Bulk 量子計算モデル上における Grover のアルゴリズムの繰返し回数について

大久保 誠也[†] 西野 哲朗[†]
太田 和夫[†] 國廣 昇[†]

本論文では，NMR 量子計算機をモデル化した，Bulk 量子計算モデル上で動作する，Grover のアルゴリズムの繰返し回数について考察する．最初に，Bulk 量子計算モデル上で Grover のアルゴリズムを用いて論理式の充足可能性判定問題（SAT）を解くのに必要となる繰返し回数について議論する．次に，解がただ 1 つのみ存在する探索問題に対する量子アルゴリズムを提案する．また，この探索アルゴリズムの秘密鍵探索問題に対する応用についても述べる．さらに，解が複数存在する探索問題に対する量子アルゴリズムも提案する．以上の考察から，本論文で提案する Bulk 量子計算モデルは，通常の量子計算モデルよりも Grover のアルゴリズムを高速に実行できる場合があることが分かる．

On the Required Number of Grover Iterations on a Bulk Quantum Computation Model

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

In this paper, we discuss the required number of Grover iterations used in a quantum search algorithm on a bulk quantum computation model which generalizes NMR (Nuclear Magnetic Resonance) quantum computers. First, we discuss the time complexity of Grover's algorithm on the bulk quantum computation model which is used to solve the satisfiability (SAT) problem. Then, we propose a quantum algorithm on the bulk quantum computation model for the search problem which has only one solution by using Grover's algorithm. And we apply this algorithm to the secret key search problem. Furthermore, we also propose a quantum algorithm on the bulk quantum computation model for the search problem which has multi solutions. From these observations, we can conclude that the bulk quantum computation model can compute faster than the ordinary quantum computation model in some situations.

1. まえがき

計算という概念を形式的に定義するために，1936 年に Turing は Turing 機械という計算モデルを提案した．Turing 機械は計算の本質を見事に抽象化しており，現在の計算機の基本的なモデルとなっている．一方，1985 年に，Deutsch は，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た[1),2)]．そして，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)]．このほかにも，さまざまな研究成果から，量子 Turing 機械は，通常の Turing 機械と比べて本質的に高速に計算を行える場合があると予想されている．

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，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．しかし，このような 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り，**Bulk 量子計算**と呼ばれ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

† 電気通信大学情報通信工学科
Department of Information and Communication Engineering, The University of Electro-Communications

われている[6)~8)].

特に，文献 7) では，NMR 量子計算が通常の量子計算よりも効率的である可能性が（計算モデルを用いずに）定性的に指摘されている．しかし，このような議論は，明確な計算モデル上で行わなければならない．なぜなら，たとえば，NMR 量子計算機が，出力値に対する無限の測定精度を持つと仮定すると，論理式の充足可能性判定問題（SAT）が多項式時間で解けるという非現実的な結果が導き出されてしまうからである．実際の NMR 装置には，測定精度に関する厳しい制約があるため，NMR 量子計算のアルゴリズムの効率について理論的に考察する際には，このような測定精度を十分考慮に入れる必要がある．そこで，本論文では，このような NMR 量子計算の枠組みを反映させた Bulk 量子計算モデルを提案し，その性質について考察する．

具体的には，出力値の測定精度について厳密な制約を設けても，Bulk 量子計算モデル上では，Grover のアルゴリズムの効率が改善できることを示す．本論文の構成は，以下のとおりである．まず，2 章で Bulk 量子計算の数学的定義を述べ，3 章で Grover のアルゴリズムについて概観する．4 章では，Bulk 量子計算モデル上で，Grover のアルゴリズムを用いて充足性判定問題を解く場合の効率について解析する．続く 5 章と 6 章では，Grover のアルゴリズムを用いて，Bulk 量子計算モデル上で探索問題を解くアルゴリズムを提案する．特に，5 章では探索すべき解が唯一の場合の探索アルゴリズムについて述べ，その秘密鍵探索問題への応用を示す．近年，量子暗号と呼ばれる秘密鍵の配送方式が活発に研究されているが，本章で述べる結果は，Bulk 量子計算モデルが，秘密鍵暗号方式に対して脅威となりうる可能性を指摘している．さらに，6 章では，より一般的な場合として，探索すべき解が複数の場合の Bulk 量子探索アルゴリズムについて述べる．最後に，7 章で結論を述べる．

2. Bulk 量子計算

1985 年に，英国人物理学者 Deutsch は，**量子回路**（quantum circuit）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[3)]．この量子回路によって構成された計算機が，**量子計算機**と呼ばれている．

通常の組合せ論理回路の 1 本のワイヤには，0 または 1 が保持できるが，量子回路の 1 本のワイヤには，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．

量子回路の 1 本のワイヤが保持できる情報量を **1 量子ビット**（quantum bit，qubit）という．量子回路の動作は，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，量子回路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．

本論文では，近い将来に比較的容易に実現可能と思われている，NMR 量子計算をモデル化した **Bulk 量子計算**について考察する．Bulk 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．一般に量子回路の出力は，量子ワイヤ上に，$\alpha|0\rangle+\beta|1\rangle$ 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，この重ね合わせ状態 $\alpha|0\rangle+\beta|1\rangle$ 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 量子計算などの Bulk 量子計算においては，同じ重ね合わせ状態を測定すると，$|\beta|^2-|\alpha|^2$ という実数値が測定できるものと仮定される．ただし，その際には測定誤差 $\varepsilon>0$ が存在し，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

$$|\beta|^2-|\alpha|^2-\varepsilon \le \theta \le |\beta|^2-|\alpha|^2+\varepsilon \qquad (1)$$

を満たす実数値 θ が読み出せるという精度保証がなされているものと仮定する．

ただし，この ε は回路の入力数に依存する値であり，さらに，NMR 量子計算におけるサンプル数のような，計算装置ごとに定まるパラメータにも依存する値として，各量子回路ごとに指定される値であるとする．

本論文で提案する Bulk 量子計算モデルは，通常の量子回路において，その出力値の読み出しに，上記の規約を仮定する．

また，Bulk 量子計算における測定では，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と仮定する．

ここで ε は 1 以下の定数であるが，たとえば NMR

装置の測定精度の場合，4 ∼ 5 量子ビットの Grover のアルゴリズムの実験においては，ε の値が $\frac{1}{8}$ 以下と仮定できるといわれている．ただし，この ε の値は，現在の液体 NMR を用いた実験におけるものであり，固体 NMR その他を用いた将来の Bulk 量子計算装置においては，ε の値がさらに改善されていくものと期待されている．

3. Grover のアルゴリズム

いま，$0 \leq r \leq 2^n - 1$ なる整数 r 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 r_0 が存在して，$x = r_0$ 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仮定する．

Grover のアルゴリズムが扱う**探索問題**は，以下のとおりである．

入力：量子オラクルとして実現されるブール関数 f の変数の個数 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 r_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，r_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．これに対し，Grover のアルゴリズムでは，このオラクル呼び出しの回数の期待値を，$O\left(\sqrt{2^n}\right) = O\left(2^{n/2}\right)$ にすることができる．本論文では，量子アルゴリズムの実行に必要な時間量を，このようなオラクル呼び出しの回数によって評価するものとする．

論文 5) で，Grover は，以下の量子探索アルゴリズムを示した．

(1) n 個の量子ビットを，$|00...0\rangle$ から $|11...1\rangle$ のすべての n ビット状態（S で表す）が等しい振幅を持つ重ね合わせ状態に初期化する．

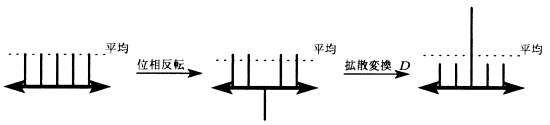

図 1 拡散変換による振幅の増幅
Fig. 1 Amplitude amplification by the diffusion transform.

(2) 以下の Grover 変換 G を $O(\sqrt{N})$ 回繰り返す．

(a) 量子オラクルを呼び出すことにより，上記重ね合わせ状態中の各状態 S に対し，以下の変換を並列実行する．

- $f(S) = 1$ の場合は**位相反転** を適用する．
- $f(S) = 0$ の場合は何も行わない．

(b) 以下のような行列 D により定義される**拡散変換** D を適用する．ただし，$N = 2^n$ とする．

$$D_{ij} = \frac{2}{N} \text{ if } i \neq j \text{ and } D_{ii} = -1 + \frac{2}{N}$$

(3) 最終的に得られた状態を測定する．少なくとも，0.5 以上の確率で状態 r_0 が得られる．

上のステップ 2 の部分が Grover のアルゴリズムの核心であり，これによって，所望の状態の振幅を $O\left(\frac{1}{\sqrt{N}}\right)$ ずつ増幅することができる．したがって，ステップ 2 を $O\left(\sqrt{N}\right)$ 回繰り返すことにより，r_0 に対応する所望の状態を得る確率を，1 に近づけることができる．

拡散変換 D は平均についての反転演算として解釈できる．すなわち，上のアルゴリズムで行っていることは，

a) 所望の状態の振幅の符号を反転させることによって平均値から遠ざけ，

b) 平均値を中心として折り返すことにより，所望の状態の振幅をより大きく，その他の状態の振幅をより小さくすることとして説明できる（**図 1** 参照）．

4. Bulk 量子計算モデル上で SAT を解く量子アルゴリズム

本章では，Bulk 量子計算機上で充足性判定問題を解く量子アルゴリズムを示し，その計算量を考察する．

4.1 充足可能性判定問題

本章で取り扱う充足性判定問題（satisfiability problem，SAT）とは，以下のような問題である．

入力：n 変数ブール式 $f(x_1, x_2, \cdots, x_n)$.

問題：$f(x_1, x_2, \cdots, x_n) = 1$ を満足する $(a_1, a_2, \cdots, a_n) \in \{0,1\}^n$ が存在するか否かを判定せよ．

ここで，$\{0,1\}^n$ の中に $f(x) = 1$ を満たす充足解 $x \in \{0,1\}^n$ は全部で t 個含まれているものとする．この t の値は未知であり，$t \ll N$ と仮定する．また，任意の解 x に対し $f(x)$ の計算は単位時間で可能であるものとする．

4.2 アルゴリズムのアイデア

Bulk 量子計算を行う量子回路の先頭の n 量子ビットを等振幅の重ね合わせ状態に設定し，$n+1$ 番目の量子ビットに $f(x)$ の計算結果を書き込んでから，$n+1$ 番目の量子ビットを観測することを考える．このとき，充足解が存在しないならば，重ね合わせ内の $n+1$ 番目の量子ビットに書き込まれている値はすべて 0 であるため，$|\beta|^2 - |\alpha|^2$ の値は -1 となる．一方，充足解が存在するならば，$|\beta|^2 - |\alpha|^2$ の値は -1 より大きな値となる．しかしながら，Bulk 量子計算においては ε の測定誤差が存在するため，充足解が存在する場合と存在しない場合を区別することができない場合がある（**図 2** の初期状態を参照）．

そこで，Grover 変換を行うことにより，充足割当てに対応する状態の振幅を増幅した後に，$n+1$ 番目の量子ビットに $f(x)$ の計算結果を書き込み，$n+1$ 番目の量子ビットを測定することを考える．この場合，充足解に対応する状態の振幅が増幅しているため，充足解が存在する場合は，$|\beta|^2 - |\alpha|^2$ の値が，Grover 変換を行わない場合よりも大きな値となる．一方，充足解が存在しない場合は，Grover 変換を行わない場合と同様に $|\beta|^2 - |\alpha|^2$ の値は -1 となる（図 2 の状態 1 を参照）．

このようにして Grover 変換を繰り返し，充足解に対応する状態の振幅を増幅することにより，充足解が存在する場合と存在しない場合を区別することができるようになる（図 2 の状態 2 を参照）．

4.3 アルゴリズム

SAT を解く Bulk 量子計算アルゴリズム BULKSAT の詳細は，以下のとおりである．

BULKSAT

[入力]： 量子オラクルとして与えられるブール関数 f の変数の個数 n.

[出力]： もし $f(x) = 1$ を満たすような $x \in \{0,1\}^n$ が存在するならば 1 を返す．それ以外の場合は 0 を返す.

[アルゴリズム] アルゴリズム BULKSAT は以下の 5 ステップからなる．

[ステップ 1] $j = 1$ に設定する．ここで，j は Grover 変換の繰返し回数のカウンタである．$n+1$ 個の量子ビットを，以下のような初期状態に設定する．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] 上記の重ね合わせ状態に Grover 変換 G を 1 回適用する（詳細は 3 章参照）．適用後の状態は以下のようになる．

$$\sum_{x \in N_{ans}} \sqrt{a_j} |x\rangle |0\rangle + \sum_{x \notin N_{ans}} \sqrt{\frac{1 - t a_j}{N - t}} |x\rangle |0\rangle$$

ここで N_{ans} は t 個の充足解からなる集合であり，$\sqrt{a_j}$ は Grover 変換を j 回適用した時点での，解である状態の振幅である．

[ステップ 3] $n+1$ 番目の量子ビットに $f(x)$ の値を書き込む．すると，以下の重ね合わせ状態が得られる．

$$\sum_{x \in N_{\mathrm{ans}}} \sqrt{a_j} |x\rangle |1\rangle + \sum_{x \notin N_{\mathrm{ans}}} \sqrt{\frac{1 - t a_j}{N - t}} |x\rangle |0\rangle$$

その後，$n+1$ 番目の量子ビットを測定する．得られた測定値を θ_a とする．

[ステップ 4] もし $\theta_a > -1 + \varepsilon$ ならば，1 を出力して停止する．そうでないならば，次のステップに進む．

[ステップ 5] もし $j > \sqrt{\varepsilon N}$ ならば，答えとして 0 を出力して停止する．成立していなければ，$j := j + 1$ とし，$n+1$ 番目の量子ビットを 0 に戻した後，ステップ 2 へ戻る．

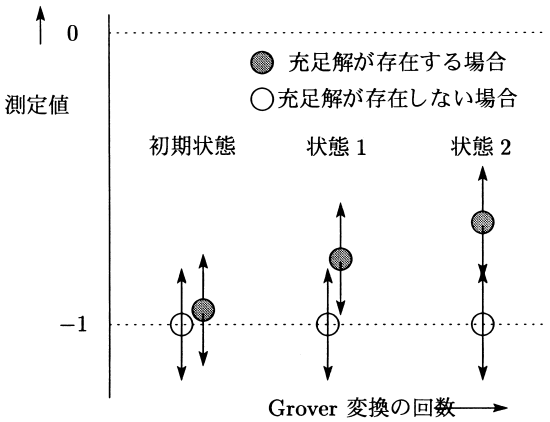

図 2 アルゴリズム BULKSAT の実行の様子
Fig. 2 The situation of the execution of BULKSAT.

4.4 アルゴリズムの正当性と計算量

上記のステップ 3 で $n+1$ 番目の量子ビットを測定したときの測定値について考える．

まず，充足解が存在するとき，つまり $t \geq 1$ の場合について考える．j 回の振幅増幅を行った結果，充足解に対応する状態の振幅が $\sqrt{a_j}$ となったとする．この場合，充足解ではない状態の振幅は $\sqrt{\dfrac{1-a_j t}{N-t}}$ となる．

このとき，$|\alpha|^2 - |\beta|^2$ の値は，

$$\left|\sqrt{a_j}\right|^2 t - \left|\sqrt{\frac{1-a_j t}{N-t}}\right|^2 (N-t) = -1 + 2a_j t$$

となる．この値が $-1+2\varepsilon$ を超えていれば，充足解が存在すると判断することができるので（図 2 参照），充足解に対応する状態の振幅が $\sqrt{a_j} > \sqrt{\dfrac{\varepsilon}{t}}$ を満たすようになるまで，Grover 変換を繰り返せばよい．

Grover のアルゴリズムでは，量子オラクルを j 回呼び出した時点での充足解に対応する状態の振幅 $\sqrt{a_j}$ は $\sqrt{a_j} = \dfrac{\sin((2j+1)\theta)}{\sqrt{t}}$ と表すことができる．ここで，$\sin\theta = \sqrt{\dfrac{t}{N}}$ である．したがって，

$$\sqrt{a_j} > \sqrt{\frac{\varepsilon}{t}}$$

つまり，

$$\sin((2j+1)\theta) > \sqrt{\varepsilon} \qquad (2)$$

を満たす j を求めればよい．また，$\varepsilon \leq \dfrac{1}{8}$ と仮定すると，$\sqrt{\varepsilon}$ は非常に小さい値と見なすことができる．式 (2) を満たす最も小さい j を求めたいので，$\sin((2j+1)\theta)$ も非常に小さい値と考えることができる．よって，$\sin((2j+1)\theta) \simeq (2j+1)\theta$ と近似することができる．また，$\frac{t}{N} \ll 1$ であるので，$\theta = \sqrt{\dfrac{t}{N}}$ と近似できる．以上のことより，式 (2) は，

$$(2j+1)\sqrt{\frac{t}{N}} > \sqrt{\varepsilon}$$

となり，この不等式を解くことにより

$$j > \frac{1}{2}\sqrt{\frac{\varepsilon N}{t}} - \frac{1}{2}$$

を得る．

したがって，$\dfrac{1}{2}\sqrt{\dfrac{\varepsilon N}{t}}$ 回 Grover 変換を繰り返せば充足解が存在することを確認できる．

充足解が 1 つでも存在するならば，$\dfrac{1}{2}\sqrt{\varepsilon N}$ 回 Grover 変換を繰り返すまでに，アルゴリズムは 1 を出力して停止する．したがって，$\dfrac{1}{2}\sqrt{\varepsilon N}$ 回 Grover 変換を繰り返すまでにアルゴリズムが停止しないならば，充足解は存在しないと判断できる．

このようにして，提案アルゴリズムは $\dfrac{1}{2}\sqrt{\dfrac{\varepsilon N}{t}}$ 回の Grover 変換を行うことで，充足可能性判定問題を解く．Grover 変換の 1 回の実行につき，関数 f の値を 3 回評価するため，全体では関数 f を $\dfrac{3}{2}\sqrt{\dfrac{\varepsilon N}{t}}$ 回評価すればよい．

5. BULK 量子計算モデル上の量子探索アルゴリズム（唯一解の場合）

本章では，BULK 量子計算機上における Grover のアルゴリズムの実行について考える．ただし，本章では，所望の解はちょうど 1 つしか存在しないと仮定する．

5.1 アルゴリズムのアイデア

初期状態では $N/2$ 個の 0 と $N/2$ 個の 1 が重ね合わされているため，$|\beta|^2 - |\alpha|^2$ の値は 0 となる（**図 3** 中の初期状態を参照）．

ここで，Grover 変換を行うことにより，充足解に対応する状態の振幅を増幅した後に，k 番目の量子ビットを測定したとする．この場合，充足解に対応する状態の振幅が増幅されているため，充足解の k ビット目が 1 であるときは，$|\beta|^2 - |\alpha|^2$ の値は，初期状態の値よりも大きな値となる．一方，充足解の k ビット目が 0 であるときは，初期状態の値よりも小さな値となる（図 3 中の状態 1 を参照）．Grover 変換を繰り返し，充足解に対応する状態の振幅を増幅することにより，充足解が存在する場合と存在しない場合を区別することができるようになる（図 3 中の状態 2 を参照）．

5.2 アルゴリズム

提案アルゴリズム BULKSEARCH1 の詳細は，以下のとおりである．

BULKSEARCH1(n)

[入力]： 量子オラクルとして与えられるブール関数 f の変数の個数 n.

[出力]： $f(x)=1$ を満たすような $x \in \{0,1\}^n$.

[アルゴリズム] アルゴリズムは以下の 3 ステップからなる．

[ステップ 1] n 個の量子ビットを以下のような初期状態に設定する．ただし，$N = 2^n$ とする．

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

[ステップ 2] Grover 変換 G を $\dfrac{1}{2}\sqrt{\varepsilon N}$ 回適用する．適用後の状態は以下のようになる．

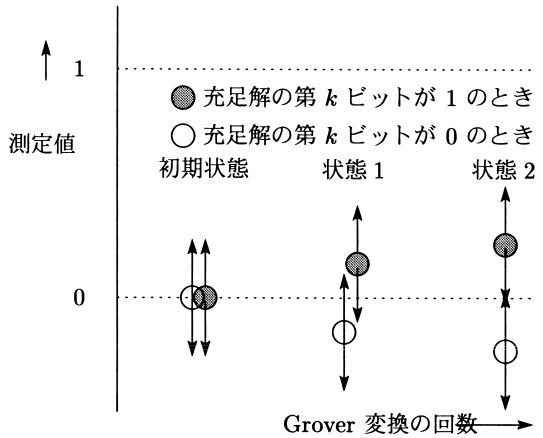

図 3 アルゴリズム BULKSEARCH1 の実行の様子
Fig. 3 The situation of the execution of BULKSEARCH.

$$\sqrt{a_j}\,|x_{ans}\rangle + \sum_{x \notin N-x_{ans}} \sqrt{\frac{1-a_j}{N-1}}\,|x\rangle$$

ここで，x_{ans} は充足解，$\sqrt{a_j}$ は充足解の振幅であるとする．

[ステップ 3] 1〜n 番目までの，各量子ビットを測定し，解を決定する．第 k 量子ビットの測定値を θ_k とする．もし $\theta_k > 0$ ならば，解の k ビット目の値を 1 とする．もし $\theta_k < 0$ ならば，解の k ビット目の値を 0 とする．

5.3 アルゴリズムの正当性と計算量

j 回の Grover 変換によって振幅増幅を行い，充足解に対応する状態の振幅が $\sqrt{a_j}$ になったときに，k 番目の量子ビットを測定したとする．充足解の k ビット目の値が 1 であったとすると，k 番目の量子ビットの重ね合わせ状態は，振幅 $\sqrt{a_j}$ を持つ $|1\rangle$ が 1 個と，振幅 $\sqrt{\frac{1-a_j}{N-1}}$ を持つ $|1\rangle$ が $N/2-1$ 個，および，振幅 $\sqrt{\frac{1-a_j}{N}}$ を持つ $|0\rangle$ が $N/2$ 個より構成されている．

このとき，$|\beta|^2 - |\alpha|^2$ の値は，$a_j + \frac{1-a_j}{N-1} * (N/2-1) - \frac{1-a_j}{N-1} * (N/2) = \frac{a_j N - 1}{N-1}$ となる．この値が閾値 ε を超えていれば，測定値として 0 よりも大きい値を読み出すことができ，解を決定することができる．したがって，$a_j \geq \frac{\varepsilon N - \varepsilon + 1}{N}$ を満たすまで Grover 変換を繰り返せばよい．

また，$\sqrt{a_j} = \sin((2j+1)\theta)$ と表すことができる．ここで，$\sin\theta = \sqrt{\frac{1}{N}}$ である．したがって，

$$\sqrt{a_j} > \sqrt{\frac{\varepsilon N - \varepsilon + 1}{N}}$$

つまり，

$$\sin((2j+1)\theta) > \sqrt{\frac{\varepsilon N - \varepsilon + 1}{N}}$$

を満たす j を求めればよい．ε は非常に小さい値であるので，$\sqrt{\frac{\varepsilon N - \varepsilon + 1}{N}}$ も非常に小さい値である．よって，4.4 節と同様に，$\sin((2j+1)\theta) \simeq (2j+1)\theta$ と近似することができる．また，$\frac{1}{N} \ll 1$ であるので，$\theta = \sqrt{\frac{1}{N}}$ と近似できる．以上のことより，4.4 節と同様の変換を行い，

$$j > \frac{1}{2}\sqrt{\varepsilon N - \varepsilon + 1} - \frac{1}{2}$$

を得る．したがって，$\frac{1}{2}\sqrt{\varepsilon N}$ 回 Grover 変換を繰り返せば，充足解の k ビット目が 1 であることを確定できる．

充足解の k ビット目が 0 である場合の解析も，同様である．

以上により，BULK 量子計算によって Grover のアルゴリズムを実行した場合，$\frac{1}{2}\sqrt{\varepsilon N}$ 回の Grover 変換の適用で十分であることが分かった．したがって，この場合には，通常の量子計算機上で Grover のアルゴリズムを動作させた場合と比べ，より少ない Grover 変換の回数で解を求めることができる可能性がある．

5.4 秘密鍵探索への応用

提案アルゴリズムを利用して暗号の秘密鍵探索を行うことを考える．

一般的な秘密鍵暗号では，秘密鍵 y を利用して平文 m の暗号化を行う．ここで，攻撃者は，平文と暗号文の組が 1 つと，たとえば，AES のような平文を暗号文に変換する暗号化アルゴリズムが手に入ったときに，暗号文を作成するために使用した秘密鍵の推測を行いたいとする．また，平文と暗号文の組が 2 つ以上ある場合，鍵 y はほぼ唯一になることが知られている．よって，もしこの秘密鍵を推測されてしまうと，暗号文作成者の他の暗号文を解読されたり，平文から暗号文を偽造されたりしてしまう可能性がある．

つまり，ここで取り扱う秘密鍵探索問題とは，以下のような問題である．

[入力] 暗号アルゴリズム E，平文 m_0，および暗号文 c_0．

[問題] $c_0 = E(m_0, y_0)$ を満たす鍵 y_0 を発見せよ．

このとき，鍵 y が $c_0 = E(m_0, y)$ を満たすかどうかを判定する量子回路（**図 4**）をオラクルとして用

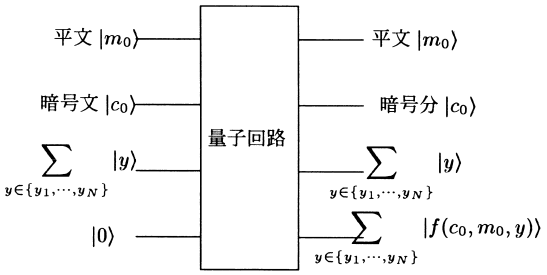

図 4 オラクルに用いる量子回路
Fig. 4 The quantum circuit as the oracle.

いることにより，Grover のアルゴリズムを使用して秘密鍵探索問題を解くことができる．つまり，秘密鍵の候補 $y_1,\cdots,y_N$ を状態 $S_1,\cdots,S_N$ にそれぞれ対応させ，オラクルである量子回路を，$C(S)=1 \Leftrightarrow f(m_0,c_0,y)=1 \Leftrightarrow c_0=E(m_0,y)$，となるように構成すればよい．ただし，この回路は通常のオラクルと違って単位時間で判定が行えるわけではないことに注意する．

鍵の長さが 58 ビットであるとき，通常の量子計算機（QC）と BULK 量子計算機上で Grover のアルゴリズムを用いて秘密鍵探索を行うのに，何回のオラクル呼び出しが必要であるかを評価した．結果を**表 1** に示す．$\varepsilon=\frac{1}{2}$ である BULK 量子計算機上で Grover のアルゴリズムを動作させたとき，必要なオラクル呼び出しの回数は，通常の量子計算機上で成功確率 $\frac{1}{2}$ で探索を行ったときと等しくなる．また，$\varepsilon=\frac{1}{256}$ であれば，QTM と比べ 8% のオラクル呼び出しの回数で解を探索することができる．

6. BULK 量子計算モデル上の量子探索アルゴリズム（複数解の場合）

5 章では解がちょうど 1 つ存在する場合の探索アルゴリズムを提案した．しかし，そのアルゴリズムでは，充足解が複数個存在する場合には，最後に特定の量子ビットを測定しても，0 である充足解と 1 である充足解の確率振幅が打ち消しあい，正しい解を求めることができない．そこで，本章では，4.3 節のアルゴリズムを利用して，解が 2 個以上存在する場合の解探索を行うことを考える．

6.1 アルゴリズムのアイデア

k 番目の量子ビットの値を 1 に設定した状態で，アルゴリズム BULKSAT を動作させると，k ビット目の値が 1 である充足解が存在するか否かを判定することができる．このとき，もし充足解が存在したならば，それ以後 k ビット目の値を 1 に固定する．逆に，充足解が存在しなかったならば，それ以後 k ビット目の値を 0 に固定する．

表 1 鍵が 58 ビット長の場合に必要なオラクル呼び出しの回数
Table 1 The number of the oracle calls when the key length is 58 bits.

	測定誤差	必要なオラクル呼び出しの回数	比
QC	（成功確率 99%）	394,768,936	187%
	（成功確率 50%）	210,828,713	100%
BULK QC	$\varepsilon=1/2$	210,828,713	100%
	$\varepsilon=1/4$	140,552,475	66%
	$\varepsilon=1/8$	97,003,748	46%
	$\varepsilon=1/16$	67,828,338	32%
	$\varepsilon=1/32$	47,703,825	22%
	$\varepsilon=1/64$	33,642,433	16%
	$\varepsilon=1/256$	16,788,157	8%

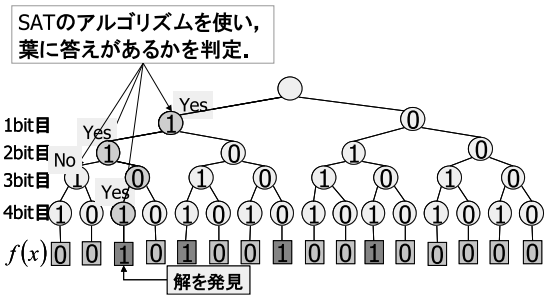

図 5 アルゴリズム BULKSEARCH2 の実行の様子
Fig. 5 The situation of the execution of BULKSEARCH2.

上の操作を $k=1$ から $k=n$ まで繰り返すことにより，最終的に 1 つの充足解を発見することができる．4 ビットの場合の実行の様子を**図 5** に示す．

6.2 アルゴリズムの詳細

提案アルゴリズム BULKSEARCH2 は以下のとおりである．ただし，そのアルゴリズム中で用いる BULKSAT2 については，後から説明する．

BULKSEARCH2(n)

[入力]： 量子オラクルとして与えられるブール関数 f の変数の個数 n.

[出力]： $f(x)=1$ を満たす充足解 $x\in\{0,1\}^n$. ただし，充足解は全部で t 個存在するものとし，$t\geq 2$ の値は未知であるとする．

[アルゴリズム] 1 から n までの i に対し，以下のステップ 1 からステップ 3 までを繰り返す．

[ステップ 1] $x_i=1$ に設定し，次のような均等な重ね合わせ状態を生成する．

$$|X_i\rangle=\sum_{x_n=0}^{1}\cdots\sum_{x_{i+1}=0}^{1}\frac{1}{\sqrt{2^{n-i}}}|x_n\cdots x_{i+1}1y_{i-1}\cdots y_1\rangle|0\rangle.$$

ここで $y_{i-1},\cdots,y_1$ はすでに固定された値と

表 2 Grover のアルゴリズムの繰返し回数（オラクル呼び出しの回数）の比較
Table 2 The comparison of the number of Grover iterations (i.e., the number of oracle calls).

		QC		BULKQC		
アルゴリズム		Grover のアルゴリズム		BULKSAT	BULKSEARCH1	BULKSEARCH2
成功確率		1/2	1			
SAT		$O\left(\sqrt{\frac{N}{t}}\right)$	$\Theta(N)$	$\frac{3}{2}\sqrt{\frac{\varepsilon N}{t}}$	対象外	対象外
探索	解の個数既知であり 1 つ	$\frac{\pi}{8}\sqrt{N}$	$O(\sqrt{N})$	対象外	$\frac{1}{2}\sqrt{\varepsilon N}$	$\frac{3(\sqrt{2}+1)}{2}\sqrt{\varepsilon N}$
	解の個数未知	$O\left(\sqrt{\frac{N}{t}}\right)$	$\Theta(N)$	対象外	対象外	$\frac{3(\sqrt{2}+1)}{2}\sqrt{\varepsilon N}$

する．

[ステップ 2] 以下で述べるサブルーチン BULKSAT2($n-i, 1y_{i-1}\cdots y_1$) を呼び出す．ここで，BULKSAT2 ($n-i, 1y_{i-1}\cdots y_1$) は $f(y_n\cdots y_{i+1}1y_{i-1}\cdots y_1) = 1$ となる $y_n\cdots y_{i+1} \in \{0,1\}^{n-i}$ が存在するとき，かつ，そのときに限り 1 を返し，さもなければ，0 を返す．

[ステップ 3] BULKSAT2($n-i, 1y_{i-1}\cdots y_1$) の出力値を y_i の値に設定し，$i := i+1$ とする．

[ステップ 4] 充足解 $y_n\cdots y_1$ を出力して停止する．

ここで，アルゴリズム BULKSAT2 の詳細は，以下のとおりである．

BULKSAT2(q, z)

[入力]： q および $z \in \{0,1\}^{n-q}$．

[出力]： もし $f(m' \circ z) = 1$ を満たすような $m' \in \{0,1\}^q$ が存在するならば，1 を返す（$\circ$ は記号列の連結を表す）．さもなければ，0 を返す．ここで，下位ビットが z である f の充足解は全部で t' 個あるものとし，t' の値は未知であるとする．

[アルゴリズム] アルゴリズム BULKSAT2 は以下の 5 ステップからなる．

[ステップ 1] $j = 1$ に設定する．ここで，j は Grover 変換の繰返し回数のカウンタである．以下のような初期状態を生成する．

$$\sum_{m=0}^{2^q-1} \frac{1}{\sqrt{2^q}} |m\rangle |0\rangle$$

[ステップ 2] Grover 変換 G を適用する．適用後の状態は以下のようになる．

$$\sum_{m\in M_{\rm ans}} \sqrt{a_j}\,|m\rangle\,|0\rangle + \sum_{m\notin M_{\rm ans}} \sqrt{\frac{1-ta_j}{2^q-t}}\,|m\rangle\,|0\rangle$$

ここで $M_{\rm ans}$ は t' 個の充足解からなる集合であり，$\sqrt{a_j}$ は充足解に対応する状態の振幅である．

[ステップ 3] $(k+1)$ 番目の量子ビットに $f(m \circ z)$ の値を書き込み，$(k+1)$ 番目の量子ビットを観測する．測定値が θ_a であったとする．

$$\sum_{m\in M_{\rm ans}} \sqrt{a_j}\,|m\rangle\,|1\rangle + \sum_{m\notin M_{\rm ans}} \sqrt{\frac{1-ta_j}{2^q-t}}\,|m\rangle\,|0\rangle$$

[ステップ 4] もし $\theta_a > -1+\varepsilon$ ならば，1 を出力する．さもなければ，次のステップに進む．

[ステップ 5] $j > \sqrt{\varepsilon 2^q}$ であれば，0 を出力する．さもなければ，$j := j+1$ とし，$(k+1)$ 番目の量子ビットを 0 に戻した後，ステップ 2 へ戻る．

6.3 アルゴリズムの計算量

i ビット目の値を決定する際の，BULKSAT2 の実行時における探索空間のサイズは $N/2^i$ であるため，たかだか $\frac{1}{2}\sqrt{\frac{\varepsilon N}{2^i}}$ 回，Grover 変換を繰り返すことにより，充足解が存在するか否かを判定することができる．このようにして，1 ビット目から n ビット目までの値を決定するためには，全体として $\sum_{k=1}^{n} \frac{1}{2}\sqrt{\frac{\varepsilon N}{2^k}} < \frac{\sqrt{2}+1}{2}\sqrt{\varepsilon N}$ 回の Grover 変換を行えばよい．1 回の Grover 変換につき，関数 f を 3 回評価しなければならないため，アルゴリズム全体としては，最悪 $\frac{3(\sqrt{2}+1)}{2}\sqrt{\varepsilon N}$ 回 f の評価を行う必要がある．

7. ま と め

本論文では，Bulk 量子計算モデル上における Grover のアルゴリズムの繰返し回数（オラクル呼び出しの回数）について，さまざまな角度から考察を行ってきた．本論文で得られた結果をまとめると，**表 2** のようにな

る．比較のために，通常の量子計算モデル上で必要とされる繰返し回数も併記した．表 2 の左から 2 列目に示した繰返し回数の $\Theta(N)$ 下界は，文献 9) による．

2 章において，Bulk 量子計算においては，実数値 θ は式 (1) を満たす値として読み出すことができるとした．そこで，以下では，この θ が式 (1) の満たす値として確実に読み出すことができる場合と，確実には読み出すことができないが，高い確率では読み出すことができる場合とに分けて評価を行う．ここで，θ の値が確実に読み出せるか否かは，Bulk 量子計算モデルの実装に依存して決まる．

θ の値をある精度内の値として，確実に読み出すことができる場合，Bulk 量子計算モデル上で，本論文で示したアルゴリズム BULKSEARCH2 を動作させれば，誤り確率 0 で正解を得ることができる．しかも，そのときに必要な繰返し回数は $O\left(\sqrt{N}\right)$ 回である．通常の量子計算機では確率 1 で解を発見するには $O(N)$ 回の繰返しが必要であるため，Bulk 量子計算モデルは，通常の量子計算モデルよりも効率的に計算を行えることが分かる．

一方，θ の値をある精度内の値として確実には読み出すことができないが，高い確率で読み出すことができる場合を考える．この場合，提案アルゴリズムには誤り確率が存在する．解が複数個あるとき，通常の量子計算機と比べ，BULKSEARCH2 は $O(\sqrt{t})$ 倍の繰返しが必要となってしまう．しかし，その場合でも，解の個数が 1 つのときには，BULKSEARCH1 は通常の量子計算モデルよりも定数倍効率的に計算を行える．

謝辞 本論文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．

本研究は，文部科学省科学研究費補助金特定領域研究（2）（課題番号：16016235，16092208）の援助を受けています．

参 考 文 献

1) Bernstein, E. and Vazirani, U.: Quantum Complexity Theory, *Proc. 25th ACM Symposium on Theory of Computing*, pp.11–20 (1993).
2) Deutsch, D.: Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proc. R. Soc. Lond.*, Vol.A 400, pp.97–117 (1985).
3) Deutsch, D.: Quantum Computational Networks, *Proc.R.Soc.Lond.*, Vol.A 400, pp.97–117 (1985).
4) Shor, P.W.: Algorithms for Quantum Computation : Discrete Log and Factoring, *Proc. 35th Annual 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) Collins, D.: Shortening Grover's search algorithm for an expectation value quantum computer, *quant-ph/0209148* (2002).
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) Beals, R., Buhrman, H., Cleve, R., Mosca, M. and de Wolf, R.: Quantum Lower Bounds by Polynomials, *quant-ph/9802049* (1998).

(平成 16 年 11 月 29 日受付)
(平成 17 年 1 月 5 日再受付)
(平成 17 年 2 月 4 日採録)

大久保誠也（正会員）

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 年電気通信大学大学院電気通信学研究科博士前期課程修了．平成 17 年電気通信大学大学院電気通信学研究科博士後期課程修了．同年，電気通信大学研究員（COE）．現在に至る．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 年～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．