効率的量子アルゴリズムの設計手法

西 野 哲 朗†

1985 年に David Deutsch は，量子並列計算が実行できる Turing 機械として，量子 Turing 機械（以下 QTM と略す）を導入した．QTM 上で実行されるアルゴリズムを量子アルゴリズムという．1994 年に Peter Shor が，整数の因数分解に対する多項式時間量子アルゴリズムを設計したことはよく知られている．本論では，Shor のアルゴリズムと Grover のアルゴリズムを具体例として，効率的量子アルゴリズムを設計するための 2 つの主要な手法を説明する．さらに，これらの手法は，種々の効率的量子アルゴリズムの設計に幅広く用いられていることも示す．一方，近年多くの研究者が量子コンピュータの物理的実現法について研究を行っている．なかでも，NMR（核磁気共鳴）が，いくつかの理由により，量子コンピュータの実現方法として有望視されている．しかし，NMR 上で実行される量子計算は，通常の QTM 上の量子計算とは若干異なる．たとえば，NMR 量子コンピュータ上では，Shor のアルゴリズムはそのままでは動作しない．本論では，NMR 量子コンピュータ上で実行される効率的なアルゴリズムの設計法も示す．

How to Design Efficient Quantum Algorithms

Tetsuro Nishino†

In 1985, David Deutsch introduced quantum Turing machines (QTMs for short) as Turing machines which can perform so called quantum parallel computations. Algorithms executed on QTMs are called quantum algorithms. It is well known that Peter Shor designed a polynomial time quantum algorithm for integer factoring in 1994. In this paper, we first illustrate two major methods of designing efficient quantum algorithms with Shor's algorithm and Grover's algorithm as examples. Furthermore, we show that these methods are widely used to design various efficient quantum algorithms. On the other hand, many researchers are studying how to physically implement quantum computers based on the QTM these days. Among others, NMR (Nuclear Magnetic Resonance) offers an appealing prospect for implementation of quantum computers because of a number of reasons. But, quantum computations performed on NMR is slightly different from those performed on QTMs. For example, Shor's algorithm cannot be executed on an NMR quantum computer as it is. In this paper, we also show how to design efficient algorithms executed on NMR quantum computers.

1. はじめに

1985 年に，英国人物理学者 David Deutsch は，量子 Turing 機械（quantum Turing machine，以下 QTM と略す）という量子力学的動作原理に基づく新たな計算モデルを提案した[2),4),7)]．この QTM に基づくコンピュータが，量子コンピュータと呼ばれている．

通常のコンピュータのメモリの 1 区画には，0 または 1 が保持できるが，QTM のメモリの 1 区画には，0 と 1 の任意の重ね合わせ状態が保持できる．ここで，重ね合わせ状態とは，0 に対応する状態ベクトル $|0\rangle$ と 1 に対応する状態ベクトル $|1\rangle$ を，それぞれ，

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

とするとき，$\alpha|0\rangle+\beta|1\rangle$ の形で表されるベクトルの和のことをいう．ただし，α と β は，条件式 $|\alpha|^2+|\beta|^2=1$ を満たす任意の複素数であり，振幅と呼ばれる．この重ね合わせ状態を観測すると，0（または 1）が確率 $|\alpha|^2$（$|\beta|^2$）で読めるものと仮定する．

QTM のテープの 1 区画が保持できる情報量を 1 量子ビット（quantum bit，qubit）という．QTM の動作は，量子ビットに対するユニタリ変換と呼ばれる線形変換の適用という形で表現できる．一方，QTM 上で実行されるアルゴリズムを量子アルゴリズムと呼ぶ．そこで以下では，量子アルゴリズムを量子ビットに適用されるユニタリ変換の系列として記述すること

† 電気通信大学
The University of Electro-Communications

にする．

1994 年に，AT & T の Peter Shor は，整数の因数分解を小さな誤り確率で高速に行う量子アルゴリズムの設計に成功し，世界的な注目を集めた．というのは，現在広く用いられている RSA などの公開鍵暗号が，因数分解問題の難しさを前提として設計されているからである．この Shor の結果に影響されて，量子コンピュータの物理的実現に関する研究が現在さかんに行われている．

現在までに考案された，効率的な量子アルゴリズムの設計法のうち，特に重要なものは次の 2 つである．

(1) 重ね合わせ状態内のある種の周期を高い確率で取り出す．Shor はこの手法を効果的に用い，因数分解と離散対数に対する効率的量子アルゴリズムを設計した[5),8)]．

(2) 重ね合わせ状態内の所望の状態の振幅を高速に増幅する．Grover はこの手法を効果的に用い，データベース検索に対する効率的量子アルゴリズムを設計した[6)]．

以下では，Shor と Grover のアルゴリズムの動作を説明しながら，上記 2 つの効率的量子アルゴリズムの設計法について述べていく．さらに，これらの手法が，種々の効率的量子アルゴリズムの設計に幅広く用いられていることを見るために，Los Alamos National Laboratory の量子物理学アーカイブからの関連論文一覧を示す．

近年，多くの研究者が量子コンピュータの物理的実現法について研究を行っている．なかでも，NMR（核磁気共鳴）が，近い将来における量子コンピュータの実現方法として有望視されている．たとえば，2001 年には IBM を中心とする研究グループが，NMR 量子計算による 15 の因数分解の実験に成功し注目を集めた．しかし，NMR 上で実行される量子計算は，通常の QTM 上の量子計算とは若干異なることが知られている．たとえば，NMR 量子コンピュータ上では，Shor のアルゴリズムをそのままの形では動作させることができない．本論では，NMR 量子コンピュータ上で実行可能な効率的量子アルゴリズムについても考察する．

2. Shor のアルゴリズム

正整数 y と n の最大公約数を (y,n) で表す．y と n が**互いに素**，すなわち $(y,n)=1$ であるとき，関係式

$$y^r \equiv 1 \bmod n$$

を満たす最小の正整数 r を y の mod n の**オーダ**という．

次のような方程式を考える．

$$x^2 \equiv 1 \bmod n \qquad (*)$$

この方程式は，つねに自明な解 $x=\pm 1 \bmod n$ を持ち，n が奇素数ならば，これらが唯一の解である．しかし，n が合成数の場合には，このほかに非自明な解も存在する．もし，$(*)$ の非自明解が与えられれば，n の因数を効率良く発見できることが，整数論の結果から知られている．

正整数 n が与えられたときに，$(*)$ の非自明解 x は，以下のような手続きにより求めることができる．

(1) $1 < y < n$ を満たす正整数 y をランダムに選ぶ．

(2) $(y,n)=1$ であったならば，y の mod n のオーダ r を求める．定義から r は以下の式を満たす．

$$y^r \equiv 1 \bmod n$$

(3) もし，r が偶数であったならば，

$$x = y^{r/2}$$

と置けば，$x^2 \equiv 1 \bmod n$ が成り立つので，x は $(*)$ の非自明解の候補となる．

Shor は，ランダムに選ばれた y のオーダ r が存在するならば，$(\log n)^k$ ステップ（k は定数）以内にそれを発見する多項式時間量子アルゴリズムを設計した．このアルゴリズムは，任意の成功確率 $1-\varepsilon$ $(\varepsilon > 0)$ で r の値を求める確率的アルゴリズムである．

以下に，Shor のアルゴリズムを示すが，その前に，mod q の**離散 Fourier 変換**（以下 DFT_q と略す）という線形変換を定義しておく．この変換は，Shor にアルゴリズムにおいて，中心的な役割を果たす．

DFT_q は，基底 $|0\rangle,\ldots,|q-1\rangle$ に関して，次のように定義される q 次元 Hilbert 空間上のユニタリ変換である（ここでは，量子論の流儀にならって，ベクトル x を $|x\rangle$ と表記している）．

$$DFT_q : |a\rangle \longmapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \exp(2\pi i ac/q)\ |c\rangle$$

このとき，$|0\rangle$ は，すべての $c \bmod q$ の等しい重ね合わせに変換されることに注意する．

Shor の因数分解アルゴリズム

(1) $n^2 \le q \le 2n^2$ を満たす，滑らかな数（定義は後述）q を選ぶ．

(2) n と互いに素な整数 x をランダムに選ぶ．

(3) 毎回，同じ x を用いて，以下の (a) から (g) のステップを，オーダ $\log q$ 回繰り返す．

(a) 量子メモリ・レジスタとして，レジスタ 1

とレジスタ 2 を用意する．レジスタ 1 の量子ビットが状態 reg1 にあり，レジスタ 2 の量子ビットが状態 reg2 にあれば，これら 2 つのレジスタの結合状態を $\left|\mathrm{reg1}, \mathrm{reg2}\right\rangle$ と表す．

(b) レジスタ 1 に DFT_q を適用することにより 0 から $q-1$ までのすべての整数をロードし，また，レジスタ 2 の全量子ビットには 0 をロードする．すなわちレジスタ全体の状態を以下のようにする．

$$\left|\psi\right\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \left|a, 0\right\rangle$$

(c) 量子並列計算により，変換 $x^a \bmod n$ をレジスタ 1 の各数に適用し，その結果をレジスタ 2 に貯える．レジスタ全体の状態は以下のようになる．

$$\left|\psi\right\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \left|a, x^a \bmod n\right\rangle$$

(d) レジスタ 2 の状態を観測し，結果 k を得る．これにより，レジスタ 1 の状態は，$x^a \bmod n = k$ を満たす値 a のみの重ね合わせに射影される．したがって，レジスタ全体の状態は以下のようになる．

$$\left|\psi\right\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} \left|a', k\right\rangle$$

ただし，$|A|$ を集合 A の要素数とするとき，$A = \left\{a' : x^{a'} \bmod n = k\right\}$ である．

(e) 次に，レジスタ 1 の射影後の状態の離散フーリエ変換を計算する．離散フーリエ変換は，各状態 $|a'\rangle$ を以下の重ね合わせに写像する．

$$|a'\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a' c/q} |c\rangle.$$

したがって，離散フーリエ変換の全体としての効果は，レジスタ 1 の射影後の状態を，次の重ね合わせに写像することである．

$$\left|\psi\right\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a' c/q} |c, k\rangle.$$

(f) レジスタ 1 の状態を観測する．この結果，ある整数 c' が得られるが，これは q/r の λ 倍の数である．ただし，r は所望の周期とする．すなわち，ある正整数 λ に対し，$c'/q \approx \lambda/r$ が成り立っている．

(g) 周期 r を決定するためには，λ を評価する必要がある．これは，分母が n より小さい間，c'/q の連分数展開を計算することにより行える．その結果，λ/r に最も近い分数が得られる．

(4) 上記のステップ (a) から (g) を繰り返して，レジスタ 1 における離散フーリエ変換のサンプルの集合を生成する．この結果，種々の整数 λ_i に対して，$1/r$ の倍数のサンプル $\lambda_1/r, \lambda_2/r, \lambda_3/r, \ldots$ が得られる．アルゴリズムを数回繰り返せば，連分数展開法を用いて λ_i を，つまりは r を計算するのに十分な，レジスタ 1 のサンプルが得られる．

(5) r が分かれば，n の因数は，$\gcd\left(x^{r/2}-1, n\right)$ および，$\gcd\left(x^{r/2}+1, n\right)$ の値として得ることができる．

Shor のアルゴリズムの直観的説明

次に，Shor のアルゴリズムの動作を直観的に説明する．因数分解すべき整数 n が与えられたら，まず n^2 以上 $2n^2$ 以下の滑らかな整数 q を選ぶ．整数 q は，そのすべての素因数ベキが $O((\log q)^k)$ であるときに，滑らかであるという．ただし，k は q とは独立な定数とする．

次に，$x \bmod n$ をランダムに選び，量子メモリ・レジスタに，$|0,0\rangle$ と記入から計算を開始する．以下では，アルゴリズムの処理の流れを，レジスタの内容の変化で説明していく．まず，DFT_q をレジスタ 1 に適用すると，レジスタの内容は以下のように変化する．

$$|0,0\rangle + |1,0\rangle + |2,0\rangle + \cdots + |q-1,0\rangle$$

これは，直観的には q 個のレジスタが重ね合わされたものを表現している．厳密には各レジスタはある振幅を持っているのだが，ここでは振幅は省略してある．

次に，$x^a \bmod n$ を計算し，その結果をレジスタ 2 に貯える．すると，レジスタの重ね合わせは以下のように変化する．

$$|0, x^0 \bmod n\rangle + |1, x^1 \bmod n\rangle + |2, x^2 \bmod n\rangle + \cdots + |q-1, x^{q-1} \bmod n\rangle$$

ここで，レジスタ 2 のラベルを決定するために観測を行う．すると，詳細は省略するが，観測後のレジスタ 1 の重ね合わせは次のようになる（以下では，レジスタ 1 の内容のみを表記する）．

$$|l\rangle + |r+l\rangle + |2r+l\rangle + \cdots + |ar+l\rangle$$

ただし，a はある整数であり，また，r は求めるべき x の $\bmod n$ のオーダである．すなわち，重ね合わせ内のレジスタ 1 の内容が，求めるべきオーダ r の周期を持っているのである．我々はこの重ね合わせから，観測によって r を読み出したいわけだが，この重ね合わせを直接観測しても，等確率で 1 つの値

$kr+l$ $(0 \le k \le a)$ が読めるだけである．k も l も未知であるから，これでは r の値は分からない．

そこで，レジスタ 1 にもう一度 DFT_q を適用する．2 回目のフーリエ変換を適用すると，レジスタ 1 の重ね合わせは以下のように変化する（ただし，ここでは話を簡単にするために，重ね合わせが以下のような簡潔な形になる，特殊な場合について説明している）．

$$|0\rangle + |q/r\rangle + |2q/r\rangle + \cdots + |(r-1)q/r\rangle$$

レジスタの内容の周期が r から q/r に変化していることに注意する．この段階でレジスタ 1 の重ね合わせを観測すると，値 $\lambda q/r$ $(\lambda = 0, \ldots, r-1)$ が等確率で読み出される．

$c = \lambda q/r$ と置くと，観測後には，$c/q = \lambda/r$ を満たす値 c が得られていることになる．ここで，c と q は既知であるから，もし，$(\lambda, r) = 1$ ならば，c/q を既約分数にまで払うことにより，r を求めることができる．λ はランダムに選ばれているので，十分大きい r に対しては，$(\lambda, r) = 1$ となる確率は $1/\log r$ よりも大きいことが知られている．したがって，上の計算を $O(\log r)$ 回繰り返せば，正しく r を求める確率をいくらでも 1 に近づけることができる．

3. Grover のアルゴリズム

いま，$0 \le k \le 2^n - 1$ なる整数 k の集合を定義域とする関数 f を考える．すなわち，f の定義域には 2^n 個の整数が含まれている．この定義域の中に，特別な整数 k_0 が存在して，$x = k_0$ のときのみ $f(x) = 1$ となり，それ以外の x に対しては $f(x) = 0$ となるものとする．関数 f に対する**オラクル**とは，f の定義域に属する整数 x が入力として与えられると，$f(x)$ の値（0 または 1）を返すブラックボックスのことをいう．また，関数 f に対する**量子オラクル**とは，f の定義域に属する整数 x の重ね合わせ $\alpha_1 x_1 + \alpha_2 x_2 + \cdots \alpha_n x_n$ が入力として与えられると，$f(x)$ の値（0 または 1）の重ね合わせ $\alpha_1 f(x_1) + \alpha_2 f(x_2) + \cdots \alpha_n f(x_n)$ を返すブラックボックスのことをいう．Grover のアルゴリズムが扱う問題は，以下のとおりである．

問題：上のような関数 f に対する量子オラクルが与えられたときに，k_0 を発見せよ．

この問題を解くために，f の定義域を古典的に探索した場合，k_0 を発見するまでの $f(x)$ の評価回数の期待値は 2^{n-1} となる．これに対し，Grover のアルゴリズムでは，この評価回数の期待値を $\sqrt{2^n} = 2^{n/2}$ にすることができる．

Grover のアルゴリズム

(1) n 量子ビットを 0 に設定し，$n+1$ 番目の量子ビットは $|\chi\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ に設定する．これは，最初に $n+1$ 番目の量子ビットを 1 にセットしておき，そこに，ユニタリ変換

$$V = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

を適用することにより，行うことができる．すなわち，以下のような変換を行う．

$$V|1\rangle = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = (|0\rangle - |1\rangle)/\sqrt{2}$$

この結果，$|\underbrace{0\cdots0}_{n \text{ times}}\rangle|\chi\rangle$ という状態が得られる．

(2) 左端の n 量子ビットに左から順に変換 V を適用する．たとえば，$n = 2$ のときには，以下のような変換が行われる．

$$\begin{aligned} &|00\rangle = |0\rangle \otimes |0\rangle \\ &\to \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle \\ &\to \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) \\ &\to \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle\tfrac{1}{2}|10\rangle + \tfrac{1}{2}|11\rangle \end{aligned}$$

結局，以下の状態が得られる．

$$|\underbrace{0\cdots0}_{n \text{ times}}\rangle|\chi\rangle \sum_{k=0}^{2^n-1} a_k|k\rangle|\chi\rangle = |\psi\rangle|\chi\rangle$$

ただし，$a_k = 1/\sqrt{2^n}$ とする．

(3) 以下のステップ (a)，(b) を m 回繰り返す（m の値は後で定める）．

(a) オラクルとして与えられたユニタリ作用素 U_f を用いて，f の値を評価し，第 $n+1$ 量子ビットにその値を書き込む．以下のような変換が行われる．

$$|\psi\rangle|\chi\rangle \to |\psi\rangle U_f|\chi\rangle \to \sum_{k=0}^{2^n-1} a_k|k\rangle(-1)^{f(k)}|\chi\rangle$$

この変換を位相回転といい T と呼ぶ．

(b) 第 1 から n 量子ビットに，拡散作用素 $D = -I + 2J/N$ を適用する．ここで，I は単位行列，J はすべての成分が 1 の行列である．D がユニタリ行列であることは容易に分かる．

$$\sum_{k=0}^{2^n-1} a_k(-1)^{f(k)}|k\rangle|\chi\rangle \to \sum_{k=0}^{2^n-1} a'_k|k\rangle|\chi\rangle$$

(4) 第 1 から n 量子ビットを観測し，k の値を決定する．

(5) $f(k)$ の値を求める．$f(k)=1$ ならば終了．さもなければ，ステップ 1 からやり直す．

例 3.1 $n=2$，$k_0=2$ とする．すなわち，$f(0)=f(1)=f(3)=0$，$f(2)=1$ とする．ステップ 1 終了後に，以下のような重ね合わせ状態が得られる．

$$\begin{aligned}&|00\rangle|\chi\rangle \to \textstyle\sum_{k=0}^{3}\frac{1}{2}|k\rangle|\chi\rangle\\&=\tfrac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)|\chi\rangle\\&=|\psi\rangle|\chi\rangle\end{aligned}$$

T の対角成分は $(-1)^{f(k)}=1-2f(k)$ であるから，

$$T=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix}$$

となる．また，

$$\begin{aligned}&D=-I+\tfrac{2J}{4}=\\&-\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}+\tfrac{1}{2}\begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}\\&=\tfrac{1}{2}\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}\end{aligned}$$

となる．よって，以下を得る．

$$\begin{aligned}&M=DT\\&=\tfrac{1}{2}\begin{pmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\\&=\tfrac{1}{2}\begin{pmatrix}-1&1&-1&1\\1&-1&-1&1\\1&1&1&1\\1&1&-1&-1\end{pmatrix}\end{aligned}$$

M を 1 回適用すると，以下を得る．

$$\begin{aligned}&|\varphi\rangle=M|\psi\rangle\\&=\tfrac{1}{2}\begin{pmatrix}-1&1&-1&1\\1&-1&-1&1\\1&1&1&1\\1&1&-1&-1\end{pmatrix}\tfrac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\end{aligned}$$

この重ね合わせ状態を観測すると，ラベル 10 が確率 1 で観測できる．ところが，変換 M を 2 回適用すると，

$$M^2|\varphi\rangle=\frac{1}{2}|10\rangle-\sum_{k\neq 2}\frac{1}{2}|k\rangle$$

となり，正解率が 1/4 になってしまう．

上記のアルゴリズムの実行前に，ステップ (3)(a)，(3)(b) のループの反復回数 m を事前に定めなければならない．そこで，反復回数に関する考察を行う．以下では，話を簡単にするために，$N=4$ の場合を考える．いま，r_0 を正解でない状態の共通の初期振幅，s_0 を正解の状態の初期振幅とする．このとき，変換 M の適用により，以下を得る．

$$\begin{aligned}&\tfrac{1}{2}\begin{pmatrix}-1&1&-1&1\\1&-1&-1&1\\1&1&1&1\\1&1&-1&-1\end{pmatrix}\begin{pmatrix}r_0\\r_0\\s_0\\r_0\end{pmatrix}\\&=\tfrac{1}{2}\begin{pmatrix}r_0-s_0\\r_0-s_0\\3r_0+s_0\\r_0-s_0\end{pmatrix}=\begin{pmatrix}r_1\\r_1\\s_1\\r_1\end{pmatrix}\end{aligned}$$

この振幅の発展の様子は，以下の 2 次の正方行列を用いて表現できる．

$$\begin{pmatrix}r_1\\s_1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1&-1\\3&1\end{pmatrix}\begin{pmatrix}r_0\\s_0\end{pmatrix}R\left(\frac{\pi}{3}\right)\begin{pmatrix}r_0\\s_0\end{pmatrix}$$

ただし，ここで，$R\left(\frac{\pi}{3}\right)$ は，原点中心 $\pi/3$ 回転を表す．

$$\begin{aligned}&\begin{pmatrix}a_1\\b_1\end{pmatrix}=\begin{pmatrix}\sqrt{3}&0\\0&1\end{pmatrix}\begin{pmatrix}1/2&-1/2\\3/2&1/2\end{pmatrix}\\&\qquad\begin{pmatrix}1/\sqrt{3}&0\\0&1\end{pmatrix}\begin{pmatrix}a_0\\b_0\end{pmatrix}R\left(\tfrac{\pi}{3}\right)\begin{pmatrix}a_0\\b_0\end{pmatrix}\end{aligned}$$

となる．初期状態ベクトルは，以下のとおりである．

$$\begin{aligned}&\begin{pmatrix}1/2\\1/2\end{pmatrix}=\tfrac{1}{2}\begin{pmatrix}\sqrt{3}&0\\0&1\end{pmatrix}\begin{pmatrix}1/2\\1/2\end{pmatrix}\\&=\begin{pmatrix}\sqrt{3}/2\\1/2\end{pmatrix}=\begin{pmatrix}\cos\pi/6\\\sin\pi/6\end{pmatrix}\end{aligned}$$

つまり，上記アルゴリズムにおいて，1 回目の反復の後には，状態ベクトルの偏角は $\pi/6+\pi/3=\pi/2$ となり，正解が観測される確率は最大値 1 をとるが，もう 1 回反復すると，状態ベクトルの偏角が $\pi/2+\pi/3=5\pi/6$ となり，正解が観測される確率は減少してしまう．

一般の場合には，

$$R(\theta)=\begin{pmatrix}1-2/\sqrt{N}&-2\sqrt{N-1}/N\\2\sqrt{N-1}/N&1-2/N\end{pmatrix}$$

となる．$\sin\theta = 2\sqrt{N-1}/N \approx 1/\sqrt{N}$

ここで，N が十分大きいと（すなわち，θ が十分小さいと）$\sin\theta \approx \theta$ より，$\theta \approx 2/\sqrt{N}$ が成り立つ．一方，$m\theta + \theta/2 \approx \pi/2$ より，以下が成り立つ．

$$m \approx \frac{\pi}{2} \times \frac{\sqrt{N}}{2} - \frac{1}{2} = \frac{\pi}{4}\sqrt{N} - \frac{1}{2}$$

4. NMR 量子計算アルゴリズム

近年，量子計算機の実現に関する研究がさかんに行われており，量子ドット，イオントラップ，単一光子などの方法が提案されている．1990 年代後半に NMR（Nuclear Magnetic Resonance，核磁気共鳴）という一般的な分析装置と，有機分子の液体によって量子計算を行う方法が提案された[3]．NMR 法は，分子を構成する原子 1 つ 1 つを区別して見ることを可能にする方法で，現在，有機化合物の分子構造解析の分野で威力を発揮している．この方法を用いた量子計算を NMR 量子計算と呼ぶ．本章では，近い将来に比較的容易に実現可能と思われている，この NMR 量子計算を取り上げる．

NMR 量子計算と通常の量子計算の相違は，計算結果の観測の規約が以下のように異なっている点にある．一般に量子計算の出力は，量子メモリレジスタ上に，$\alpha|0\rangle + \beta|1\rangle$ という形の重ね合わせ状態として保持される．ただし，α と β は，条件式 $|\alpha|^2 + |\beta|^2 = 1$ を満たす任意の複素数であり，振幅と呼ばれるのであった．

通常の量子計算の場合，重ね合わせ状態 $\alpha|0\rangle + \beta|1\rangle$ を観測すると，0（または 1）が確率 $|\alpha|^2$（$|\beta|^2$）で読めるものと仮定される．一方，NMR 量子計算においては，同じ重ね合わせ状態を観測すると，確率 1 で，$|\beta|^2 - |\alpha|^2$ という実数値が観測できるものと仮定される．また，NMR における観測では，波束が収縮しないので，重ね合わせ状態を乱さずに定数回の観測を行うことができる．

入力長の多項式時間で実行できるアルゴリズム**多項式時間アルゴリズム**といい，また答が yes または no である問題を**判定問題**という．QTM 上の多項式時間計算量のクラス EQP は次のように定義される．判定問題 L がクラス **EQP**（Exact Quantum Polynomial time）に属するのは，ある量子アルゴリズムと，ある多項式 p が存在して，任意の入力記号列 x に対し，時刻 $p(|x|)$ に観測を行うと，x に対する問題 L の答が yes であるか no であるかを，確率 1 で正しく判定できるときをいう．

次に，クラス EQP に対応する NMR 量子計算の計算量クラス EBQP を以下のように定義する．問題 L がクラス **EBQP**（Exact Bulk Quantum Polynomial time）に属するのは，ある NMR 量子計算アルゴリズムと，ある多項式 p が存在して，任意の入力記号列 x に対し，時刻 $p(|x|)$ に観測を行うと，x に対する L の答が yes ならば観測値 1 が確率 1 で観測され，no ならば観測値 -1 が確率 1 で観測されるときをいう．このとき，以下の定理が証明できる．

定理 4.1 $EQP = EBQP$

証明 （$L \in EQP \Longrightarrow L \in EBQP$ の証明） $L \in EQP$ より，ある量子アルゴリズム M と，ある多項式 p が存在して，任意の入力記号列 x に対し，時刻 $p(|x|)$ に観測を行うと，x に対する L の答が yes ならば値 1 が確率 1 で観測され，no ならば値 0 が確率 1 で観測される．これとまったく同様の計算が，NMR 量子コンピュータによっても実行できる．ただし，結果の観測の部分だけが，以下のように異なってくる．

x に対する L の答が yes のとき，時刻 $p(|x|)$ に値 1 が確率 1 で観測されるので，量子メモリ・レジスタの重ね合わせ状態 $\alpha|0\rangle + \beta|1\rangle$ においては，$|\alpha|^2 = 0$ かつ $|\beta|^2 = 1$ より，$|\beta|^2 - |\alpha|^2 = 1$ となる．よって，NMR 量子コンピュータでは，観測値 1 が確率 1 で観測される．

x に対する L の答が no のときは，時刻 $p(|x|)$ に値 0 が確率 1 で観測されるので，レジスタの重ね合わせ状態 $\alpha|0\rangle + \beta|1\rangle$ においては，$|\alpha|^2 = 1$ かつ $|\beta|^2 = 0$ より，$|\beta|^2 - |\alpha|^2 = -1$ よって，NMR 量子コンピュータでは，観測値 -1 が確率 1 で観測される．

（$L \in EQP \Longleftarrow L \in EBQP$ の証明） $L \in EBQP$ より，NMR 量子計算アルゴリズムと，ある多項式 p が存在して，任意の入力記号列 x に対し，時刻 $p(|x|)$ に観測を行うと，x に対する L の答が yes ならば観測値 1 が確率 1 で観測され，no ならば観測値 -1 が確率 1 で観測される．

x に対する L の答が yes のとき，時刻 $p(|x|)$ に観測値 1 が確率 1 で観測されるので，M の受理セルの重ね合わせ状態 $\alpha|0\rangle + \beta|1\rangle$ において，$|\beta|^2 - |\alpha|^2 = 1$ かつ $|\alpha|^2 + |\beta|^2 = 1$ より，$|\beta|^2 = 1$ となる．よって，量子メモリ・レジスタに対して，通常の観測を行うと，値 1 が確率 1 で観測される．

x に対する L の答が no のとき，時刻 $p(|x|)$ に観測値 -1 が確率 1 で観測されるので，レジスタの重ね合わせ状態 $\alpha|0\rangle + \beta|1\rangle$ において，$|\beta|^2 - |\alpha|^2 = -1$ かつ $|\alpha|^2 + |\beta|^2 = 1$ より，$|\alpha|^2 = 1$ となる．よって，通常の観測を行うと，値 1 が確率 1 で観測される．

以上により，$L \in EQP \Longleftrightarrow L \in EBQP$ が証明された． □

誤り限定確率の計算とは，誤り確率がある正の定数 $\varepsilon < \frac{1}{2}$ でおさえられる計算のことをいう．誤り限定確率の量子計算量クラス BQP は次のように定義される．問題 L がクラス **BQP**（Bounded error Quantum Polynomial time）に属するのは，ある量子アルゴリズムと，ある多項式 p が存在して，任意の入力記号列 x に対し，受理セルを時刻 $p(|x|)$ に観測を行うと，x に対する L の答を確率 $\frac{2}{3}$ 以上で正しく判定できるときをいう．

次に，クラス BQP に対応する NMR 量子計算量のクラス BBQP を定義する．問題 L がクラス **BBQP**（Bounded error Bulk Quantum Polynomial time）に属するのは，ある NMR 量子計算アルゴリズムと，ある多項式 p が存在して，任意の入力記号列 x に対し，時刻 $p(|x|)$ に観測を行うと，x に対する L の答が yes ならば $\frac{1}{3}$ 以上の観測値が確率 1 で観測され，一方，no ならば $-\frac{1}{3}$ 以下の観測値が確率 1 で観測されるときをいう．定理 3.1 とほぼ同様にして，以下の定理も証明できる．

定理 4.2 $BQP = BBQP$ □

上の定理からも分かるように，判定問題に対しては，NMR 量子コンピュータは通常の量子コンピュータをまったく同じ効率の計算を行える．しかし，因数分解のように，答が 1 ビットになるとは限らない関数問題においては，NMR 量子コンピュータが通常の量子コンピュータと同じ効率の計算が行えるか否かは明らかではない．

しかし，Grover のアルゴリズムについては，通常の解が 1 つしか存在しない場合には，NMR 量子計算アルゴリズムとしてもそのまま正しく動作することが分かる．また，Shor の因数分解アルゴリズムの実行や，NP 完全問題の解法にも，NMR 量子計算が適応可能であることが分かっている[1)]．

5. おわりに

量子計算，量子暗号，量子通信などに関する最も豊富な情報を提供しているアーカイブは，Los Alamos National Laboratory の量子物理学アーカイブ

http://xxx.lanl.gov/archive/quant-ph

である．

Shor のアルゴリズムと Grover のアルゴリズムがさまざまな量子アルゴリズムの設計に応用されていることを見るために，Los Alamos National Laboratory の量子物理学アーカイブに登録された関連論文一覧を付録として掲載しておく．この一覧を見ると，Grover のアルゴリズムが，その簡潔性から幅広く応用されていることがよく分かる．

本論は，量子コンピュータに関する研究の中でも，特に量子アルゴリズムに話題を限定しているが，このアーカイブには，量子アルゴリズムに関する論文以外にも，量子コンピュータの実現についての物理寄りの論文などが多数登録されている．ただし，このアーカイブに登録される論文は，査読前のものもあり，また，著者が頻繁に変更を加える場合もあることを，あらかじめお断りしておく．

Shor と Grover の方法以外の，効率的量子アルゴリズムの新たな設計手法の開発が，量子アルゴリズム論における最も重要な課題となっている．

参考文献

1) 渥美賢嗣，西野哲朗：NMR 量子計算による NP 完全問題と因数分解の解法，情報処理学会論文誌：数理モデル化と応用（本号）．
2) Bernstein, E. and Vazirani, U.: Quantum Complexity Theory, *Proc. 25th ACM Symposium on Theory of Computing*, pp.11–20 (1993).
3) Chuang, I.L., Gershenfeld, N., Kubinec, M.G. and Leung, D.W.: Bulk Quantum Computation with Nuclear Magnetic Resonance: Theory and Experiment, *Proc. R. Soc. Lond.*, Vol.A 454, pp.447–467 (1998).
4) Deutsch, D.: Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proc. R. Soc. Lond.*, Vol.A400, pp.97–117 (1985).
5) Ekert, A. and Jozsa, R.: Quantum computation and Shor's factoring algorithm, *Reviews of Modern Physics*, Vol.68, No.3, pp.733–753, July (1996).
6) Grover, L.: A Fast Quantum Mechanical Algorithm for Database Search, *Proc. 28th Annual ACM Symposium on Theory of Computing*, pp.212–219, ACM, New York (1996).
7) 西野哲朗：量子コンピュータ入門，東京電機大学出版局 (1997).
8) Shor, P.W.: Algorithms for Quantum Computation: Discrete Log and Factoring, *Proc. 35th Annual IEEE Symposium on Foundations of Computer Science*, pp.124–134 (1994).

付録　Los Alamos National Laboratory 量子物理学アーカイブに登録された関連論文一覧

Shor のアルゴリズム関連

(1) Quantum Algorithm and the Fourier Transform, Richard Jozsa, quant-ph/9707033
(2) Fast versions of Shor's quantum factoring algorithm, Christof Zalka, quant-ph/9807006
(3) Sampling Fourier Transforms on Different Domains, Lisa Hales and Sean Hallgren, quant-ph/9812060
(4) The Influence of Superpositional Wave Function Oscillations on Shor's Quantum Algorithm, Gennady P. Berman, Gary D. Doolen, and Vladimir I. Tsifrinovich, quant-ph/9906045
(5) Introduction to Quantum Algorithms, Peter W. Shor, quant-ph/0005003

Grover のアルゴリズム関連

(1) Tight bounds on quantum searching, Michel Boyer, Gilles Brassard, Peter Hoyer, and Alain Tapp, quant-ph/9605034.
(2) A Quantum Algorithm for Finding the Minimum, Christoph Durr, and Peter Hoyer, quant-ph/9607014
(3) Quantum Algorithm for the Collision Problem, Gilles Brassard, Peter Hoyer, and Alian Tapp, quant-ph/9705002
(4) Quantum computers can search arbitrarily large databases by a single query, Lov K.Grover, quant-ph/9706005
(5) Quantum Mechanics helps in searching for a needle in haystack, Lov.K.Grover, quant-ph/9706033
(6) On the Complexity of Quantum Searching Using Complex Queries, Markus Grassl, and Thomas Beth, quant-ph/9706052
(7) Quantum Database Searching by a Single Query, Dong Pyo Chi, and Jinsoo Kim, quant-ph/9708005
(8) Quantum Mechanical Square Root Speedup in a Structured Search Problem, Edward Farhi, and Sam Gutmann, quant-ph/9711035
(9) Grover's quantum searching algorithm is optimal, Christof Zalka, quant-ph/9711070
(10) Quantum computers can search rapidly by using almost any transformation, Lov K. Grover, quant-ph/9712011
(11) Quantum search on structured problems, Lov K. Grover, quant-ph/9802035
(12) Local Search Method for Quantum Computers, Tad Hogg, and Mehmet Yanik, quant-ph/9802043
(13) Implementation of a Quantum Search Algorithm on a Nuclear Magnetic Resonance Quantum Computer, J.A. Jones, M. Mosca, R.H. Hansen, quant-ph/9805069
(14) Quantum Counting, Gilles Brassard, Peter Hoyer, and Alain Tap, quant-ph/9805082
(15) Nested quantum search and NP-complete problems, N.J. Cerf, L.K. Grover, and C.P. Williams, quant-ph/9806078
(16) Grover's Quantum Search Algorithm for an Arbitrary Initial Amplitude Distribution Eli Biham, Ofer Biham, David Biron, Markus Grassl, and Daniel A.Lidar, quant-ph/9807027
(17) Fast quantum search algorithm and Bounds on it, Arun Kumar Pati, quant-ph/9807067
(18) A Modification of Grover's Algorithm as a Fast Database Search, D.A. Ross, quant-ph/9807078
(19) Fast Quantum verification for the formulas of predicate calculus, Yuri Ozhigov, quant-ph/9809015
(20) How fast can a quantum computer search?, Lov K. Grover, quant-ph/9809029
(21) Reasoning about Grover's Quantum Search Algorithm using Probabilistic wp, Michael Butler, and Pieter Hartel, quant-ph/9810066
(22) Searching in Grover's Algorithm, Richard Jozsa, quant-ph/9901021
(23) Could Grover's quantum algorithm help in searching an actual database?, Christof Zalka, quant-ph/9901068
(24) A Grover-based quantum search of optimal order for an unknown number of marked elements, Christof Zalka, quant-ph/9902049
(25) Noise in Grover's Quantum Search Algo-

rithm, B. Pablo-Norman and M. Ruiz-Altaba, quant-ph/9903070
(26) Generalized Quantum Search with Parallelism, Robert Gingrich, Colin P. Williams, and Nicolas Cerf, quant-ph/9904049
(27) Arbitrary phase rotation of the marked state can not be used for Grover's quantum search algorithm, Gui Lu Long, Wei Lin Zhang, Yan Song Li and Li Niu, quant-ph/9904077
(28) Phase matching in quantum searching, Gui Lu Long, Yan Song Li, Wei Lin Zhang and Li Niu, quant-ph/9906020
(29) Grover's Algorithm for Multiobject Search in Quantum Computing, G. Chen, S.A. Fulling, snd M.O. Scully, quant-ph/9909040
(30) An intrinsic limitation on the size of quantum database, Gui Lu Long, Yan Song Li, Wei Lin Zhang and Chang Cun Tu, quant-ph/9910076
(31) Grover's Algorithm for Multiobject Search in Quantum Computing, G. Chen, S.A. Fulling, M.O. Scully, quant-ph/9909040
(32) Quantum Algorithms and the Genetic Code, Apoorva Patel, quant-ph/0002037
(33) Rapid sampling through quantum computing, Lov K. Grover, quant-ph/9912001
(34) Fast Quantum Search Algorithms in Protein Sequence Comparison - Quantum Biocomputing, Lloyd C.L. Hollenberg, quant-ph/0002076
(35) Quantum searching with continuous variables, Arun K. Pati, Samuel L. Braunstein and Seth Lloyd, quant-ph/0002082
(36) Quantum Amplitude Amplification and Estimation, Gilles Brassard, Peter Hoyer, Michele Mosca, Alain Tapp, quant-ph/0005055
(37) Finding Matches between Two Databases on a Quantum Computer, Mark Heiligman, quant-ph/0006136
(38) Generalization of Grover's Algorithm to Multiobject Search in Quantum Computing, Part II: General Unitary Transformations, Goong Chen, Shunhua Sun, quant-ph/0007124
(39) Quantum Algorithms for Weighing Matrices and Quadratic Residues, Wim van Dam, quant-ph/0008059
(40) A Family of Grover's Quantum Searching Algorithms, Alberto Galindo, Miguel A. Martin-Delgado, quant-ph/0009086
(41) A New Formulation of Grover's Algorithm, Michael Stay, quant-ph/0010028
(42) Analysis of Generalized Grover's Quantum Search Algorithms Using Recursion Equations, Eli Biham, Ofer Biham, David Biron, Markus Grassl, Daniel A. Lidar, and Daniel Shapira, quant-ph/0010077
(43) Artificial Orbitals and a Solution to Grover's Problem, Michael Stay, quant-ph/0010065
(44) An Exponentially Fast Quantum Search Algorithm, Goong Chen and Zijian Diao, quant-ph/0011109
(45) Searching with Quantum Computers, Lov K. Grover, quant-ph/0011118
(46) Faster Database search in Quantum Computing, Li-Yi Hsu and Yih-Yuh Chen, quant-ph/0102068
(47) Grover Algorithm with zero theoretical failure rate, G.L. Long, quant-ph/0106071
(48) Quantum Search by Local Adiabatic Evolution, Jeremie Roland and Nicolas J. Cerf, quant-ph/0107015
(49) Quantum Optimization, Carlo A. Trugenberger, quant-ph/0107081

(平成 14 年 6 月 26 日受付)
(平成 14 年 7 月 3 日採録)

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 年電気通信大学電子情報学科助教授．現在に至る．理学博士．回路計算量理論，量子計算量理論，計算論的学習理論等の研究に従事．平成 7 年本学会 Best Author 賞，平成 10 年人工知能学会研究奨励賞各受賞．日本ソフトウェア科学会，人工知能学会，日本数学会，ACM，IEEE，EATCS 各会員．