物理的実現可能性に優れたNMR量子探索アルゴリズム

大久保 誠也[†] 西野 哲朗[††]
太田 和夫[††] 國廣 昇[††]

本論では，測定誤差が $\varepsilon < 1$ である NMR（Nuclear Magnetic Resonance）量子計算機（NMRQC と略記）上で動作する，新しい量子探索アルゴリズムを提案する．具体的には，解が複数個存在する探索問題に対する，新しい NMR 量子探索アルゴリズムを提案する．探索問題の解空間のサイズを N とするとき，このアルゴリズムは，$\varepsilon N + \min\{n, \log \frac{1}{\varepsilon}\}$ 回のオラクル呼び出しを行うことにより，成功確率 1 で解を発見する．通常の量子計算機上で成功確率 1 で解探索を行うためには，N 回のオラクル呼び出しが必要であることが知られているので，提案アルゴリズムの方がより高速に動作する．そして，量子オラクルを作り替えることができるような問題に対しては，提案アルゴリズムの実行において必要となる量子ビット数を節約できることを示す．さらに，提案アルゴリズムは，量子重ね合わせ状態を維持しなければならない時間が短いので，物理的実現可能性が非常に高い．

A New Physically Realizable Quantum Search Algorithm

Seiya Okubo,[†] Tetsuro Nishino,[††] Kazuo Ota[††]
and Noboru Kunihiro[††]

In this paper, we propose a new quantum search algorithm on NMR (Nuclear Magnetic Resonance) quantum computers (NMRQCs for short) with the measurement accuracy $\varepsilon < 1$. That is, we propose a new NMR quantum search algorithm to solve search problems which have multiple solutions. Our algorithm can search one solution with certainty using $\varepsilon N + \min\{n, \log \frac{1}{\varepsilon}\}$ oracle calls, where N is the cardinality of the search space. Since, it is known that the ordinary quantum computer requires N oracle calls to solve the search problem with certainty, our NMR quantum search algorithm solves the problem more efficiently. Then, we show that our algorithm can be executed with small number of qubits for the problems where the quantum oracle can be reconstructed. Since, our algorithm requires short entanglement time, we can conclude that our algorithm is highly physically realizable.

1. まえがき

1985 年に Deutsch が，量子力学に基づく新たな計算モデルとして量子 Turing 機械を提案し，量子計算機のモデル化を行って以来，量子計算機実現に向けての研究が活発に行われてきた[1)~3)]．たとえば，1994 年に Shor は，量子 Turing 機械上で，整数の因数分解を多項式時間内に高い成功確率で行う量子アルゴリズムを示した[4)]．さらに，1996 年には Grover が，解探索問題に対する効率的量子アルゴリズムを提案した[5)]．

このような理論研究の流れを受けて，近年，NMR やイオントラップ，単一光子，量子ドットなどを用いて量子 Turing 機械を物理的に実現し，量子計算機を構築しようという研究がさかんに行われている．なかでも，NMR（Nuclear Magnetic Resonance，核磁気共鳴）を用いた量子計算は，近い将来に実現可能であると考えられている．NMR 法は，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が，NMR 装置を用いて行う **NMR 量子計算**は，通常の量子計算とは若干異なる枠組みであるため，NMR 量子計算の理論的基礎を与えるための研究も行われている[6)]．

近年，一部の研究者の間から，通常の量子回路に基づく量子計算機の実現可能性について様々な疑問が提示され始めている．たとえば，大きな整数の因数分解を行う際に，Shor の因数分解アルゴリズムで使用される量子重ね合わせ状態が，人工的には実現不可能であるとする主張や，実用的な量子計算機の実現可能性そのものに対する懐疑論が出始めている[7)]．これは，従

† 電気通信大学電気通信学研究科
Graduate School of Electro-Communications, The University of Electro-Communications
†† 電気通信大学情報通信工学科
Department of Information and Communication Engineering, The University of Electro-Communications

来，純粋な理論モデルに基づいてトップダウンに量子計算機を実現しようとしてきた研究の流れに対する警鐘であり，量子計算機実現のための数多くの物理実験が行われている現状においては，実現可能な量子計算機構という観点から，量子計算機をボトムアップに構築してゆく方向性の研究が重要であることを示唆している．

量子計算を実際に正しく行うためには，量子重ね合わせ状態と呼ばれる量子状態を一定時間維持しなければならないが，長時間にわたってその状態を維持することは技術的にきわめて困難であり，また，現状では物理的に実現可能な量子ビット数も非常に少ない．このため，物理的実現可能性が高く，実験などが行いやすい量子アルゴリズムが，実験家からは求められている．

一方，NMR 量子計算については，現在の液体分子を使う方式のほかに，固体 NMR を用いる方式なども検討され始めており，将来的には，現在よりもかなり高い能力を持った NMR 量子計算機が出現する可能性がある．このような状況下では，まずは，現状の NMR 量子計算機でどの程度有益な計算が行えるかを明らかにし，さらに，NMR 装置の測定精度などが改善された際に，その直接的波及効果として，どのような計算効率の向上がただちに期待できるのかということを，明らかにしておくことは大変重要である．

以上のようなことをふまえ，本論では，量子重ね合わせ状態が維持できる時間が短く，かつ，使用可能な量子ビット数が少ないという条件のもとで動作する NMR 量子探索アルゴリズムを提案する．本 NMR 量子探索アルゴリズムの利点は，以下のとおりである．

(1) 提案アルゴリズムは，確率 1 で所望の解を発見することができる．このことは，得られた解が正しいことを検算することが難しい，最小値探索問題などの解法において有効である．

(2) 通常の量子計算機上では，確率 1 で所望の解を発見するには，少なくとも N 回（N は重ね合わされた状態の個数）のオラクル呼び出しが必要であることが知られている．一方，本提案アルゴリズムでは，たかだか $\varepsilon N + \min\{n, \log \frac{1}{\varepsilon}\}$ $(0 < \varepsilon < 1)$ 回のオラクル呼び出しで解を発見することができる．

(3) 以下の理由により，本アルゴリズムは物理的実現可能性が高く，実験などにも利用しやすい．
   (a) 量子アルゴリズムを正しく動作させるために必要な，量子重ね合わせ状態を維持しておかなければならない時間が非常に短い．
   (b) ある種の探索問題においては，使用する量子ビット数を節約できる．

本論の具体的な構成は，以下のとおりである．まず，2 章で NMR 量子計算の数学的定義を述べる．そして，3 章で本論で提案する NMR 量子探索アルゴリズムのアイディアについて概観した後，4 章で提案アルゴリズムの詳細について述べる．続く 5 章と 6 章では，提案アルゴリズムの動作例を示した後に，アルゴリズムの正当性の証明と，計算量の評価を行う．さらに，7 章では，本アルゴリズムの使用者が量子オラクルを作り替えることができる問題では，使用する量子ビット数を削減できることを示す．最後に，8 章で結論を述べる．

なお，本提案アルゴリズムは，論文 8) のアルゴリズムを簡略化し，その物理的実現可能性を飛躍的に高めたものとなっている．

2. 量 子 計 算

1985 年に，英国人物理学者 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[9),10)]．この QTM に基づく計算機が，**量子計算機**と呼ばれている．

通常の計算機のメモリの 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，

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

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にする．

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[11]．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．本論では，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．

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測定すると，確率 1 で，$|\beta|^2 - |\alpha|^2$ という実数値が測定できるものと仮定される．ただし，その際の測定誤差を $\varepsilon = 1/2^k$ とすると，重ね合わせ状態 $\alpha\,|0\rangle + \beta\,|1\rangle$ にある量子ビットを測定すると，実際には，以下の関係式を満たす実数値 θ が確率 1 で読み出せるものとする．

$$|\beta|^2 - |\alpha|^2 - \varepsilon < \theta < |\beta|^2 - |\alpha|^2 + \varepsilon$$

また，NMR における測定では，波束が収縮しないので，重ね合わせ状態を乱さずに測定を行うことができる．なお，現在の NMR 装置においては，測定精度は通常 2 進数 5 桁（測定誤差としては $\varepsilon = \frac{1}{2^5}$）程度である．

3. 提案アルゴリズムのアイディア

いま，$0 \le y \le 2^n - 1$ なる整数 y 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．この定義域のなかに，特別な整数 y_0 が存在して，$x = y_0$ 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 $\alpha_1\,|x_1, 0\rangle + \alpha_2\,|x_2, 0\rangle + \cdots + \alpha_n\,|x_n, 0\rangle$ 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 $\alpha_1\,|x_1, f(x_1)\rangle + \alpha_2\,|x_2, f(x_2)\rangle + \cdots + \alpha_n\,|x_n, f(x_n)\rangle$ を返すブラックボックスのことをいう．ここで，任意の入力に対し，量子オラクルは単位時間で出力を返すものとする．本論では，量子アルゴリズムの計算量を，オラクル呼び出しの回数（**質問量**と呼ぶ）によって評価するものとする．

本論で取り扱う**探索問題**とは，以下のような問題である．

> **入力：**入力に含まれる重ね合わせの個数 N．
> **問題：**n 変数ブール関数 f に対する量子オラクルが与えられたときに，上記の条件を満たす y_0 を発見せよ．

探索問題に対しては，量子計算・古典計算を問わず，様々な研究がなされている．文献 5) では，通常の量子計算機上で動作し，$O(\sqrt{N})$ 回のオラクル呼び出しによって高い確率で解を発見する Grover のアルゴリズムが提案されている（ここで，$N = 2^n$ とする）．このアルゴリズムは，Grover 変換と呼ばれる変換を繰り返すことにより，成功確率を 1 に近づけることができるが，$O(\sqrt{N})$ 回のオラクル呼び出しでは，成功確率を 1 にすることはできない．また，測定の規約の違いにより，そのままでは NMR 量子計算機上では動作しない．さらに，その実行においては，$O(\sqrt{N})$ 回の Grover 変換が行えるだけの時間，量子重ね合わせ状態を維持することが必要となる．

一方，文献 12) では，$O(\sqrt{N})$ 回の Grover 変換で確率 1 で正解を出力する NMR 量子計算アルゴリズムが提案されている．しかしながら，このアルゴリズムでは量子重ね合わせ状態を，$\frac{1}{2}\sqrt{\varepsilon N}$ 回の Grover 変換が行えるだけの時間，維持することが必要となる．現在のところ，量子計算機が物理的に実現できたとしても量子重ね合わせ状態を維持できる時間には厳しい制約があると予想されるため，$\frac{1}{2}\sqrt{\varepsilon N}$ 回の Grover 変換は行うことは非常に困難であると考えられる．

また，文献 8) では，Grover 変換を用いずに NMR 量子計算機上で探索を行うアルゴリズムが提案されている．しかし，このアルゴリズムは，Grover 変換は使用していないものの，必要な量子重ね合わせ状態の維持時間は $O(\sqrt{N})$ 回の関数の評価を行うだけの時間となり，アルゴリズム全体で必要となる関数の評価回数も観測誤差が $\varepsilon = 1/\sqrt{N}$ のときに $\sqrt{N}$ 回となる．しかも，成功確率は 1 ではない．

最後に，古典計算機を用いて定義域を古典的に探索した場合には，y_0 を発見するまでの $f(x)$ の評価回数（オラクル呼び出しの回数）の期待値は 2^{n-1} と

なる．この場合，与えられた関数の性質などを用いることにより，より高速に解を発見することができる可能性もあるが，本論におけるように，関数がオラクルというブラックボックスとして与えられているという仮定のもとでは，個別の関数の解析を行うことはできない．

次に，提案アルゴリズムの基本となるアイディアについて説明する．提案アルゴリズムでは，量子オラクルとして与えられたブール関数の充足可能性判定問題に対する，NMR 量子計算アルゴリズムをサブルーチンとして利用する．そこで，最初に充足可能性判定問題と，充足可能性判定問題に対する NMR 量子計算アルゴリズムについて説明する．

充足可能性判定問題（satisfiability problem，SAT）とは，以下のような問題である．

入力：入力に含まれる重ね合わせの個数 N．

問題：n 変数ブール関数 f に対する量子オラクルが与えられたときに，$f(x_1, x_2, \ldots, x_n) = 1$ を満足する $(a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ が存在するか否かを判定せよ．

ここで，$\{0,1\}^n$ 中に $f(x) = 1$ を満たす充足解は全部で t 個存在するものとし，この t の値は未知であるとする．また，任意の状態 x に対し $f(x) = 1$ であるか否かは単位時間で判定できるものとする．

以下の NMR 量子計算アルゴリズムを使用して，上記の充足可能性判定問題を解くことができる．

ステップ 1：以下のような等振幅の重ね合わせ状態を生成する．$n+1$ 番目の量子ビットは 0 に設定する．ただし，$N = 2^n$ とする．

$$\sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} |x\rangle |0\rangle$$

ステップ 2：$f(x)$ の値を計算し，$n+1$ 番目の量子ビットに書き込む．

ステップ 3：$n+1$ 番目の量子ビットを測定する．

もし，$f(x) = 1$ を満たす x がただ 1 つしか存在しないならば，ステップ 3 で得られる測定値 $|\beta|^2 - |\alpha|^2$ の値は

$$\frac{1}{N} - \frac{N-1}{N} = \frac{2-N}{N} \qquad (1)$$

である．解が 1 つ以上存在するならば，式 (1) 以上の値となる．また，充足解が存在しないならば，$|\beta|^2 - |\alpha|^2$ の値は -1 である．N の値が大きいとき，つまり重ね合わされている状態の個数が多いときは，**図 1** の状況 0 のようになり，測定誤差の影響で，充足解が存在する場合と存在しない場合の区別をすることができない．逆に，N の値が小さくなればなるほど，充足解が存在する場合と存在しない場合の $|\beta|^2 - |\alpha|^2$ の値の差は大きくなってゆく（図 1 の状況 1 参照）．そして，$|\beta|^2 - |\alpha|^2$ の値の差が 2ε 以上ならば，充足解が存在するか否かを正確に判定することができる（図 1 の状況 2 参照）．つまり，

$$\frac{2-N}{N} \geq -1 + 2\varepsilon$$

$$\frac{1}{\varepsilon} \geq N$$

が満たされているならば，充足解の有無を判定することができる．すなわち，測定値が $-1+\varepsilon$ 以上ならば充足解が存在し，$-1+\varepsilon$ よりも小さければ充足解は存在しないと判定できる．

以上のことにより，重ね合わされた状態の個数 N が $\frac{1}{\varepsilon} = 2^k$ 以下ならば，オラクル呼び出しを 1 回行うだけで充足可能性判定問題を確率 1 で解くことができることが分かった．そこで，探索空間 $\{0,1\}^n$ を，オラクル呼び出し 1 回で充足可能性判定問題を解くことができるサイズの部分集合 $\{0,1\}^k$ に分割した後，充足可能性判定問題に対する，上述の NMR 量子計算ア

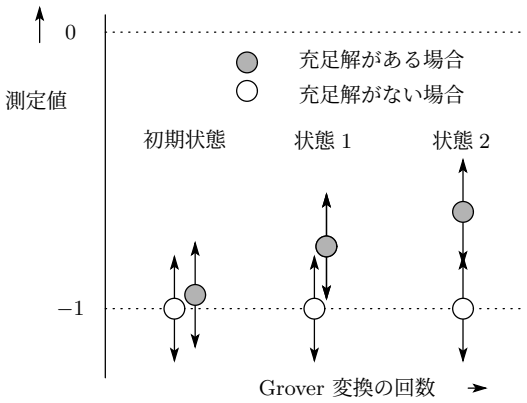

図 1 提案アルゴリズムの実行
Fig. 1 The execution of the proposed algorithm.

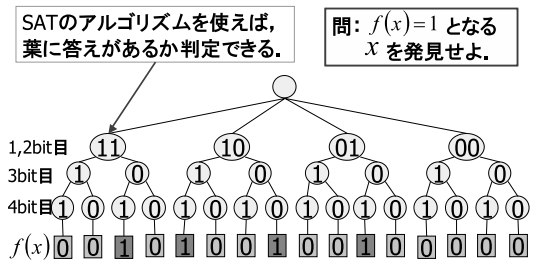

図 2 アルゴリズムの実行（その 2）
Fig. 2 The execution of the proposed algorithm (cont.).

ルゴリズムを用いることによって，それぞれの部分集合に充足解が存在するか否かを判定して上位ビットを決定する．次に，上述の NMR 量子計算アルゴリズムを再びサブルーチンとして用い，下位ビットを 2 分探索を行う．このようにして，関数 f に対する充足解を探索することができる（**図 2** 参照）．

4. アルゴリズムの詳細

以下では，0 と 1 からなる記号列を 2 進数と同一視して取り扱う．要素数が $N = 2^n$ である解の候補集合を X，解の候補の下位 k ビットからなる集合 $\{0,1\}^k$ を X_L（ここで，k は NMRQC の測定誤差 $\varepsilon = 1/2^k$ から定まる定数），解の候補の上位 $n-k$ ビットからなる集合 $\{0,1\}^{n-k}$ を X_H で表し，ある解の候補 $x \in X$ の上位ビットを $x_H \in X_H$，下位ビットを $x_L \in X_L$ と表記する．

本論で提案する NMR 量子探索アルゴリズムは，上位ビットを決定するフェーズと下位ビットを決定するフェーズに分かれている．

上位ビットの決定フェーズ　上位ビットの決定フェーズは，以下のステップ 1〜5 からなる．

ステップ 1：$x_H := 1^{n-k} \in \{0,1\}^{n-k} = X_H$ とする．

ステップ 2：量子メモリを初期化した後，以下のような重ね合わせ状態を Walsh-Hadamard 変換 $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ を用いて生成する．特に，$n+1$ 番目の量子ビットの値は 0 に設定する．

$$\sum_{x_L \in X_L} \frac{1}{\sqrt{2^k}} |x_H \circ x_L\rangle |0\rangle$$

ここで，記号 $\circ$ は，文字列の連接を表す．

ステップ 3：オラクル呼び出しにより $f(x_H \circ x_L)$ の値を得て，$n+1$ 番目の量子ビットに書き込む．すると，以下の重ね合わせ状態を得る．

$$\sum_{x_L \in X_L} \frac{1}{\sqrt{2^k}} |x_H \circ x_L\rangle |f(x_H \circ x_L)\rangle$$

ステップ 4：$n+1$ 番目の量子ビットを測定する．測定された値が $-1+\varepsilon$ 以上ならば，下位決定フェーズのステップ 6 に進む．さもなければ，ステップ 5 に進む．

ステップ 5：$x_H = 0^{n-k}$ ならば，充足解は存在しないと出力して停止する．さもなければ，$n+1$ 番目の量子ビットの値を 0 に戻し，$x_H := x_H - 1$ としてから，ステップ 2 へ戻る（ここで，$x_H := x_H - 1$ は，0 と 1 からなる記号列を 2 進数と同一視して，計算を行うことを意味している）．

下位ビットの決定フェーズ　下位ビットの決定フェーズは，以下のステップ 6〜10 からなる．

ステップ 6：$z_H := x_H$，$i := 1$ とする．

ステップ 7：以下のような重ね合わせ状態を Walsh-Hadamard 変換を用いて生成する．

$$\sum_{z_L \in \{0,1\}^{k-i}} \frac{1}{\sqrt{2^{k-i}}} |z_H \circ 1 \circ z_L\rangle |0\rangle$$

ステップ 8：オラクル呼び出しにより $f(z_H \circ 1 \circ z_L)$ の値を得て，$n+1$ 番目の量子ビットに書き込み，その量子ビットを測定する．

ステップ 9：測定値が $-1+\varepsilon$ よりも大きければ，$z_H := z_H \circ 1$ とする．さもなければ，$z_H := z_H \circ 0$ とする．

ステップ 10：$i = k$ ならば，充足解として z_H を返して終了する．$i < k$ ならば，$i := i+1$ としてステップ 7 に戻る．

本アルゴリズムでは，Grover のアルゴリズムで用いられる拡散変換などは利用しておらず，必要となるユニタリ変換は単純なもののみである．また，本アルゴリズムの実行においては，ステップ 3 やステップ 7 で NMR 装置を再起動して用いている．したがって，ステップ 3 から 5 の間，および，ステップ 7 から 9 の間だけ，NMR 装置内において量子重ね合わせ状態が保持されていればよい．

5. アルゴリズムの動作例

本章では，前章で示した NMR 量子探索アルゴリズムの動作例を示す．ただし，解の候補 x は 4 ビットで表現されるものとし，NMR 量子計算機の測定誤差 ε は $\frac{1}{4}$ であるとする．また，$f(x) = 1 \iff x = 1010$ であるものとする．

(1)　$n = 4$，$\varepsilon = \frac{1}{4}$ であるので，上位ビットの空間 X_H を $\{0,1\}^2$ とし，x_H の値として 11 を選択する（アルゴリズムのステップ 1 参照）．

(2)　以下のような重ね合わせ状態を生成する（ステップ 2 参照）．

$$\frac{1}{\sqrt{2^2}} \{|11 \circ 00\rangle |0\rangle + |11 \circ 01\rangle |0\rangle + |11 \circ 10\rangle |0\rangle + |11 \circ 11\rangle |0\rangle\}$$

(3) オラクル呼び出しにより $f(x)$ の値を得て，その値を 5 番目の量子ビットに書き込む（ステップ 3 参照）．以下の重ね合わせ状態が得られる．

$$\frac{1}{\sqrt{2^2}}\{|11\circ 00\rangle|0\rangle+|11\circ 01\rangle|0\rangle +|11\circ 10\rangle|0\rangle+|11\circ 11\rangle|0\rangle\}$$

(4) 5 番目の量子ビットを測定すると，測定値として開区間 $(-1-\varepsilon,-1+\varepsilon)$ 内のある値が得られる（ステップ 4 参照）．その値は $-1+\varepsilon$ より小さく，かつ $x^H=11\neq 00$ であるので，$x_H:=10$ とし，5 番目の量子ビットの値を 0 に戻す（ステップ 5 参照）．重ね合わせ状態は以下のようになる．

$$\frac{1}{\sqrt{2^2}}\{|10\circ 00\rangle|0\rangle+|10\circ 01\rangle|0\rangle +|10\circ 10\rangle|0\rangle+|10\circ 11\rangle|0\rangle\}$$

(5) オラクル呼び出しにより $f(x)$ の値を得て，その値を 5 番目の量子ビットに書き込む（ステップ 3 参照）．以下の重ね合わせ状態が得られる．

$$\frac{1}{\sqrt{2^2}}\{|10\circ 00\rangle|0\rangle+|10\circ 01\rangle|0\rangle +|10\circ 10\rangle|1\rangle+|10\circ 11\rangle|0\rangle\}$$

(6) 5 番目の量子ビットを測定すると，測定値として開区間 $(-\frac{1}{2}-\varepsilon,-\frac{1}{2}+\varepsilon)$ 内のある値が得られる（ステップ 4 参照）．その値は $-1+\varepsilon$ 以上の値であるので，上位 2 ビットが 10 であるような解が存在する．

(7) 以下のような重ね合わせ状態を生成する（ステップ 6，7 参照）．

$$\frac{1}{\sqrt{2}}\{|10\circ 1\circ 0\rangle|0\rangle+|10\circ 1\circ 1\rangle|0\rangle$$

(8) オラクル呼び出しにより $f(x)$ の値を得て，その値を 5 番目の量子ビットに書き込む（ステップ 8 参照）．以下の重ね合わせ状態が得られる．

$$\frac{1}{\sqrt{2}}\{|10\circ 1\circ 0\rangle|1\rangle+|10\circ 1\circ 1\rangle|0\rangle$$

(9) 5 番目の量子ビットを測定すると，測定値として開区間 $(0-\varepsilon,0+\varepsilon)$ 内のある値が得られる（ステップ 4 参照）．その値は $-1+\varepsilon$ 以上の値であるので，上位 3 ビットが 101 であるような解が存在する（ステップ 9，10 参照）．

(10) 以下のような重ね合わせ状態を生成する（ステップ 7 参照）．

$$\frac{1}{\sqrt{2^0}}\{|101\circ 1\rangle|0\rangle\}$$

(11) オラクル呼び出しにより $f(x)$ の値を得て，その値を 5 番目の量子ビットに書き込む（ステップ 8 参照）．以下の重ね合わせ状態が得られる．

$$\frac{1}{\sqrt{2^0}}\{|101\circ 1\rangle|0\rangle\}$$

(12) 5 番目の量子ビットを測定すると，測定値として開区間 $(-1-\varepsilon,-1+\varepsilon)$ 内のある値が得られる（ステップ 4 参照）．その値は $-1+\varepsilon$ より小さい値であるので，上位 4 ビットが 1011 であるような解は存在しない．したがって，上位 4 ビットは 1010 である（ステップ 9 参照）．

(13) すべてのビットの値が確定したので，充足解 1010 を出力して，停止する（ステップ 10 参照）．

以上により，解の候補集合 $X=\{0,1\}^4$ の中から，$f(x)$ の充足解 1010 を発見することができた．

6. アルゴリズムの正当性と計算量

4 章で示したアルゴリズム中，ステップ 1〜5 までは充足解の上位ビットの決定に，ステップ 6〜10 までは充足解の下位ビットの決定に，それぞれ相当する．

最初に，ステップ 1〜5 で充足解の上位ビットが正しく決定できることを示す．集合 $X_L=\{0,1\}^k$ であるので，ステップ 2 で重ね合わされている状態の個数は 2^k である．もし，この重ね合わせ中に充足解が存在するのならば，$|\beta|^2-|\alpha|^2\geq -1+2\varepsilon$ となる．この状態を測定した場合，その測定値は $-1+\varepsilon$ より大きい値となり，充足解が重ね合わせ中に存在することを，測定により正しく判定することができる．逆に，存在しないならば，$|\beta|^2-|\alpha|^2=-1$ となる．この状態を測定した場合，その測定値は $-1+\varepsilon$ より小さい値となり，充足解が存在しないことを正しく判定することができる．したがって，上位ビットが x_H であるような充足解が存在するか否かを正しく判定することができる．また，ステップ 1〜5 では X_H 内を全探索しているので，もし解の候補集合 X 内に充足解が存在するならば，必ず，ある解 x の上位ビット x_H を発見することができる．

次に，ステップ 6〜10 で解の下位ビットが正しく決定できることを示す．いま，上位 $n-k+i$ ビットが z_H であるような充足解が存在すると仮定する．この場合，$z_H\circ 1$ もしくは $z_H\circ 0$ を上位 $n-k+i+1$ ビットとするような充足解が存在する．ステップ 7 で生成された状態内で，重ね合わされた状態の個数は 2^{k-i} 個であるため，オラクル呼び出しを 1 回行うことで，重ね合わせ状態内に充足解が含まれているか否かを判定することができる．つまり，$z_H\circ 1$ を上位 $n-k+i+1$

ビットとするような充足解が存在するか否かを判定することができる．もし，このような充足解が存在しないと判定されたら，$z_H \circ 0$ を上位 $n-k+i+1$ ビットとするような充足解が存在することになる．したがって，ステップ 7〜9 を実行することによって，ある充足解の i 番目の量子ビットの値を決定することができる．したがって，ステップ 7〜9 を k 回繰り返すことにより，下位 k ビットの値を正確に決定することができる．

以下では，提案アルゴリズムの実行に必要なオラクル呼び出しの回数（質問量）を評価する．

最初に，ステップ 1〜5 で上位ビットを決定するのに必要なオラクル呼び出しの回数を評価する．x_H の値を 1^{n-k} から 0^{n-k} まで変化させることで，$f(x)=1$ を満たす x の上位ビットを決定することができる．また，各 x_H に対して，1 回のオラクル呼び出しが行われる．したがって，ステップ 1〜5 の実行においては，たかだか $2^{n-k} = \varepsilon N$ 回のオラクル呼び出しが行われる．

次に，ステップ 6〜10 で充足解の下位 k ビットを決定するのに必要なオラクル呼び出しの回数を評価する．ステップ 7〜9 を実行することにより，充足解の値を 1 ビットずつ決定することができる．1 ビットの決定に，オラクル呼び出しを 1 回行う必要があるので，下位 k ビットをすべて決定するには，$k = \min\{n, \log \frac{1}{\varepsilon}\}$ 回のオラクル呼び出しを行う必要がある．

よって，全体では，たかだか $\varepsilon N + \min\{n, \log \frac{1}{\varepsilon}\}$ 回のオラクル呼び出しを行うことで，確率 1 で充足解を発見することができる．このことは，発見した解が正しいことを検算することが難しい，最小値探索のような問題に対し，成功確率 1 を保証したい場合などに有用である．ここで最小値探索問題とは，オラクル $g : \{0,1\}^n \to \{0,1\}^m$ が与えられたとき，$g(x)$ を最小とする x を発見する問題である．

提案アルゴリズムと既存のアルゴリズムの計算量の比較を行う．通常の量子計算に関しては，以下の定理が示されている[13]．

> 誤りなしで N 項目データベースの検索を行う量子アルゴリズムは，N 回のオラクル呼び出しを必要とする．

したがって，解の探索空間が 32 ビットである場合，少なくとも $2^{32} = 4{,}294{,}967{,}296$ 回のオラクル呼び出しを必要とする．一方，提案アルゴリズムを NMR 量子計算機上で動作させた場合，およそ，その ε 倍程度のオラクル呼び出しで解を発見することができる．NMR 装置の測定誤差が $\frac{1}{2^7} \le \varepsilon \le 1$ の場合における，必要なオラクル呼び出しの回数を**表 1** に示す．$\varepsilon = \frac{1}{128}$ の測定誤差を持つ NMR 量子計算機を用いれば，通常の量子計算機上で探索を行う場合に比べ 0.8% 程度のオラクル呼び出しを用いればよいことが分かる．しかしながら，ε は NMR 量子計算機の物理的実装によって決まってくる定数であるため，提案アルゴリズムを使用しても必要なオラクル呼び出しの回数はやはり $O(N)$ である．

表 1 32 ビット長の探索空間において必要なオラクル呼び出し回数
Table 1 The number of the oracle calls when the search space is corresponding to 32 bit long.

	測定誤差	オラクル呼び出しの回数	比
QC		4,294,967,296	100%
NMR QC	$\varepsilon = 1$	4,294,967,296	100%
	$\varepsilon = 1/2$	2,147,483,649	50%
	$\varepsilon = 1/4$	1,073,741,826	25%
	$\varepsilon = 1/8$	536,870,915	12.5%
	$\varepsilon = 1/16$	268,435,460	6.25%
	$\varepsilon = 1/32$	134,217,733	3.125%
	$\varepsilon = 1/64$	67,108,870	1.5625%
	$\varepsilon = 1/128$	33,554,439	0.78125%

7. 量子ビット数の節約

本章では，NMR 量子計算機の量子メモリが十分に確保できない場合の，提案アルゴリズムの実行についての考察を行う．ここで，探索空間を表すのに必要なビット数を n，利用可能な NMR 量子計算機の量子ビット数を l，NMR 量子計算機の測定誤差を $\varepsilon = \frac{1}{2^k}$ で表すものとする．

提案アルゴリズムでは，ステップ 3 でオラクル呼び出しを行う際の重ね合わせ状態内で，異なった値を保持している量子ビットは第 $n-k+1$ ビット目から n ビット目までの k ビットのみであり，それ以外の量子ビットはアルゴリズム中のステップ 1 もしくは 4 で設定された値 x_H を保持している．この値 x_H をステップ 3 で用いるオラクル内に組み込むことことができれば，x_H を表す $n-k$ 量子ビット分を節約できる．一方，この方法を利用するためには，x_H の値を変更するたびに，オラクル呼び出しに相当する量子回路を作成し直さなけらばならない．したがって，この方法を使うには，オラクルの中身が分かっている必要がある．このように，オラクルの内部構成が明らかとなるような事例としては，公開されている暗号化関数をオラクルとして用いて，暗号解読を行う場合などが考えられる．

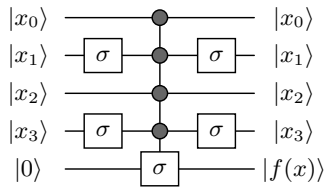

図 3 オラクルを実現する量子回路
Fig. 3 The quantum circuit realizing an oracle.

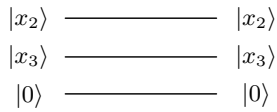

図 4 5 章 (3) で用いられる量子回路
Fig. 4 The quantum circuit used in section 5 (3).

簡単な例を示す．5 章で使用した，$f(x) = 1$ を満たす $x = 1010$ を発見する際に，オラクルとして用いた量子回路について考える．使用する NMR 量子計算機で利用可能な量子ビットが 3 ビット，測定誤差が $\varepsilon = \frac{1}{2^2}$ であるとする．つまり $n = 4$，$l = 3$，$k = 2$ と仮定する．また，関数 $f : \{0,1\}^4 \mapsto \{0,1\}$ は，実際には $f(x) = x_0 \wedge \bar{x}_1 \wedge x_2 \wedge \bar{x}_3$ であり，その量子回路は**図 3** のような回路であったとする．この図では量子ビットを 5 ビット使用していることに注意する．5 章の (3) において，上位 2 ビットは 11 に固定されていた．したがって，この場合，関数 $f(x)$ は

$$\begin{aligned} f(x) &= x_0 \wedge \bar{x}_1 \wedge x_2 \wedge \bar{x}_3 \\ &= 1 \wedge \bar{1} \wedge x_2 \wedge \bar{x}_3 \\ &= 1 \wedge 0 \wedge x_2 \wedge \bar{x}_3 \\ &= 0 \end{aligned}$$

と簡略化できる．この式に対応する量子回路を**図 4** に示す．同様に，5 章 (6) においては，上位 2 ビットは 10 に固定されているため，

$$\begin{aligned} f(x) &= x_0 \wedge \bar{x}_1 \wedge x_2 \wedge \bar{x}_3 \\ &= 1 \wedge \bar{0} \wedge x_2 \wedge \bar{x}_3 \\ &= x_2 \wedge \bar{x}_3 \end{aligned}$$

と簡略化できる．この式に対応する量子回路を**図 5** に示す．図 3 の量子回路をオラクルとして用いる代わりに，(3) で図 4 の量子回路を，(6) で図 5 の量子回路を用いることでも，同様の結果を得ることができる．図 4，5 では，固定された値 x_H が回路内に組み込み済みであるため，3 量子ビットしか使用していないことに注意する．この例では，$n - k = 2$ 量子ビットを削減することに成功している．

本章では，提案アルゴリズムを用いて量子ビットを節約する方法について述べたが，この方法を用いるには，オラクルとして利用する量子回路を効率的に再構成する必要がある．しかし，通常の回路の場合と異なり，NMR 量子計算においては，各計算ステップに対応するユニタリ変換は何らかの磁場をかけることによって実現される．したがって，NMR 量子計算機において，提案アルゴリズムを用いて量子ビットを節約するには，この磁場のかけかたを適切に変化させることが必要となる．

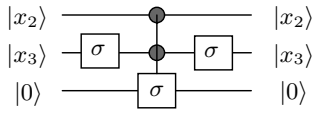

図 5 5 章 (6) で用いられる量子回路
Fig. 5 The quantum circuit used in section 5 (6).

8. おわりに

NMR 量子計算機上で動作する新たな量子探索アルゴリズムを提案し，$\varepsilon N + \min\{n, \log \frac{1}{\varepsilon}\}$ 回のオラクル呼び出しによって確率 1 で解を発見できることを示した．解の個数の情報が何も与えられていない場合，通常の量子計算機を用いて確率 1 で解を探索すると，N 回以上のオラクル呼び出しが必要であることが示されている．したがって，この場合には，本提案アルゴリズムは，通常の量子探索アルゴリズムよりも定数倍高速に動作する．

この場合，量子計算機のクロックが古典計算機のクロックの ε 倍よりも速ければ，本提案アルゴリズムの方が高速になる．このように，NMR 装置の測定誤差 ε の改善が，計算の効率化と密接に関係していることが明らかとなった．

さらに，提案アルゴリズムを使用すると，必要な量子ビット数を節約できることも示した．また，量子計算機を動作させる場合，量子重ね合わせ状態を維持できる時間が本質的に重要である．たとえば，通常の量子計算機上で Grover のアルゴリズムを，NMR 量子計算機上で文献 12) のアルゴリズムを，それぞれ動作させるには，少なくとも $O(\sqrt{N})$ 回のオラクル呼び出しを実行する間，量子重ね合わせ状態を維持する必要がある（ただし，通常の量子探索アルゴリズムの場合，このときの成功確率は 1 ではないことに注意する）．提案アルゴリズムは充足解を発見するのに $\varepsilon N + \min\{n, \log \frac{1}{\varepsilon}\}$ のオラクル呼び出しが必要であるが，その実行に際しては，オラクル呼び出しを 1 回行うのに必要な時間だけ，量子重ね合わせ状態を保持することができればよい．その意味で，本提案アルゴリズムは，文献 12) のアルゴリズムよりも多くの計算量を必要とするが，物理的実現性に優れている．

謝辞 本論に対して貴重なコメントをくださった，担当委員と査読者の方々に深謝いたします．

参 考 文 献

1) Tanaka, K.: Quantum Bit-Commitment for Small Storage Based on Quantum One-Way Permutations, *New Generation Computing*, pp.339–346 (2003).
2) Iwama, K. and Yamashita, S.: Transformation Ruless for CNOT-based Quantum Circuits and Their Applications, *New Generation Computing*, pp.297–318 (2003).
3) Mihara, T.: On the complexity of finding cycles in periodic functions using the quantum Turing machine, *IEICE Trans. Information and Systems*, Vol.E79-D, pp.579–583 (1996).
4) Shor, P.W.: Algorithms for Quantum Computation: Discrete Log and Factoring, *Proc. 35th Anniual IEEE Symposium on Foundations of Computer Science* (1994).
5) Grover, L.K.: Quantum Mechanics Helps in Searching for a Needle in a Haystack, *Physical Review Letters*, Vol.79, No.2, pp.325–328 (1997).
6) Nishino, T.: Mathematical Models of Quantum Computation, *New Generation Computing*, Vol.20, pp.1–9 (2002).
7) Aaronson, S.: Multilinear Formulas and Skepticism of Quantum Computing, *to appear in SIAM Journal of Computing. Also in STOC 2004, 118-127. Conference version* (2004).
8) Ohta, K., Nishino, T., Okubo, S. and Kunihiro, N.: A Quantum Algorithm using NMR Computers to Break Secret-Key Cryptosystems, *New Generation Computing*, pp.347–361 (2003).
9) Bernstein, E. and Vazirani, U.: Quantum Complexity Theory, *Proc. 25th ACM Symposium on Theory of Computing*, pp.11–20 (1993).
10) Deutsch, D.: Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proc. R. Soc. Lond.*, Vol.A 400, pp.97–117 (1985).
11) Chuang, I.L., Gershenfeld, N., Kubinec, M. and Leung, D.: Bulk Quantum Computation with Nuclear Magnetic Resonance : Theory and Experiment, *Proc. R. Soc. Lond.*, Vol.A 454, pp.447–467 (1998).
12) 大久保誠也，西野哲朗，太田和夫：NMR 量子計算機を用いた探索アルゴリズムについて，信学技報，COMP2002-82，pp.55–59 (2003).
13) Beals, R., Buhrman, H., Cleve, R., Mosca, M. and de Wolf, R.: Quantum Lower Bounds by Polynomials, *IEEE Symposium on Foundations of Computer Science*, pp.352–361 (1998).

(平成 16 年 6 月 22 日受付)
(平成 17 年 4 月 1 日採録)

大久保誠也（学生会員）

昭和 52 年生．平成 12 年電気通信大学電気通信学部卒業．平成 14 年電気通信大学電気通信学研究科修了．現在，電気通信大学大学院博士後期課程在学中．量子計算と暗号の研究に従事．

西野 哲朗（正会員）

昭和 34 生．昭和 57 年早稲田大学理工学部数学科卒業．昭和 59 年早稲田大学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．現在に至る．理学博士．平成 8 年情報処理学会 Best Author 賞，平成 10 年人工知能学会研究奨励賞，平成 14 年電子情報通信学会ソサイエティ論文賞各受賞．量子計算量理論，回路計算量理論，計算論的学習理論等の研究に従事．電子情報通信学会，人工知能学会，日本ソフトウェア科学会，日本数学会，ACM，IEEE，EATCS 各会員．

太田 和夫（正会員）

昭和 52 年早稲田大学理工学部数学科卒業．昭和 54 年早稲田大学大学院修士課程修了．平成 2 年理学博士．昭和 54〜平成 13 年日本電信電話（NTT）研究所に勤務．平成 13 年〜現在，電気通信大学教授．専門は情報セキュリティ，特に暗号理論．電子情報通信学会，IACR，IEEE 各会員．編著書に，『情報セキュリティの科学』（講談社ブルーバックス），『暗号・ゼロ知識証明点・数論』（共立出版），『ほんとうに安全？ 現代の暗号』（岩波科学ライブラリー）等．翻訳書に，『暗号理論』（岩波，1 冊でわかるシリーズ），『計算理論の基礎』（共立出版）．

國廣　昇

昭和 46 年生．平成 8 年東京大学大学院工学系研究科計数工学専攻修士課程修了．同年日本電信電話（株）入社．平成 8 年より平成 14 年まで，NTT コミュニケーション科学基礎研究所に勤務．平成 14 年より電気通信大学講師．情報セキュリティ，暗号理論，量子計算の研究に従事．著書に,『ほんとうに安全？　現代の暗号』（岩波科学ライブラリー）等．翻訳書に,『暗号理論』（岩波，1 冊でわかるシリーズ）．博士（工学）．平成 9 年「SCIS 論文賞」受賞．電子情報通信学会，数式処理学会，IACR 各会員．