電気通信大学紀要 16 巻 1 号 pp.23-29（2003）〔解説〕

量子計算と量子アルゴリズム

西　野　哲　朗

Quantum Computations and Quantum Algorithms

Tetsuro Nishino

Abstract

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 several major methods of designing efficient quantum algorithms with Shor's algorithm as an example. On the other hand, many researchers are studying how to physically implement quantum computers based on QTM. 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 factoring algorithm cannot be executed on an NMR quantum computer as it is. In this paper, we show how to factor integers in polynomial time by using NMR quantum computers.

Key words: quantum computation, NMR quantum computation, quantum algorithms, integer factoring

1　はじめに

現在インターネットで，公開鍵暗号系が広く利用されている。その代表的なものは，現在のコンピュータが 300 桁以上の整数の因数を現実的時間内には発見できないであろうという仮定に基づいて設計されている。

そもそも現在のコンピュータは，1936 年頃に英国の数学者 Alan Turing によって考案された Turing 機械という数学的モデルに基づいている。Turing 機械は，テープの 1 つの区画に 1 つの記号を保持することができる。

量子力学は原子的なスケールにおける現象を記述するが，そのスケールにおける物理現象は，日常我々が経験する物理現象とは本質的に異なっている。量子力学の対象となる物理系は，時には波動のように振舞い，また時に粒子のように振舞う。

この量子力学の概念をとり入れた計算モデルである，量子 Turing 機械を，1985 年に英国人の物理学者 David Deutsch が考案した[7]。量子 Turing 機械が通常の Turing 機械と異なる点は，テープの 1 つの区画に状態の理論上，任意の重ね合わせを保持できる点にある。つまり，量子 Turing 機械では単一のプロセッサ上で，理論上，任意の並列度の並列計算が行なえる。

量子Turing機械Mは，状態の有限集合Qとテープ記号の有限集合Γを用いて，状態遷移関数δにより定義される。例えば，量子Turing機械Mの状態遷移規則$\delta(p,a,b,q,d)=c$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，テープ上の現在ヘッドがある区画に記号bを書き込み，状態をqに遷移させ，ヘッドを方向$d\in\{L,R\}$に 1 区画動かす（Mのこの様相をc_2と呼ぶ）という事象の振幅がcであることをあらわしている（cは複素数）。このとき，Mが様相c_1からc_2に遷移する確率は，$|c|^2$となる。

通常のコンピュータのメモリの一区画には，0または1が保持できるが，QTMのメモリの一区画には，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，

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

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，$\alpha$と$\beta$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のテープの一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盛んに行われている。

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[26]。
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[12]。

以下では，Shorのアルゴリズムの動作を説明しながら，量子計算の基本原理 [3, 19, 20, 21, 22, 27] と，効率的量子アルゴリズムの設計法 [2, 23] について述べていく。

一方，量子計算機の実現に対する研究も現在盛んに行われており，イオントラップ，量子ドット，cavity QEDや，NMRを用いた方法などが提案されている。量子力学的状態が崩れる，デコヒーレンスという現象を考えた場合，NMRは緩和時間が長いため非常に有利であり，このため，量子計算機の実現を目指す研究者の間で広く注目を集めている[4, 5, 6, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 24, 25, 28]。例えば，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を用いた量子計算は通常の量子計算とは若干異なっている。このため，量子Turing機械上で動作するアルゴリズムでも，そのままでは，NMR装置上では正しく動作しないものが存在する。Shorの因数分解アルゴリズムもその1つである。そこで本論では，Shorの因数分解アルゴリズムをNMR量子コンピュータ上で正しく実行させるための，修正方法についても解説する。

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$\bmod n$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，常に自明な解$x=\pm 1 \bmod n$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，この他に非自明な解も存在する。もし，(1)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$\bmod n$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$|0\rangle$，...，$|q-1\rangle$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$|\mathrm{reg1}, \mathrm{reg2}\rangle$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。

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

   （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。

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

   （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。

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

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

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

   （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λ_1/r，λ_2/r，λ_3/r，...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がわかれば，nの因数は，$\gcd(x^{r/2}-1, n)$および，$\gcd(x^{r/2}+1, n)$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mod 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，等確率でひとつの値$kr+l$ $(0 \leq k \leq a)$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の値はわからない。

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$\lambda q/r$（$\lambda = 0, ..., r-1$）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　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盛んに行われており，量子ドット，イオントラップ，単一光子等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[5]。NMR法は，分子を構成する原子一つ一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なうことができる。

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 3.1 [22]　$EQP = EBQP$　□

誤り限定確率の計算とは，誤り確率がある正の定数$\varepsilon < \frac{1}{2}$で押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 3.2 [22]　$BQP = BBQP$　□

上の定理からもわかるように，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ことがわかる。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わかる。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わかっている。

4　BQTM上における因数分解アルゴリズム

Shorのアルゴリズムの観測においては，所望の値が複数存在し，それぞれ異なっているため，前節のアルゴリズムをそのままBQTM上で実行しても正しい値を読み出すことができない。また，BQTMの測定はアンサンブル平均を取ることに相当するため，測定の回数を増やしても，ほぼ同じ測定値が得られるだけで，アルゴリズムの成功確率を増幅することができない。そこで，以下のように，アルゴリズムを修正する必要がある[2]。なお，以下では一般性を失うことなく，奇数の合成数の因数分解のみを考える。

1. 入力Nに対して，滑らかな数qを１つ選び，Nと互いに素なx mod（$N-1$）をランダムに選んで，$|N, q, x, 0,\cdots,0\rangle$という状態の量子メモリ・レジスタから計算を始める（以下，レジスタは必要な個数だけ使用できるものとする）。ここで，x mod（$N-1$）と選ぶのは，論文[1]より，入力として奇数が与えられた場合，$x=N-1$を選ぶとNが素数と判定されてしまうためである。また，ラベルの右端の連続した０の個数をlとする。
2. $DFTq$をすべての０に順次適用する。その結果をa_i, $0\le i\le l-1$とする。この時点での重ね合わせ状態は以下のようになる。

$$\frac{1}{\sqrt{q^l}}\sum_{a_0=0}^{q-1}\cdots\sum_{a_{l-1}=0}^{q-1}|N, q, x, a_0, \ldots, a_{l-1}\rangle$$

3. 第（$l+4$）区画以降に$x^{a_i} \bmod N$を順次格納し，以下の重ねあわせを得る。

$$\frac{1}{q^l}\sum_{C=0}^{q-1}\sum_{A=0}^{q-1}\exp\left(2\pi i\sum_{j=0}^{l-1}(a_jc_j)/q\right)|N, q, x, C, M\rangle,$$

ただし，$C=c_0, \ldots, c_{l-1}, A=a_0, \ldots, a_{l-1}$,
$M=x^{a_0} \bmod N, \ldots, x^{a_{l-1}} \bmod N$。

4. C_i $/q$の連分数展開により得られた値r'_iを第（$2l+4$）区画以降に順次格納する。得られる重ね合わせ状態は以下のようになる。

$$\frac{1}{q^l}\sum_{C=0}^{q-1}\sum_{A=0}^{q-1}\exp\left(2\pi i\sum_{j=0}^{l-1}(a_jc_j)/q\right)|N, q, x, C, M, R'\rangle$$

ただし，$R'=r'_0, r'_1, \cdots, r'_{l-1}$。

5. 上式において，R'に含まれる値はほとんどが正しいオーダであり，その他の値は，その約数となることに注意する。r'_0に対して，以下のような$r'_0\neq\pm1 \bmod N$であるときは，第（$3l+4$）区画に０の列を書き込み，それ以外のときはr'_0を書き込む。（各区画は$O(\log n)$ビットを含むものとする。）すると，オーダの定義より，０の列もしくは，正しいオーダが第（$3l+4$）区画に書き込まれる。
次に，r'_1に対して，同様の判定を行ない，その結果を第（$3l+4$）区画の内容とビットごとにORを取る。そして，第（$3l+5$）区画にその結果を格納する。
以下同様に，r'_i（$2\le i\le l-1$）に対して，同様の判定を行ない，その結果と第（$3l+i+3$）区画の内容のORを取って，第（$3l+i+4$）区画にその結果を格納する。
r_{l-1}まで同様の処理が終了したならば，第（$4l+3$）区画を測定する。

次に，上記アルゴリズムの正当性と成功確率を考察する。まず，ステップ４のR'に含まれる整数rは正しいオーダ，もしくは，その約数であることをみる。説明を簡単にするために，いま，qがrで整除できるものとする。この場合，Shorの因数分解アルゴリズムの実行後に最終的に観測される値cは，$\lambda\frac{q}{r}$,（$\lambda=0, 1, \cdots, r-1$）と表される１つの値となる。つまり，

$$c=\lambda\frac{q}{r} \tag{1}$$

であり，q, cは既知の値，λ, rは未知の値である。式（1）を変形すると以下のようになる。

$$\frac{c}{q}=\frac{\lambda}{r} \tag{2}$$

したがって，λとrが互いに素であるようなcを観測できれば，c/qを既約分数にまで払うことにより，その分母から正しいオーダを得ることができる（実際，これは連分数展開の結果と等しい）。一方，λとrが互いに素でなければ，そのときは，c/qを既約分数にまで払うことによって，その分母から，正しいオーダの約数を得ることになる。したがって，rは正しいオーダ，もしくは，その約数となる。

最後に，本アルゴリズムの成功確率について考察する。本来のShorのアルゴリズムにおけるオーダrの，重ね合わせ状態内における占有率Pは$4/(\pi^2\log N)$と置くことができる。

（$4l+3$）区画でのrの占有率をP_lとすると，P_lは，

$$P_l=(1-P_{l-1})P+P_{l-1} \tag{3}$$

と表すことができる。この漸化式を解くと$P_l=1-(1-P)^l$となる。

$P_l>\frac{1}{2}$となるlを求めると，

$$\begin{aligned} 1-(1-P)^l &> \frac{1}{2} \\ \exp(-Pl) &< \frac{1}{2} \\ -Pl &< -\ln 2 \\ l &> \frac{\pi^2 \ln 2 \log N}{4} \end{aligned} \tag{4}$$

を得る。したがって，所望の結果は，$l=O(\log N)$個の連続した0を用いることにより，任意に高い確率で求めることができ，測定の精度に依存せずに所望の結果を得ることができる。

5　おわりに

本論では，まずNMR量子計算アルゴリズムの概念を紹介し，NMR量子コンピュータ上でも，整数の因数分解が多項式時間内に行えることを示した。現在，NMRを用いる方式が，量子コンピュータの実現方法として最も現実性があると考えられている。本論の結果は，NMR量子計算ばかりではなく，その他のBulk量子計算に対しても適用可能である。将来，本論の理論的結果を物理的に実現し，飛躍的に高速な量子コンピュータを実現するために，物理学者や電子工学者との活発な共同研究が必要となっていくであろう。

References

[1] 渥美賢嗣，西野哲朗：因数分解に対する量子アルゴリズムのシミュレーション，電子情報通信学会論文誌A，Vol.J81-A, No.12, pp.1670-1677（1998）.

[2] 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，Vol.43，No.SIG7(TOM6)，pp.10-18（2002）.

[3] Bernstein, E., and Vazirani, U. : "Quantum Complexity Theory", in *Proc. 25th Annual ACM Symposium on Theory of Computing*, ACM, New York, 1993, pp.11-20. Also in Special issue of *SIAM J. Comp.*, October, 1997.

[4] Brun, T., and Schack, R. : "Realizing the quantum baker's map on an NMR quantum computer", quant-ph/9807050, 1998.

[5] Chuang, I. L., Gershenfeld, N., Kubinec, M.G., and Leung, D.W. : "Buik Quantum Computation with Nuclear Magnetic Resonance : Theory and Experiment", *Proc. R. Soc. Lond.*, Vol. A 454, pp.447-467（1998）.

[6] Cory, D. G., Fahmy, A. F., and Havel, T. F. : "Ensemble Quantum Computing by Nuclear Magnetic Resonance Spectroscopy", *Proc. Natl. Acad. Sci.* 94, pp.1634-1639（1997）.

[7] Deutsch, D. : "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer", *Proc. R. Soc. Lond.*, Vol. A 400, pp.97-117（1985）.

[8] Dorai, K., Kumar, A., and Kumar A. : "Implementing quantum logic operations, pseudo-pure states and the Deutsch-Jozsa algorithm using non-commuting selective pulses in NMR", quant-ph/9906027, 1999.

[9] Fang, X., Zhu, X., Feng, M., Mao, X., and Du, F. : "Experimental Implementation of Dense Coding Using Nuclear Magnetic Resonance", quant-ph/9906041, 1999.

[10] Fu, L., Luo, J., Xiao, L., and Zeng, X. : "Experimental Realization of Discrete Fourier Transformation on NMR Quantum Computer", quant-ph/9905083, 1999.

[11] Gershenfeld, N., and Chuang, I. L. : "Bulk Spin-Resonance Quantum Computation", *Science*, Vol.275, pp.350-356（1997）.

[12] Grover, L. : "A Fast Quantum Mechanical Algorithm for Database Search", in *Proc. 28th Annual ACM Symposium on Theory of Computing*, ACM, New York, 1996, pp.212-219.

[13] Havel, T. F., Somaroo, S. S., Tseng C.-H., and Croy, D. G. : "Principles and Demonstrations of Quantum

Information Processing by NMR Spectroscopy", quant-ph/9812086, 1998.

[14] Jones, J. A., and Mosca, M. : "Approximate quantum counting on an NMR ensemble quantum computer", quant-ph/9808056, 1998.

[15] Jones, J. A., and Knill, E. "Efficient Refocussing of One Spin and Two Spin Interactions for NMR Quantum Computation", quant-ph/9905008, 1999.

[16] Linden, N., Barjat, H., and Freeman, R. : "An implementation of the Deutsch-Jozsa algorithm on a three-qubit NMR quantum computer", quant-ph/9808039, 1998.

[17] Luo, J., and Zeng, X. : "NMR Quantum Computation with a hyperpolarized nuclear spin bulk", quant-ph/9811044, 1998.

[18] Marx, R., Fahmy, A. F., Myers, J. M, Bermel, W., and Glaser, S. J. : "Realization of a 5-Bit NMR Quantum Computer Using a New Molecular Architecture", quant-ph/9905087, 1999.

[19] 西野哲朗：「量子コンピュータ入門」，東京電機大学出版局，1997.

[20] 西野哲朗：量子計算量理論，電子情報通信学会論文誌 D-I, Vol.J84-D-I, No.1, PP.3-17（2001）.

[21] 西野哲朗：「量子コンピュータの理論」，培風館，2002.

[22] Tetsuro Nishino : Mathematical Models of Quantum Computation, *New Generation Computing*, Vol.20（2002），pp.317-337.

[23] 西野哲朗：効率的量子アルゴリズムの設計手法，情報処理学会論文誌：数理モデル化と応用，Vol.43, No.SIG7(TOM6), pp.1-9（2002）.

[24] Pravia, M., Fortunato, E., Weinstein, Y., Price, M. D., Teklemariam, G., Nelson, R. J., Sharf, Y., Somaroo, S., Tseng, C. H., Havel, T. F., and Cory, D. G. : "Observations of Quantum Dynamics by Solution-State NMR Spectroscopy", quant-ph/9905061, 1999.

[25] Schulman, L. J., and Vazirani, U. : "Scalable NMR Quantum Computaion", quant-ph/9804060, 1998.

[26] Shor, P. W. : "Algorithms for Quantum Computation : Discrete Log and Factoring", *in Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp.124-134. Alsox in Special issue of *SIAM J. Comp.*, October, 1997.

[27] Simon, D. R. : "On the Power of Quantum Computation", *in Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp.116-123. Also in Special issue of *SIAM J. Comp.*, October, 1997.

[28] Wei, H., Xue, X., and Morgera, S. D. : "NMR Quantum Automata in Doped Crystals", quant-ph/9805059, 1998.