような問題は，量子並列計算と適当な観測方法とをうまく組み合わせれば，効率よく解けるような構造を持っていることが分かる．

3. 量子 Turing 機械

3.1 テンソル積

以下で述べるように，量子 Turing 機械は，物理的には，2状態物理系の合成系としてテンソル積を用いて表現される．そこで，ベクトルの**テンソル積**について復習しておく（ご存じの方は読み飛ばしていただきたい）．ベクトル空間 V_m と V_n の基底ベクトルを，それぞれ $\mathrm{e}_i, i=1,2,\cdots,m$ および，$\mathrm{f}_j, j=1,2,\cdots,n$ とする．このとき，$m\times n$ 個の基底ベクトル $\mathrm{e}_i\mathrm{f}_j$ で張られる mn 次元ベクトル空間を V_m と V_n の**直積空間**といい，$V_m\otimes V_n$ で表す．

例 3.1 $m=3, n=2$ の場合について考える．V_3 の基底ベクトルを，

$$\mathrm{e}_1=\begin{pmatrix}1\\0\\0\end{pmatrix},\quad \mathrm{e}_2=\begin{pmatrix}0\\1\\0\end{pmatrix},\quad \mathrm{e}_3=\begin{pmatrix}0\\0\\1\end{pmatrix}$$

とし，V_2 の基底ベクトルを，

$$\mathrm{f}_1=\begin{pmatrix}1\\0\end{pmatrix},\quad \mathrm{f}_2=\begin{pmatrix}0\\1\end{pmatrix}$$

とする．このとき，6次元の直積空間 $V_3\otimes V_2$ の基底ベクトルを $\mathrm{e}_1\mathrm{f}_1, \mathrm{e}_1\mathrm{f}_2, \mathrm{e}_2\mathrm{f}_1, \mathrm{e}_2\mathrm{f}_2, \mathrm{e}_3\mathrm{f}_1, \mathrm{e}_3\mathrm{f}_2$ の順にとる．V_3 内のベクトル a と，V_2 内のベクトル b を，それぞれ，

$$\mathrm{a}=\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix},\quad \mathrm{b}=\begin{pmatrix}b_1\\b_2\end{pmatrix}$$

とすれば，

$$\mathrm{a}\otimes\mathrm{b}=\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}\otimes\begin{pmatrix}b_1\\b_2\end{pmatrix}=\begin{pmatrix}a_1b_1\\a_1b_2\\a_2b_1\\a_2b_2\\a_3b_1\\a_3b_2\end{pmatrix}$$

となる． □

一般に，V_m から V_m への写像 A が

$$A(ax+by)=aAx+bAy$$

を満たすとき，A を V_m の線形作用素という．ただし，a, b はスカラとし，$x, y\in V_m$ とする．以下では，線形作用素のことを単に**作用素**と呼ぶことにする．

A を V_m の作用素，B を V_n の作用素とするとき，$V_m\otimes V_n$ の作用素 $A\otimes B$ を次のように定義する．

$$(A\otimes B)(z\otimes w)=Az\otimes Bw \tag{3.1}$$

$$(A\otimes B)(ax+by)=a(A\otimes B)x+b(A\otimes B)y \tag{3.2}$$

ここに，a, b はスカラ，$x, y\in V_m\otimes V_n, z\in V_m, w\in V_n$ とする．量子並列計算の基本原理は，上の2式によって説明される（**4.** を参照されたい）．

3.2 量子 Turing 機械の物理的表現

情報の最小単位である**1ビット**を2状態物理系（たとえば，スピン−1/2系等）で構成する．この2状態に対応する物理状態を[0]と[1]で表す．通常，

$$[0]=\begin{pmatrix}1\\0\end{pmatrix},\quad [1]=\begin{pmatrix}0\\1\end{pmatrix}$$

ととる．

また，複数ビットは，同時に観測可能な2状態物理系の合成系により構成される．それゆえ，n **ビット**に対応する物理状態 $[x_1, x_2, \cdots, x_n]$ は，1ビットの物理状態のテンソル積として，以下のように表現される．

$$[x_1,x_2\cdots,x_n]\overset{\text{def.}}{=}[x_1]\otimes[x_2]\otimes\cdots\otimes[x_n]$$

ただし，$x_i\in\{0,1\}, i=1,2,\cdots,n$ とする．

量子Turing機械Mは，通常のTuring機械と同様に，有限制御部，無限長のテープ，およびテープヘッドからなり，それぞれに対応する物理系の合成系として構成される．有限制御部に対応する物理系を$[C]$,テープに対応する物理系を$[T]$,テープヘッドに対応する物理系を$[H]$とする．これらの各物理系もまた，1ビットの物理系の合成系として構成される．すなわち，$C_i\in\{0,1\}, i=1,2,\cdots, u=\log|Q|$とするとき，$[C]=[C_1]\otimes[C_2]\otimes\cdots\otimes[C_u]$と表現できる．また，$M$が$S(n)$-**領域限定**☆ならば，$[T]=[T_1]\otimes[T_2]\otimes\cdots\otimes[T_v], T_i\in\{0,1\}, i=1,2,\cdots, v=S(n)$と表現でき，また$[H]=[H_1]\otimes[H_2]\otimes\cdots\otimes[H_w], H_i\in\{0,1\}, i=1,2,\cdots, w=\log S(n)$と表現できる．

このとき，Mを構成する物理系$[M]$は，これらの物理系の合成系として，以下のように表現される．

$$[M]=[C]\otimes[H]\otimes[T]$$

よって，M**の状態**は，

$$[C;H;T]=[C_1,\cdots,C_u,H_1,\cdots,H_w,T_1,\cdots,T_v]$$

と表現される．これは，2^{u+v+w}次元のHilbert空間内の長さ1のベクトルとして取り扱われる．

3.3 量子Turing機械の定義

定義3.1[5] 量子**Turing機械**（QTM）とは，7項組$M=(Q,\Sigma,\Gamma,U,q_0,B,F)$のことをいう．ただし，

Qは**状態**の有限集合，

Γは**テープ記号**の有限集合，

$B\in\Gamma$は**空白記号**，

$\Sigma\subseteq\Gamma$は**入力記号**の集合，

δは**状態遷移関数**で，$Q\times\Gamma\times\Gamma\times Q\times\{L,R\}$からC（複素数全体）への写像，

$q_0\in Q$は**初期状態**，

$F\subseteq Q$は**受理状態**の集合とする． □

$\delta(p,a,b,q,d)=c$は，Mが状態pで記号aを読んでいるとき（Mのこの様相をc_1と呼ぶ）に，テープ上のヘッドのあるマス目に記号bを書き込み，状態をqに遷移させ，さらにヘッドを方向$d\in\{L,R\}$に1マス分動かす（Mのこの様相をc_2と呼ぶ）という事象の**振幅**(amplitude)がcであることを表している．このとき，Mが様相c_1からc_2に遷移する確率は，$|c|^2$であると定義する☆．

さて，この状態遷移関数δは，以下の行列M_δで表されるような，Mの様相の**重ね合わせ**の線形空間における線形写像を定義する．M_δの各行，各列にはMの様相が対応する．c_1, c_2をMの二つの様相とするとき，M_δのc_1行c_2列成分は，c_2からc_1へのMの1ステップの遷移と対応したδの値である．もしこのような遷移がMに存在しなければ，M_δの対応する成分は0とする．

制約：QTMにおいては，時間推移行列M_δは**ユニタリ行列**でなければならないものとする．

すなわち，$M_\delta^\dagger$をM_δの転置共役行列，Iを単位行列とするとき，$M_\delta^\dagger M_\delta=M_\delta M_\delta^\dagger=I$が成り立つものとする．なお，この制約は量子力学の枠組みを反映したものである．

例3.2 いま，簡単のために，QTM Mの可能な様相がc_1とc_2の二つしかない場合を考えよう．すなわち，

$$M_\delta=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$$

とする．ただし，M_δの各成分a_{ij}は，様相c_jからc_iへのMの1ステップの遷移に対応したδの値とする．このとき，様相c_1はベクトル${}^t(1,0)$で表されるので，c_1からのMの1ステップの遷移は，以下のように表現される．

$$\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}a_{11}\\a_{21}\end{pmatrix}$$

このように，M_δが1回作用するたびにQTMの状態が変化し，計算が1ステップ進行する．上の遷移を，

$$c_1\xrightarrow{M_\delta}a_{11}c_1+a_{21}c_2$$

と表す． □

3.4 計算過程と結果の観測

M**による計算**は，ユニタリ行列M_δによって定義された物理状態の発展過程である．Mの初期状態を$[\psi(0)]$と記す．

$$[\psi(0)]=[q_0;1;T_0]$$

と表わせる．ここで，T_0はMの起動前のテープの内容であり，1マス目から入力が記入され，その入力の右側には無限にBが並んでいるものとする．s時間後の状態を$[\psi(s)]$と記すと，

☆ 記憶領域として，テープ上のたかだか$S(n)$個のマス目しか使えないこと．

☆ 振幅という概念の導入や，振幅に基づく確率の定義等は，量子力学の流儀を踏襲している．

$[\phi(\tau t)]=M_\delta^t[\phi(0)]$

となる．ただし，τ は M が1ステップの実行に要する時間である．

量子力学においては，外部からの観測によって物理系の状態が変化してしまうので，QTM では，計算が終了するまではテープの内容を外部から観測することができない．そこで，計算が停止したことを外部に知らせるために，有限制御部の1ビットを**停止フラグ**として用意する．このビットのみ，外部から観測しても他の状態に影響を与えないものとする．停止フラグは最初0にセットされ，計算が終了すると1に変化する．

さて，停止フラグが1になったときに，テープ上の内容は以下のようにして**観測**することができる．テープ上に様相の重ね合わせ $\psi=\sum_i\alpha_i c_i$ が記入されていたとする．このとき，任意のベクトル ϕ に対し，ψ と ϕ が平行であることを，確率 $|(\phi,\psi)|^2$ で正しく観測することができる．特に，ψ と c_i が平行であることは，確率 $|\alpha_i|^2$ で正しく観測できる．

ここで，QTM の動作が通常の確率法則には従っていないことを見ておこう．QTM M が様相 c_1 および c_2 から様相 c に遷移する振幅が，ともに $\sqrt{p}$ であったとしよう．このとき，c_1 または c_2 から M を起動し，1ステップ後に M の様相を観測したときに，c が観測される確率は p である．次に，M を様相の重ね合わせ $\alpha_1c_1+\alpha_2c_2$ から起動する場合を考えよう．この場合，起動時に M を観測すれば，c_1 が観測される確率は $|\alpha_1|^2$ であり，c_2 が観測される確率は $|\alpha_2|^2$ である．どちらの場合にも，その観測の1ステップ後に再び M を観測すれば，c を観測する条件付き確率は p である．すなわち，M の起動時に c_1 を観測し，その1ステップ後に c を観測する条件付き確率は p である（c_2 の場合も同様）．一方，起動時の観測は行わずに，1ステップ後に初めて M を観測すれば，c を観測する確率は $|\sqrt{p}\,\alpha_1+\sqrt{p}\,\alpha_2|^2=p|\alpha_1+\alpha_2|^2$ であり，$p(|a_1|^2+|a_2|^2)$ ではない☆．このことは，c_1 からの計算と c_2 から計算を同時に行うと，それらが互いに**干渉**することを意味している．たとえば極端な場合として，$\alpha_1=-\alpha_2$ ならば，c_1 と c_2 の寄与は相殺されて，1ステップ後に c が観測される確率は0になる．したがって，QTM の計算の最中に機械の様相を観測することは，計算の流れを本当に変えてしまうことになる．

☆ 通常の確率法則に従って考えると，1ステップ後に c が観測される確率は，起動時に c_1 が観測された1ステップ後に c が観測される確率 $p|\alpha_1|^2$ と，起動時に c_2 が観測された1ステップ後に c が観測される確率 $p|\alpha_2|^2$ の和になるが，量子力学における確率法則に従うと，そのようにはならない．

3.5 万能量子 Turing 機械

Deutsch が導入した万能 QTM $\mathcal{Q}$ のプログラムの記述にあたっては，古典的 Turing 機械で使用可能なすべての操作と，以下の8種類の操作が使用可能である[6]．これら8種類の操作は，いずれも1ビットの状態空間に対するユニタリ変換を表しており，古典的 Turing 機械にはないものである．

$$V_0=\begin{pmatrix}\cos\alpha & \sin\alpha\\ -\sin\alpha & \cos\alpha\end{pmatrix},$$

$$V_1=\begin{pmatrix}\cos\alpha & i\sin\alpha\\ i\sin\alpha & \cos\alpha\end{pmatrix},$$

$$V_2=\begin{pmatrix}e^{i\alpha} & 0\\ 0 & 1\end{pmatrix},\quad V_3=\begin{pmatrix}1 & 0\\ 0 & e^{i\alpha}\end{pmatrix},$$

$V_4=V_0^{-1}$, $V_5=V_1^{-1}$, $V_6=V_2^{-1}$, $V_7=V_3^{-1}$

ここで，α は π の任意の倍数とする．古典的万能 Turing 機械 $\mathcal{U}$ を模倣する QTM $\mathcal{Q}_0$ は，Deutsch が示した方法によって構成でき[6]，$\mathcal{Q}_0$ は $\mathcal{U}$ と同じステップ数で動作する．万能 QTM $\mathcal{Q}$ は，上で述べた8個のユニタリ変換を実行する機能を，$\mathcal{Q}_0$ に付加した QTM である．そこで，$\mathcal{Q}$ のプログラムの実行時間は，以下の規約に従って数えるものとする．

規約　万能 QTM $\mathcal{Q}$ は，古典的 Turing 機械の1ステップを1ステップで実行し，また，上記8種類の各変換は定数ステップで実行する．

4. 量子並列化機能を用いた問題の解法例

D. Deutsch と R. Jozsa は，従来の決定性 Turing 機械と比較して，QTM が指数倍速く解くことができる問題が存在することを示した[8]．本章ではその問題を紹介する．ただし，その問題は，量子並列化機能が効果を発揮するように作られた特殊な問題であることを，あらかじめお断りしておく．しかし，その問題は量子並列化機能を説明する際の最も簡潔な例となっている．実際，**5.** で述べるように，因数分解や離散対数のような現実的な問題に対しても，量子並列化機能を用いた

効率的アルゴリズムがすでに知られているが，それらのアルゴリズムは，本章で示すものよりもかなり複雑であり，本稿の範囲を越えている．

問題 $Z_i=\{0,1,\cdots,i-1\}$ とする．自然数 n と，関数 $f: Z_{2n}\to Z_2$ を計算するオラクル U_f が与えられたときに，以下の二つの文のうちから真であるものを一つ発見せよ．

（a） 関数 f は定数関数0または1ではない．

（b） 関数 f の値の列 $f(0),\cdots,f(2n-1)$ は，正確に n 個の0を含んでいない．

ここで，オラクルとは，常に1ステップで答を返してくれるサブルーチンと考えればよい．ただし，通常のサブルーチンとは異なり，そのソースコード等は見ることができない．その意味で，オラクルはブラックボックスである．特に，ここでのオラクルは，量子 Turing 機械から与えられる量子重ね合わせ状態の入力に対して答を返さなければならないので，いわば「量子オラクル」である．すなわち，量子 Turing 機械と同様な入出力関係を与えるオラクルである．

まず最初に，問題の定義から，(a)と(b)のうち，少なくとも一方は常に真であることに注意する．なぜならば，もし(a)が偽ならば，f は定数関数0または1であるから，$f(0),\cdots,f(2n-1)$ のうちのちょうど n 個（半数）が0であることはなく，したがって，(b)が真となる．逆に，(b)が偽ならば，$f(0),\cdots,f(2n-1)$ のうちのちょうど n 個（半数）が0なので，f は定数関数0または1ではありえず，したがって(a)が真となる．

QTM を用いた，上の問題に対する解法を以下に示すが，その前に，作用素が入力の特定のビットに作用する様子を，入力が2ビットの簡単な場合で見ておこう．入力が x_1x_2 の様相と y_1y_2 の様相（ただし，$x_1,x_2,y_1,y_2\in\{0,1\}$）は，それぞれ $[x_1]\otimes[x_2],[y_1]\otimes[y_2]$ と表現される（略記法では $[x_1,x_2],[y_1,y_2]$ と書かれる）．これらの重ね合わせに対して，作用素 $A\otimes E$（E は恒等作用素）を作用させると，以下のようになる（3.の作用素の定義参照）．

$$(A\otimes E)([x_1]\otimes[x_2]+[y_1]\otimes[y_2])$$
$$=(A\otimes E)([x_1]\times[x_2])$$
$$+(A\otimes E)([y_1]\otimes[y_2])\cdots(3.2)\text{より}$$
$$=(A[x_1]\otimes E[x_2])+(A[y_1]\otimes E[y_2])\cdots(3.1)$$
より
$$=(A[x_1]\otimes[x_2])+(A[y_1]\otimes[y_2])\cdots E\text{が恒等作用素であることより}$$

上の式は，作用素 A が入力の1ビット目に対して線形に作用する様子を表している．

問題を解くための計算を始める前に，二つのユニタリ行列を定義する．

$$S=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad U_2=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$$

これらの行列は，QTM の様相内の1ビットに対して以下のように作用し，様相を遷移させる．

$$S[j]=(-1)^j[j],$$
$$U_2[j]=\frac{1}{\sqrt{2}}([j]+(-1)^j[1-j])$$

QTM の初期様相を

$$[\underbrace{0}_{\text{入力}},\underbrace{0}_{\text{出力}}]$$

と表記する．これは正確には，QTM の様相を，関数 f に対する入力ベクトルと出力ベクトルのテンソル積として表示していることになる．

以下では，QTM のテープ上に書かれた，関数 f の入力と出力を並べて表記し，その組を QTM の様相と考える．つまり，QTM における計算の進行を，そのテープ上の内容のみを表記して示す．まず，関数 f への入力すべての重ね合わせを以下のようにして用意する．

$$[0,0]\xrightarrow{U_{2n}}\frac{1}{\sqrt{2n}}\left(\sum_{i=0}^{2n-1}[i,0]\right)=\varphi$$

ここで，U_{2n} は U_2 を2値の場合から $2n$ 値の場合に拡張した行列である．上の操作は，$\log_2 2n$ ステップで実行できる．実際には，

$$\underbrace{U_2\otimes\cdots\otimes U_2}_{\log_2 2n}$$

で定義されるユニタリ変換を行う．

オラクル U_f が与えられているので，U_f, S, U_f を続けて適用することにより，様相の重ね合わせ φ は以下のように遷移する☆．

$$\varphi\xrightarrow{U_f}\frac{1}{\sqrt{2n}}\left(\sum_{i=0}^{2n-1}[i,f(i)]\right)$$
$$\xrightarrow{E\otimes S}\frac{1}{\sqrt{2n}}\left(\sum_{i=0}^{2n-1}(-1)^{f(i)}[i,f(i)]\right)$$
$$\xrightarrow{U_f}\frac{1}{\sqrt{2n}}\left(\sum_{i=0}^{2n-1}(-1)^{f(i)}[i,0]\right)\equiv\psi$$

☆ ここで，U_f は2ビットの状態空間に対する作用素であり，S は1ビットの状態空間に対する作用素であることに注意する．

この時点でQTMは停止するので，テープ上のベクトルϕとψが平行であるかを観測する．この観測が正しく行われる確率は，

$$|(\varphi,\psi)|^2=\left(\frac{1}{2n}\left|\sum_{i=0}^{2n-1}(-1)^{f(i)}\right|\right)^2$$

である．ϕとψが平行であると観測されたら，(b)が真であると結論し，ϕとψが平行でないと観測されたら，(a)が真であると結論する．

以下では，この方法に従うと，問題が確率1で正しく解けていることを示す．まず，上で述べたように，常に(a)または(b)の少なくとも一方は真であることに注意する．ϕとψが平行なときは，$(\phi,\psi)=1$なので，確率$|(\phi,\psi)|^2=1$でϕとψが平行であることが観測される．したがって，確率1で，(上式の右辺)$=1$であること，すなわち(a)が偽であることが分かるので，(b)が真であると結論できる（ϕとψが平行なときが，(a)が偽となる唯一の場合であることに注意する）．

一方，ϕとψが直交するときは，ϕとψが平行であると観測される確率は$|(\phi,\psi)|^2=0$である．したがって，ϕとψが平行でないと観測されたときには，常に(b)が偽（すなわち(a)が真）と結論しておけば，(b)が偽である唯一の場合（ϕとψが直交するとき）に誤った結論を出すことはない．最後に，ϕとψが平行ではなく，しかも直交もしないときには，(a)と(b)は両方とも真なので，どちらが真であると答えても間違いはない．

以上から上の問題は，QTMを用いれば2回のオラクル呼び出しを用いて，$O(\log n)$ステップで解くことができる．一方，この問題の解法に古典的決定性Turing機械を用いると，少なくとも$n+1$回のオラクル呼び出しが必要となるので[8]，QTMの場合と比較すると指数倍のステップ数がかかる．

5. 量子計算量のクラスについて

量子Turing機械が，古典的Turing機械よりも強力な計算能力を持つかという問題は，文献5)，8)において提出されたが，まだ満足のいく解答が得られていない．たとえば，BPP(Bounded-error Probabilistic Polynomial time，誤り確率限定の確率的Turing機械で多項式時間で解ける問題のクラス）に属することが知られていない問題を，量子Turing機械上で多項式時間で解く方法は知られていない．逆に，古典的Turing機械を用いて，量子Turing機械を指数倍の速度低下なしに模倣する方法も知られていない．

古典的計算量クラスPとBPPに対応する量子計算量クラスを，それぞれEQPおよびBQPという．EQPとBQPは，量子Turing機械上で効率よく解ける問題のクラスと考えることができる．

定義5.1[5] 言語LがクラスEQP (Exact or Error-free Quantum Polynomial time) に属するのは，特別な受理セルを持ったあるQTMと，ある多項式pが存在して，任意の入力記号列xに対し，受理セルを時間$p(n)$に観測すると，xがLに属するか否かを正しく判定できるときをいう．より一般的に，この判定が2/3より大きな確率で正しく行われるならば，言語LはBQP (Bounded-error Quantum Polynomial time) に属するという．

QTMは，通常の意味で計算不能な関数を計算することはできない．実際，BQP⊆PSPACEであることは容易に分かる☆．ここでPSPACEとは，記憶領域のサイズが入力長の多項式で限定された決定性Turing機械で解くことができる問題のクラスである．

定理5.1[5] BQP⊆PSPACE □

BPP ⫋ BQPは成り立つだろうか？直観的には，この関係は成立しそうだが，もしBPP ⫋ BQPが示されれば，定理5.1より，長年の未解決問題であるBPP≠PSPACEも同時に示されることになる．したがって，BPP ⫋ BQPを直接示すことは相当難しいと考えられるので，以下のような研究のアプローチを検討するのが良いであろう．

1. BQP⊆BPPが成り立つと仮定すると，現在異なると信じられている古典的計算量クラスの階層が縮退することを示す．このことが示せれば，BQP⊆BPPとはならないことの状況証拠が得られたことになる．

2. NP⊆BQPであることが示せれば，NP⊆BPPではないと信じられているので，BPP ⫋ BQPの状況証拠が得られる．

☆ 少し詳しいことが知りたい読者へ：Valiantは，定理5.1がBQP⊂#Pに強められることを指摘している[5]．

3. 多項式時間アルゴリズムが知られていないような，よく知られている問題がBQPに属することを証明する．そのような結果が証明できれば，少なくとも，量子並列化機能によって得られた余分な計算能力を，古典的計算によって達成するのが難しいことが示されたことになる．Bernstein と Vazirani[5] も，BPPに属することが知られていない問題に対するQTM上の多項式時間アルゴリズムを与えたが，彼らの問題はその目的のために特別に考えられたものであった．一方，**離散対数問題**と整数の**因数分解問題**は，盛んに研究されているにもかかわらず，多項式時間アルゴリズムが発見されていない数論の問題である．事実，これらの問題は難しいと広く信じられているので，これらの難しさに基礎を置いた暗号系が提案されている．ごく最近，Shor はこれらの問題がQTM上で確率的に多項式時間で解けることを証明した[23]．

量子コンピュータが構築されていない現状においても，Shor の結果は，以下のような重要な意味を持っている．任意のハミルトニアンを古典的コンピュータ上で効率よく模倣できれば，量子コンピュータを古典的コンピュータ上で効率的に模倣することができる．したがって，たかだか多項式倍の速度低下で量子コンピュータを模倣する方法が発見できれば，Shor の結果を用いて，整数の因数分解を行う（通常の意味での）多項式時間アルゴリズムを導くことができる．

6. 量子Turing機械によるNP完全問題の解法について

現在の決定性Turing機械は，NP 完全問題の解法においても必要となる，全解探索の効率化に対してはまったく無力のように思われる．一方，上で述べた量子並列化機能は，このような全解探索の効率化に最も効果的な機能であるように思われる．量子Turing機械を用いて，NP完全問題が多項式時間で解ける可能性はないのであろうか？筆者らは，量子Turing機械を用いたSAT（論理式の充足可能性判定問題）の解法について研究を行い，以下のような結果を得た[16]．

仮定A 様相の重ね合わせの中に，ある特定の様相 C が存在するかを観測したときに，C がその重ね合わせ内に存在していれば，そのことを確率1で，C の入力サイズに関する多項式時間で観測することができる．

定理6.1 仮定Aのもとでは，SATを多項式時間で解く量子Turing機械が存在する． □

SAT がNP完全問題であることより，以下の系がただちに得られる．

系6.1 仮定Aのもとでは，NP⊆EQPが成り立つ． □

ただし，上の仮定Aは「現在の量子力学」においてはまったく支持されていないもので，我々が純粋に数学的目的のために導入した仮定である．そこで，この仮定をもう少し弱めて，以下のような結果を得た[17]．

仮定B 様相の重ね合わせは，観測の後も収束せずに保存される．さらに，重ね合わせ内の各様相は，その重ね合わせ内に存在する様相の個数に比例した時間で観測することができる．

定理6.2 仮定Bのもとでは，SATを $O(2^{\frac{n}{4}})$ 時間で解く量子Turing機械が存在する．ここで，n は充足可能性を判定すべき命題論理式の記述長とする．

この仮定Bも，やはり「現在の量子力学」においては支持されていない．しかし，量子力学における**観測問題**☆は，物理学者の間でもいまだに議論が続いている大問題であり，この問題の答について明確な合意が得られているわけではない．実際，量子力学の分野では非常に高名なY. Aharonovらが，昨年，観測に対するまったく新しい見解を示したが[1]，彼らが示した見解は上の仮定Bに近いものであった．しかし，彼らの見解は実験によって確かめられたものではない．将来，もし仮定Bが実験によって確認されれば，量子コンピュータ上で定理6.2に示した効率が理論的には実現できることになる．

さらに，もし未来の量子力学において仮定Aが支持されるようなことになれば，量子コンピュータを用いてNP完全問題を多項式時間で解くことが可能になるわけである．いずれにしても，量子力学における観測問題の今後の展開が，NP完全問題の効率的解法の可能性に非常に大きな影

☆ 物理系を観測したときに何が起こっているのかを，量子力学自身によって記述する問題．観測による波動関数の収束を，量子力学の枠組みの中で理解したいという要求が，この問題の発端であった．

響を及ぼすことが，明かになったわけである．

7. おわりに

7.1 量子力学，計算量，人間

筆者の力不足から，まとまった話はできないが，最後に，量子力学，計算量理論と人間の三つ巴の関係について，簡単に触れてみたいと思う．

まず，量子力学の計算機科学への貢献について考えてみよう．本文でも述べたとおり，量子コンピュータは可逆的計算システムであるから，将来，発熱の非常に少ない計算機を実現する際のヒントを与えてくれるだろう．また，**5.** と **6.** で紹介したように，量子コンピュータが従来のコンピュータよりも高速に動作する可能性がいくつか指摘されている．

今度は逆に，計算量理論の量子力学への貢献の可能性について考えてみる．もし BPP＝BQP が証明できれば，古典力学で量子力学を効率的に模倣できることになる．一方，BPP≠BQP が証明できれば，そのことが，量子力学が古典力学と真に異なっていることの証拠になる．その意味で，量子計算量理論における結果が，量子力学の成り立ちそのものに影響を与えることになる．将来，計算機科学者がノーベル物理学賞を受賞するなどということは，起こらないのであろうか？

次に，計算量理論や量子力学の観点から，人間について考えてみよう．人間の脳の機能を計算機に模倣させようという研究は，人工知能やニューラルネットワーク等の分野において，ずいぶん昔から活発に行われている．しかし，現在，それぞれの分野で研究者たちは壁にぶつかっているようである．一方，物理学者たちは，人間の脳もひとつの物理的計算装置であるから，物理学的アプローチによって，人間の脳のメカニズムが解明できると考えているようである．Deutsch は 1985 年の論文の中で，「量子 Turing 機械によって，すべての有限な物理的計算装置は完全に模倣できる」と述べている．ということは，人間の脳も量子 Turing 機械であると主張していることになる．はたして，人間の脳は量子効果を利用して動作しているのだろうか？このことについては，物理学者の間でも意見が分かれているようである．

7.2 量子コンピュータの実現可能性について

いまのところ，量子コンピュータの構築法はまだ知られていない．現在の量子力学の枠組みの中で可能な量子コンピュータの設計法について，いくつかの提案がなされたが[14),15),25)]，このうちのどの方法を採用しても本質的な困難があるとの指摘もある[12)]．量子コンピュータの実現可能性については，まだ研究がスタートしたばかりであり，今後の研究成果を待たなければ確実なことは分からない．いずれにしても，Shor の論文のような優れた理論的結果が次々に示されれば，量子コンピュータの実現可能性に関する研究は，いまにも増して加速するであろう．

近年，量子効果デバイスの研究が盛んである．それら量子効果デバイスに基づく計算機のことを量子コンピュータと呼ぶ場合があるようだが，本稿で述べた量子コンピュータとはまったく異なる概念である．前者の量子コンピュータとは，現段階では，量子効果デバイスに基づいて古典的 Turing 機械の動作を実現しようとするモデルのようである（筆者が勉強不足で誤解していた場合には，ご容赦いただきたい）．一方，本稿で紹介した量子コンピュータは，量子力学的効果をそのまま計算の原理として用いようという計算機モデルである．しかし，これら二つの研究がまったく独立であるとは思われない．本稿で説明した量子コンピュータが，将来，実現できるかどうかはまったく分からないが，たとえば，量子効果デバイスの研究成果等から何らかのヒントが得られるのかもしれない．

謝辞　本稿を読んで貴重なコメントをくださった，北陸先端科学技術大学院大学情報科学研究科博士課程の三原孝志君と，閲読者の方々に感謝申しあげます．

参考文献

1) Aharonov, Y., Anandan, J. and Vaidman, L.: Meaning of the Wave Function, Phys. Rev., Vol. A 47, pp. 4616-4626 (1993).
2) Arora, S., Lund, C., Motowani, R., Sudan, M. and Szegedy, M.: Proof Verification and Hardness of Approximation Problems, in Proc. 33 rd IEEE Symp. on Foundations of Comput. Sci. (1992).
3) Benioff, P. A.: Quantum Mechanical Hamiltonian Models of Discrete Processes That Erase Their Own Histories: Application to Turing Machines, Int. J. Theor. Phys., Vol. 21, pp. 177-201 (1982).

4) Bennett, C. H.: Logical Reversibility of Computation, IBM J. Res. Dev., Vol. 6, pp. 525-532 (1973).
5) Bernstein, E. and Vazirani, U.: Quantum Complexity Theory, in Proc. 25 th ACM Symp. on Theor. of Comput., pp. 11-20 (1993).
6) Deutsch, D.: Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, Proc. R. Soc. Lond., Vol. A 400, pp. 97-117 (1985).
7) Deutsch, D.: Quantum Computational Networks, Proc. R. Soc. Lond., bf A 400, pp. 97-117 (1985).
8) Deutsch, D. and Jozsa, R.: Rapid Solution of Problems by Quantum Computation, Proc. R. Soc. Lond., A 439, pp. 553-558 (1992).
9) Feynman, R.: Simulating Physics with Computers, Int. J. Theo. Phys., Vol. 21, pp. 467-488 (1982).
10) Feynman, R.: Quantum Mechanical Computers, Foundations of Phys., Vol. 16, pp. 507-531 (1986).
11) 井宮 淳：計算の物理モデル—量子計算機を中心に—，情報処理，Vol. 35, No. 4, pp. 300-305 (Apr. 1994).
12) Landauer, R.: Is Quantum Mechanics Useful ?, Proc. R. Soc. Lond., to Appear (1994).
13) マイケル・ロックウッド著，奥田 栄訳：心身問題と量子力学，産業図書 (1992).
14) Lloyd, S.: A Potentially Realizable Quantum Computer, Science, Vol. 261, pp. 1569-1571 (1993).
15) Lloyd, S.: Envisioning a Quantum Supercomputer, Science, Vol. 263, p. 695 (1994).
16) Mihara, T. and Nishino, T.: Quantum Computation and NP-Complete Problems, in Proc. Fifth Ann. Int. Symp. on Algorithms and Comput., Beijing, August 25-27 (1994).
17) Mihara, T. and Nishino, T.: On a Method of Solving SAT Efficiently Using Quantum Turing Machine, in Proc. 1994 Workshop on Phys. and Comput., Dallas, Texas, November 17-20 (1994).
18) 森田憲一：計算における可逆性，情報処理，Vol. 35, No. 4, pp. 306-314 (Apr. 1994).
19) 並木美喜雄：量子力学入門，岩波新書 (1992).
20) 太田和夫，岡本龍明：クラス NP の新しい特徴付け，情報処理，Vol. 35, No. 1, pp. 55-68 (Jan. 1994).
21) Penrose, R.: The Emperor's New Mind, Oxford University Press (1989).
22) J. C.ポーキングホーン著，宮崎 忠訳：量子力学の考え方，講談社ブルーバックス (1987).
23) Shor, P. W.: Algorithms for Quantum Computation: Discrete Log and Factoring, DIMACS Tech. Rep. 94-37 (June 1994).
24) 竹内外史：線形代数と量子力学，裳華房 (1987).
25) Teich, W. G., Obermayer, K. and Mahler, G.: Structural Basis of Multistationary Quantum Systems II: Effective Few-Particle Dynamics, Phys. Rev. B, Vol. 37, pp. 8111-8121 (1988).
26) Yao, A.: Quantum Circuit Complexity, in Proc. 34 th Symp. on Foundations of Comput. Sci., pp. 352-361, IEEE Press (1993).

(平成 6 年 8 月 19 日受付)

西野 哲朗 (正会員)

昭和 34 年生．昭和 57 年早稲田大学理工学部数学科卒業．昭和 59 年同大学院理工学研究科博士前期課程修了．同年日本アイ・ビー・エム(株)入社．昭和 62 年東京電機大学理工学部情報科学科助手．平成 4 年北陸先端科学技術大学院大学助教授．平成 6 年電気通信大学助教授．理学博士．自然言語の基礎理論，計算量理論等の研究に従事．電子情報通信学会，LA 各会員．

訂　正

本誌第36巻5号（1995）pp.421-430に掲載されました「ソフトウェアライフサイクルプロセス」のうち，図-1「ソフトウェアライフサイクルプロセスの役割と関係」，図-2「ソフトウェアライフサイクルプロセス，視点およびアクティビティ」，図-4「ソフトウェアを中心としたシステムの取引に関する共通フレーム体系（1994年版）」にある著作権表示は著者の関知しないところで発生した誤りですので，削除してください．お詫びして訂正します．

本誌第36巻4号（1995）pp.337～347に掲載されました「量子コンピュータ」の著者西野哲朗氏の申し出により，p.347の参考文献7）を以下のように訂正します．

7）Deutsch, D:Quantum Computational Networks, Proc. R. Soc. Lond., A 425, pp.73-90 (1989).