4 情報・物理双方から見た量子探索アルゴリズム

加藤　豪〔日本電信電話（株）NTT コミュニケーション科学基礎研究所〕
谷 誠一郎〔日本電信電話（株）NTT コミュニケーション科学基礎研究所／
JST ERATO-SORST 量子情報システムアーキテクチャ〕

量子計算アルゴリズムの中で，Shor の因数分解アルゴリズムと並び，最も有名なものは，Grover の探索アルゴリズムであろう．最良の古典アルゴリズムとの性能比は，因数分解アルゴリズムのそれに及ばないが，探索アルゴリズムが扱っている問題は非常に一般性があり，さまざまな応用が期待されている．本稿では，Grover の探索アルゴリズムと，その主な発展形について解説する．

量子探索とは？

量子探索を理解するためには，まず，ここでいう「探索」とは，どのようなものか説明しなければならない．「探索」問題とは，簡単にいうと，「0」または「1」の値をとる n 個の要素 $(x_1, x_2, \cdots, x_n)$ が入力として与えられたとき，ある i に対して $x_i = 1$ であればインデックス i を解として出力し，すべての i に対して $x_i = 0$ ならば，「解なし」と出力する問題である．ここでは，n 個の要素がソートされていたり，何か構造を持つことを仮定しない．この問題に対して，「出力に誤りを許さない」という条件を満たす探索アルゴリズムは，n 個の要素すべての値を調べるような方法しかないことは比較的容易に証明できる．さらに，「出力誤りは許す」という緩い条件下でさえ，n 個程度の要素の値を調べる必要があることが理論的に証明されている．しかし，驚くべきことに，この誤りを許すという条件下であれば，量子探索アルゴリズムを用いると，わずか $\sqrt{n}$ 回程度，要素の値を調べるだけで，問題が解けることを Grover は示したのである[1]．もちろん，要素の値を調べる回数を少なくできたからといって，それが直ちに，アルゴリズム全体の時間計算量の低減につながるわけではない．しかし，実際に，要素を調べる回数の低減化はアルゴリズム全体の時間計算量の低減の大きなよりどころになる場合が少なくないため，大変な関心を持って量子探索に関する多くの研究がなされてきた．本稿では，それらの中から主な発展形について解説する．

オラクル計算モデル

量子探索を行うアルゴリズムは，多くの場合，オラクル計算モデルを仮定して議論される．そこでまず，古典版オラクル計算モデルにおける探索問題を説明する．古典版オラクル計算モデルでは，探索問題の入力 $(x_1, x_2, \cdots x_n)$ は，「オラクル」と呼ばれるブラックボックスとしてのみ与えられる．そのため，各変数の値を知るためには，このブラックボックスに対して，まず「i 番目の変数の値は何か？」という質問をしなければならない．この質問に対して，ブラックボックスは，i 番目の変数 x_i の値（この例の場合，0 または 1）を出力する．このように古典版オラクル計算モデルでは，アルゴリズムはオラクルに対して質問を繰り返すことにより，計算を進める．

古典版オラクル計算モデルにおけるアルゴリズムのコストは，オラクルに対する質問回数として定義される．オラクル計算モデルの量子版も，考え方は基本的に同じであるが，アルゴリズムにおける情報操作に量子計算を使える点，および，オラクルへの質問を重ね合わせとして行える点が根本的に異なる．以下に，量子版のオラクル計算モデルについて述べる．

量子オラクル計算モデルでは，オラクルを入力に依存した量子操作を行うブラックボックスであると考える．量子操作は，量子力学の公理により，常に可逆操作でなければならない．たとえば，オラクルに対する入力が変数のインデックス i であったとき，x_i を出力とする $(x_i$

は，変数 x_i の値を表すものとする）．オラクルは，可逆操作でなければならないので，x_i から入力 i を計算できなければならない．しかし，i から x_i のこの場合の対応は，一般に 1 対 1 対応ではないのでこれは不可能である．そこで，オラクルは，入力 (i, b)（ただし，$b \in \{0, 1\}$ は，定数とする）に対して，組 $(i, b \oplus x_i)$ を出力すると仮定する．この操作が可逆であることは自明である．この操作は，量子状態を表すケット記号 $|\cdot\rangle$ を用いて，通常次のように記述される．

$$|i, b\rangle \mapsto |i, b \oplus x_i\rangle. \tag{1}$$

この操作は量子力学の公理に反しないので量子操作と見なすことができる．そこで，一般的には上に示した操作をオラクルと定義する．**図 -1** にオラクルに対する入出力の様子を示す．量子力学の公理により，量子操作は複数の入力の重ね合わせ（数字によって特定される量子状態を正規直交基底とする複素線型空間中に含まれる長さ 1 のベクトル）も入力とすることが可能でなければならない．さらに，重ね合わされた入力に対する量子操作の出力は，個々別々に入力した場合の量子操作の出力に関する重ね合わせでなければならない（つまり，量子操作は上述の複素線型空間に対する線型演算子でなければならない）．そのため，オラクルは，

$$\sum_{i=1}^{n}\sum_{b=0,1}\alpha_{i,b}\,|i,\ b\rangle \mapsto \sum_{i=1}^{n}\sum_{b=0,1}\alpha_{i,b}\,|i,\ b\oplus x_i\rangle \tag{2}$$

と記述できる．ここで，入力を $|i, \phi\rangle = (|i, 0\rangle - |i, 1\rangle)/\sqrt{2}$（$\phi$ は 0, 1 などの数で表せないものであることの記号による表現）の重ね合わせに制限することを考える．$|i, \phi\rangle$ をオラクルの入力とした場合，(2) を用いることで

$$|i,\ \phi\rangle \mapsto \frac{|i,\ x_i\rangle - |i,\ \overline{x_i}\rangle}{\sqrt{2}}$$

が得られ，これは，

$$|i,\ \phi\rangle \mapsto (-1)^{x_i}\frac{|i,\ 0\rangle - |i,\ 1\rangle}{\sqrt{2}}$$

すなわち，

$$|i, \phi\rangle \mapsto (-1)^{x_i}\,|i, \phi\rangle \tag{3}$$

である．つまり，オラクルは制限された入力に対して $(-1)^{x_i}$ を乗ずる役割を果たしていると見ることができる．実際，オラクルを (3) により定義するほうが，アルゴリズムの記述には見通しがよい場合が多い．以下の文章においては (3) をオラクルの定義（ただし，ϕ はすべてにおいて共通なので省略する）とする．表現を簡単にするために，量子操作であるオラクルに対応する演算子を $\mathcal{O}$ と記述し，オラクルと $\mathcal{O}$ を同一視することにする．結果として，オラクルに何らかの入力がなされて出力が得られることを，入力に対応するベクトルに演算子 $\mathcal{O}$ を作用させると出力に対応するベクトルが生成されることと同一視する．

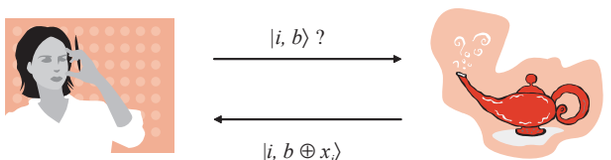


図 -1　量子オラクルによる計算モデル

Grover のアルゴリズム

Grover のアルゴリズムを詳細に理解するためには具体例を見ることが適切である．そこで，3 量子ビットでかつ「解」が 1 つだけ存在する場合を以下に示す．

今，仮に解を 5 とする．するとオラクル $\mathcal{O}$ は

$$\begin{aligned}&\alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle\\ &+ \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle\\ \mapsto\ &\alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle\\ &+ \alpha_4|100\rangle - \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle\end{aligned}$$

と記述される．以下，演算子 $\mathcal{O}$ 以外において「5」の情報を使わずに，量子計算機で「5」を探すわけである．まず量子計算機を $|\psi^{(0)}\rangle = |000\rangle$ に初期化する．次にすべての量子ビットにアダマール演算子

$$H := \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

を作用させる．すると状態 $|\psi^{(0)}\rangle$ はすべての基底に均等に重みがかかった状態

$$\begin{aligned}|\psi^{(1)}\rangle &= H^{\otimes 3}|\psi^{(0)}\rangle\\ &= \tfrac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle\\ &\quad + |100\rangle + |101\rangle + |110\rangle |111\rangle)\end{aligned}$$

となる．ここまでが準備である．次に準備した状態にオラクルを作用させると

$$\begin{aligned}|\psi^{(2)}\rangle &= \mathcal{O}|\psi^{(1)}\rangle\\ &= \tfrac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle\\ &\quad + |100\rangle - |101\rangle + |110\rangle + |111\rangle)\end{aligned}$$

次にアダマールをすべての量子ビットに作用させ

$$\begin{aligned}|\psi^{(3)}\rangle &= H^{\otimes 3}|\psi^{(2)}\rangle\\ &= \tfrac{1}{4}(3|000\rangle + |001\rangle - |010\rangle + |011\rangle\\ &\quad + |100\rangle - |101\rangle + |110\rangle - |111\rangle)\end{aligned}$$

となる．次にゼロ基底以外の係数すべてを反転する演算子 V を作用させ，さらにアダマールをすべての量子ビットに作用させることで

$$\begin{aligned}|\psi^{(4)}\rangle &= H^{\otimes 3}V|\psi^{(3)}\rangle\\ &= \tfrac{1}{4\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle\\ &\quad + |100\rangle + 5|101\rangle + |110\rangle + |111\rangle)\end{aligned}$$

が得られる．ここで，準備した状態 $|\psi^{(1)}\rangle$ と，それに演算 $H^{\otimes 3}VH^{\otimes 3}\mathcal{O}$ を作用させた状態 $|\psi^{(4)}\rangle$ を比較してほしい．「5」に関する情報はオラクル $\mathcal{O}$ のみしか使わずに，基底 $|101\rangle$ の係数のみが増加$\left(\frac{1}{2\sqrt{2}} \rightarrow \frac{5}{4\sqrt{2}}\right)$し他の係数は減少$\left(\frac{1}{2\sqrt{2}} \rightarrow \frac{1}{4\sqrt{2}}\right)$している．つまり，演算 $H^{\otimes 3}VH^{\otimes 3}\mathcal{O}$ を作用させる前より演算を作用させた後の方が，解の「5」を観測結果として出力する確率は増えている．そこで，Grover のアルゴリズムでは，演算 $H^{\otimes 3}VH^{\otimes 3}\mathcal{O}$ を適当な回数行ってから，観測をする．すると解を観測結果として出力する確率は非常に高くなる．実際，この場合においては，この演算を 2 回繰り返してから観測すると結果として「5」を出力する確率は 95％にもなる．以上が Grover のアルゴリズムである．

Grover のアルゴリズムを用いれば，この例でいえば平均して 3 回強だけオラクルを使用すれば正しい解が得られることを示している．他方，3 ビットの数字を入力とし解が 1 つである探索問題を量子的にではなく古典的に解くと，平均して 4 回強は質問が必要である．つまり，量子計算を用いることで問題を解くために必要なオラクルに質問する回数が減ったということである（本来，オラクルへの質問回数の「オーダー」が古典的設定より量子的設定の方が小さいことを主張しているのであり，この比較は少々問題がある．しかし，量子計算が古典計算より優れていることを具体的に確かめられるという点であえて比較してみた）．

では Grover アルゴリズムはなぜ速いのであろうか？以下に，この問いに直感的な答を示したい．準備した状態 $|\psi^{(1)}\rangle$ に演算 $H^{\otimes 3}VH^{\otimes 3}\mathcal{O}$ を m 回だけ施したときに，状態は

$$\cos\{(2m+1)\theta\}\left(2\sqrt{\frac{2}{7}}|\psi^{(1)}\rangle - \frac{1}{\sqrt{7}}|101\rangle\right) + \sin\{(2m+1)\theta\}|101\rangle$$

となる．ただし $\sin\theta = \frac{1}{2\sqrt{2}}$ である．ここで，第 1 項のベクトルは $|\psi^{(1)}\rangle$ から $|101\rangle$ の成分のみをゼロにしたベクトルに平行である．このようになることは，演算 $H^{\otimes 3}VH^{\otimes 3}\mathcal{O}$ の幾何的作用をとらえることで，直感的に理解できる．$\mathcal{O}$ と $H^{\otimes 3}VH^{\otimes 3}$ という演算子ならびに演算はそれぞれ，$|\psi^{(1)}\rangle$ と $|101\rangle$ で張られる空間において閉じている演算である．そして，**図 -2** で示すとおり，$\mathcal{O}$ は $|101\rangle$ に垂直な方向を軸とする鏡面反転操作であり，$H^{\otimes 3}VH^{\otimes 3}$ は $|\psi^{(1)}\rangle$ を軸とする鏡面反転操作を意味する．よって，この 2 つの演算を順次施すことで，状態は $|\psi^{(1)}\rangle$ から $|101\rangle$ 方向への回転操作となっている．ここで，状態 $|\psi^{(1)}\rangle$ は従来の計算機が扱う値から一番遠い状態であり，$|101\rangle$ に至る途中で生じている状態は，$|101\rangle$ と $|\psi^{(1)}\rangle$ の重ね合わせである．まさに，量子系としての特有の状態を利用しており，これが資源となって高速化を実現したのである．

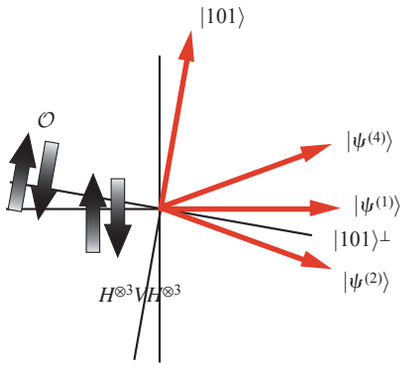


図 -2　演算子 $\mathcal{O}, H^{\otimes 3}VH^{\otimes 3}$ の幾何学的挙動

以上具体例を見てきたが，n 量子ビットの場合にも同様のことが成り立つことを概略的に見ていこう．仮に解が「a」のみであるとする．前処理として状態 $|00\cdots0\rangle$ に初期化した後，アダマール演算子をすべての量子ビットに施す．この状態を $|\psi_n^{(1)}\rangle$ とし，この状態に $H^{\otimes n}VH^{\otimes n}\mathcal{O}$ を m 回作用させると

$$\cos\{(2m+1)\theta\}\left(\sqrt{\frac{n}{n-1}}|\psi_n^{(1)}\rangle - \frac{1}{\sqrt{n-1}}|a\rangle\right) + \sin\{(2m+1)\theta\}|a\rangle$$

となる．ただし，$\sin\theta = \frac{1}{\sqrt{n}}$ である．この表現を見れば分かるように，オラクルへの質問を約 $\frac{2\sqrt{n}}{\pi}$ 回施すことで，解を得られる確率が高くなる．正解までの平均リクエスト回数は通常のオラクル問題に比べて平方根のオーダーで減ることが分かる．この場合においても，解の数が 1 つであることを仮定していた．しかし，解が複数の場合においても上述の方法を拡張することは可能である．しかも，リクエスト回数が減る原理は上述の式にすべて含まれている．

以上，具体例を交えて Grover のアルゴリズムの具体的形を示した．注意すべき点は，このアルゴリズムに含まれている演算子はすべてユニタリであるということである．これは量子計算に求められる必要条件である．

Grover のアルゴリズムの一般化

前の章で示した Grover のアルゴリズムには確率振幅増幅 [2] と呼ばれる重要な一般化がある．具体的には，Grover のアルゴリズムの中で使っていた演算子 $H^{\otimes n}$ の任意のユニタリ演算子 A への置き換えという一般化である（本章以降においても，解の数を 1 つと仮定して議論していくが，基本的には本質的な違いはない）．

以下，Grover のアルゴリズムと同様の書き方で確率振幅増幅の詳細を述べてみる．仮に解が「a」であるとする．前処理として，状態を $|00\cdots0\rangle$ に初期化する．次に演算 A を実行する．この状態を $|\phi^{(1)}\rangle$ とし，この状態に

$AVA^{\dagger}O$ を m 回作用させると

$$\frac{\cos\{(2m+1)\theta\}}{\sqrt{1-|\langle a|\phi^{(1)}\rangle|^2}}\left(|\phi^{(1)}\rangle-\langle a|\phi^{(1)}\rangle|a\rangle\right)$$
$$+\sin\{(2m+1)\theta\}\frac{\langle a|\phi^{(1)}\rangle}{|\langle a|\phi^{(1)}\rangle|}|a\rangle$$

が得られることが分かる．ただし，$\sin\theta=|\langle a|\phi^{(1)}\rangle|$ である．この表現から，約 $\frac{2}{\pi|\langle a|\phi^{(1)}\rangle|}$ 回だけオラクルへの質問をすることで高い確率で解が観測結果として得られる．上述の表現の中において $A^{\dagger}$ は A のエルミート共役な演算子とする．上で示した式においてすべての A を $H^{\otimes n}$ に置き換えると，まさに Grover のアルゴリズムになることは容易に導ける．

ではこの演算子の「一般化」は何を意味するのであろうか？　それは，解決する問題が一般化されているのである．Grover のアルゴリズムが解決しているのはオラクル以外に「1」を出力するインデックス（解）の情報が一切ないという問題を解くアルゴリズムである．他方，確率振幅増幅が解いているのは，解の情報が何らかの形である問題を解くアルゴリズムである．その情報を基に $|\langle a|A|00\cdots0\rangle|$ の値が大きくなる A が見つけられたとき，確率振幅増幅がうまく働くのである．注意として，今までに示した式を見れば分かるように，解に関する知識がなく適当な確率分布で A を選んだ場合，質問回数の期待値は必ず Grover のアルゴリズムより増えてしまう．

最後にこのアルゴリズムがなぜ確率振幅増幅と呼ばれているかを示そう．問題をオラクルに関して古典的な質問しか受け付けない問題へと変えた場合，解を得る方法として以下のような単純なアルゴリズムが考えられる．まず，与えられた情報を基に量子状態 $A|00\cdots0\rangle$ を作る．この状態の観測結果として得られる数字をオラクルに質問して「1」を出力するかどうかをチェックする．これを「1」が得られるまで繰り返す．するとアルゴリズムが終わるまでに必要な質問回数の平均は $|\langle a|A|00\cdots0\rangle|^{-2}$ となる．他方，確率振幅増幅を用いたときの質問回数は上で述べたとおり $2|\langle a|A|00\cdots0\rangle|^{-1}/\pi$ であり，一般的な場合（絶対値の値が十分小さい場合）には後者の方がはるかに小さくなる．つまり，量子情報の入力を受け付けないオラクルから受け付けるオラクルへと問題設定を変更したときに，オラクル 1 回あたりの解を見つけられる確率を増幅させる一般的な処方箋をこのアルゴリズムは示しているために確率振幅増幅と呼ばれているのである．

オラクルの拡張による量子探索の応用

これまで，オラクルを，まったくのブラックボックスとして扱ってきた．見方を変えれば，ブラックボックスの実現方法によらず，量子探索アルゴリズムは動作することができる．たとえば，量子探索アルゴリズム中のオラクルへの質問部分を，他の量子アルゴリズムへのサブルーチンコールに置き換えることを考えると，これは，より複雑なアルゴリズムを構成することになる（**図 -3**）．本章では，拡張されたオラクルに対する量子探索アルゴリズムを通して，量子探索の応用例について述べる．

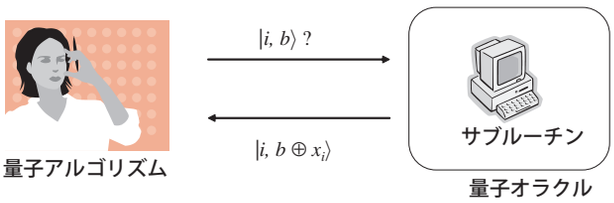


図 -3　オラクルの拡張

❒ 誤りのあるオラクル

前章までに紹介した量子探索アルゴリズムでは，オラクルは，質問に対して，常に正しい答えを出力することを前提としてきた．しかし，オラクルに誤りを許さない量子探索アルゴリズムでは，サブルーチンとして使えるのは，誤りのないアルゴリズムに限られてしまう．出力誤りのあるアルゴリズムをサブルーチンとして使えば，前章までのアルゴリズムは，その正しさにおいて，何の保証も与えてくれない．

Høyer らは，オラクルの出力誤りが量子的なもの☆1 に限定され，かつ，誤り率がたかだか定数（たとえば 1/3 未満）であるならば，量子探索アルゴリズムが必要とするオラクルへの質問回数は，出力誤りのないオラクルの場合と比べて，ほとんど変わらない（たかだか定数倍である）ことを具体的な量子探索アルゴリズムを与えることにより示した[3]．この事実により，（たとえば，量子探索アルゴリズムを再帰的に呼ぶなどといった）出力誤りのあるアルゴリズムをオラクルに使った多様な量子アルゴリズムを構築する道が開かれた．

❒ 量子探索の分散的な実現

オラクルに置き換わるサブルーチンは，その中で，通信が発生していてもよい．たとえば，量子計算機 A と量子計算機 B は，それぞれ，n ビット $\{x_1^A,\ldots,x_n^A\}$ および $\{x_1^B,\ldots,x_n^B\}$ を持っているとする．このとき，$x_i^A\wedge x_i^B$ であるようなインデックス i を探索する問題を考える．もし，「i 番目の値は？」という質問に対して，「$x_i^A\wedge x_i^B$」と答えてくれるオラクルが用意できれば，「n 個の変数の

☆1　量子的な出力誤りとは，たとえば，正しい出力が 1（$|\cdot\rangle$ 記号で書けば $|1\rangle$）であるにもかかわらず，オラクルが 0 と 1 の重ね合わせ（$\alpha|0\rangle+\beta|1\rangle$）を出力してしまう誤りのことである．このとき，$|\alpha|^2$ をオラクルの誤り率と呼ぶ．

中から 1 の値をとる変数のインデックスを探せ」という通常の探索問題に対するアルゴリズムを使って，高い確率で解くことができる．明らかに，このオラクルを実現するのに，質問 1 回につき，2 回のメッセージをやりとりすれば十分である．まったく同じアイディアが，量子のモデルについても当てはまる．このようにして，オラクルを分散的に実現することにより，量子探索アルゴリズムから，分散計算を行うプロトコルを構成することができる．このアイディアの一般化として，次の事実が知られている．$x \in \{0, 1\}^n$ と $y \in \{0, 1\}^n$ に依存するブール関数 $f(x, y)$ を計算するプロトコルを構成したい．ただし，x と y は，それぞれ，量子計算機 A と B に与えられるものとする．今，

$$f(x, y) = g(x \circ y)$$

と記述できるものと仮定する．ただし，$\circ$ は，ビットごとの任意の 2 項ブール演算を表す．このとき，g を計算する質問回数 T の量子アルゴリズム $\mathcal{A}_g$ があれば，f を計算する，$O(T \log n)$ の量子ビットを通信するプロトコル $\mathcal{P}_f$ を構成できる．なお，$\mathcal{P}_f$ の計算結果の誤り率は，$\mathcal{A}_g$ のそれに等しい．

上記は，オラクルを分散的に実現しているが，探索アルゴリズム自体は，分散的ではない．実は，オラクルに加えて，探索アルゴリズムも分散的に実現することは可能である．通常，探索アルゴリズムを分散的にすると，計算や通信のコストの点で，得にならない場合が多いが，必要に迫られる場合もある．たとえば，リーダ選挙問題と呼ばれる次のような問題を考える．n 台の計算機が(簡単のため)リング状にネットワーク接続されているものとする．各計算機には，変数 v を持ち，初期値は 0 である．問題の要請は，何らかの分散計算を行うことにより，ただ 1 台の計算機に対してだけ $v = 1$ と設定し，他の計算機については，$v = 0$ と設定する（**図 -4**）．各計算機がそれぞれ固有に識別子を持つ場合は，容易に解くことができるが，そうでない場合は，古典決定性計算では，解くことができないことがよく知られている．その理由は，各計算機がまったく同等で識別不可能な場合を考えると分かる．この場合，すべての計算機上で，まったく同じ決定性アルゴリズムが実行されるので，v の値は，すべての計算機に対して同じ値に設定されてしまい，リーダ選挙問題を解くことができない．Tani らは，量子計算機と量子通信が仮定できる場合に，確率振幅増幅を適用することにより，有限時間かつ誤りなし（量子版決定性）でこの問題を解いている [4]．ここでは，詳細には触れず，キーとなるアイディアだけ述べる．最初に，各計算機は，状態 $|0\rangle$ の量子ビットを用意し，状態 $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ に変換する．たとえば $n = 3$ の場合，分散システムには 3 量子ビット存在し，その状態は，$(|0\rangle + |1\rangle)^{\otimes 3}/\sqrt{2}$ となり，これは，Grover のアルゴリズムの具体例における $|\psi^{(1)}\rangle$ そのものである．アルゴリズムの基本的なアイディアは，$(|0\rangle + |1\rangle)^{\otimes n}/\sqrt{2}$ を構成する 2^n 個の基底状態のうち，ハミング重みが 1 であるような基底状態の振幅を増幅し，それ以外の基底状態の振幅を 0 にすることである(sin θ の値(上記の場合$\sqrt{n/2^n}$)が正確に分かる場合にのみこれが可能となることが知られている [2])．問題は，演算子 V と $\mathcal{O}$ の分散的な実現である．O については，各々の量子ビットをリングに沿って 1 周させれば，どの基底状態の係数を正負反転すればよいかは分かる．ただ，n 台の計算機のうち，1 台だけが代表して，反転操作を行うわけにはいかない．計算機同士は，識別不能で，皆同等だからである．すなわち，全計算機が同じ操作を行って，全体として正負反転を実現しなければならない．ポイントは，正負反転を，「係数に $e^{\pi i}$ を乗ずる」と考えることである．つまり，n 台の各計算機が $e^{\pi i/n}$ を乗ずる演算を実行すれば，全体として，正負反転を実現したことになる．V についても，同様である．

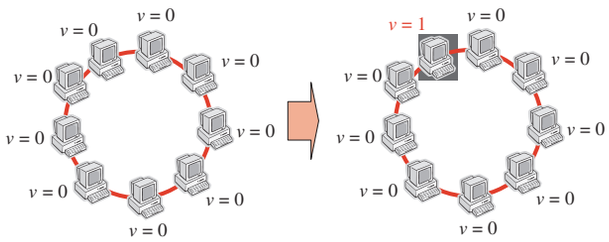


図 -4　リーダ選挙問題

このように，オラクルに加えて量子探索アルゴリズム自体も，分散化することが可能であり，またそれにより，新たな分散アルゴリズムを生み出すのである．

物理的な制約への対応

前章ではオラクルモデルの変化への対応，つまり問題設定の変化への対応であった．以下では，問題設定自体は変わらないものの実際の量子計算機を利用することによる物理的制約への対応を示す．

❒ 量子状態の初期化の困難性

そもそも，量子計算機というのは演算の実行そのものが非常に難しいが，特に状態を特定の状態に初期化するという制御は非常にエネルギーを要する作業である．というのも，量子計算機が扱う量子ビットを具体的な物で実現するわけだが，多くの場合，熱による状態の揺らぎは無視できないほどに大きい．しかし，この熱による揺らぎとは，状態がどこにあるのか分からないということを意味しており，通常の特定の演算子を単に実行する以

上に何らかの工夫が必要である．その工夫とは，量子計算機を構成する媒体に依存するわけだがどのような媒体であれ，非常に困難であり，多くの量子計算機の構成方法において，どのように初期化するかというのは量子計算機を実現するための大きな問題であり続けている．

これに対し，Biham らは初期化を行わなくても，オラクルへの質問を $O(\sqrt{n})$ 回行うことで，成功確率が $\Omega(1)$ となることを示した[5]．ただし，ここでいう成功確率とは，初期状態として適当な確率分布を仮定した場合のその確率分布に対する平均である．このような「現実的」仮定が散見されるのは，量子計算機の実態を意識した研究に見られる特徴と思われる．

❐ オラクル以外の演算コスト

ここまでは基本的にオラクルに何回質問したかという回数のオーダーをコストとしてきた．計算理論としての研究としては一番確固とした思考の基盤である．しかし，量子計算の実行に必要なコストというのは，オラクル以外の演算にもコストがかかる．しかし，そのコストは具体的演算の種類・量子計算機の実現方法によって非常に異なる．その一方で，一般論として将来実現するであろう（スケーラブルな）量子計算機の方法においては，多くの場合 1 量子ビットのみに作用する演算は 2 量子ビット以上に相関をもって作用する演算よりも，はるかに小さいコストで実現できると考えられている．

Grover のアルゴリズムを見ると，オラクルに質問するという操作以外の演算においても 2 量子ビット以上に相関をもって作用する演算を非常に多数必要としている．オラクル以外の演算において，複数の量子ビットに作用する演算を極力減らすことは，実際の計算時間を削減する上では一般的に効果的である．これに対し，Kato はオラクル以外に 2 量子ビット以上に作用する演算を使用しない量子回路で，オラクルに質問する回数が Grover の量子回路とオーダーが等しい回路でも，成功確率が $\Omega(1)$ とできることを示した[6]．

以下少し具体的に見てみよう．Grover のアルゴリズムを演算子の積であると見なした場合，$(H^{\otimes n}VH^{\otimes n}O)^m H^{\otimes n}$ と書けることは n 量子ビットにおける Grover のアルゴリズムで書いたとおりである．この中で演算子 V は量子ビット間の相関が非常に大きい演算であるため，スケーラブルな量子計算機において，この演算子の実行には非常に時間がかかることが一般的に予想される．そこで，$H^{\otimes n}VH^{\otimes n}$ を $S_x^{\otimes n}$ と置き換えることを考える（ただし，$S_x := \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$）．これはまさに，個々の量子ビットへの演算の集まりであり，非常に簡単に実行できると考えられている．このとき θ を n のに依存させて適当に選ぶと，

$(H^{\otimes n}VH^{\otimes n}O)^m H^{\otimes n}|00\cdots0\rangle$,

$(S_x^{\otimes n}O)^{m'} H^{\otimes n}|00\cdots0\rangle$

という 2 つの状態は非常に近い状態であることが示せる（m' は m に対して適宜選んだ数とする）．上の状態はまさに Grover のアルゴリズムによって生成される状態であり，下が実行時間を考慮して変形したアルゴリズムによって生成される状態である．状態が近いということはつまりは，下の状態においても正しい解が出力される確率が高くなることを意味している．

以上，オラクル以外の演算コストを考慮した変形を簡単に示した．このような研究は，量子計算機が実際に実現され量子探索を実行しようという場合の回路のチューニングにおいて，非常に有用である．

量子探索アルゴリズム研究の意義

以上，量子探索アルゴリズムの基礎理論と，情報・物理双方の立場からの発展的研究を見てきた．それぞれの研究の底流に流れているものは重ね合わせ状態の利用であり，これはまさに量子計算の本質である．この意味において，量子探索アルゴリズムの研究は「ある問題を解決するアルゴリズム」の研究であるにとどまらず，量子計算の本質を追及する研究でもある．

参考文献

1）Grover, L. K. : Quantum Mechanics Helps in Searching for a Needle in a Haystack, Phys. Rev. Lett., Vol.14, pp.325-328 (1997).
2）Brassard, G., Høyer, P., Mosca, M. and Tapp, A. : Quantum Amplitude Amplification and Estimation, Quantum Computation and Quantum Information : A Millenium Volume, Vol.305 of AMS Contemporary Math, Series, pp.53-74 (2003).
3）Høyer, P., Mosca, M. and de Wolf, R. : Quantum Search on Bounded-error Inputs, in Proceedings of 30th ICALP, Vol.2719 of LNCS, pp.291-299, Springer Verlag (2003).
4）Tani, S., Kobayashi, H. and Matsumoto, K. : Quantum Leader Election via Exact Amplitude Amplification, in Proceedings of ERATO Conference on Quantum Information Science, pp.11-12 (2005).
5）Biham, E., Biham, O., Biron, D., Grassl, M. and Lidar, D. A. : Grover's Quantum Search Algorithm for an Arbitrary Initial Amplitude Distribution, Phys. Rev. A, Vol.60, pp.2742-2745 (1999).
6）Kato, G. : Grover-algorithm-like Operator Using Only Single-qubit Gates Phys. Rev. A, Vol.72, pp.032319 (2005).

（平成 18 年 10 月 23 日受付）

加藤　豪
kato@theory.brl.ntt.co.jp
昭和 51 年生．平成 16 年東京大学大学院理学系研究科物理学専攻博士課程修了．同年日本電信電話（株）入社．量子計算，量子通信に関する研究に従事．理学博士．日本物理学会会員．

谷　誠一郎（正会員）
tani@theory.brl.ntt.co.jp
昭和 45 年生．平成 7 年東京大学大学院理学系研究科情報科学専攻修士課程修了．同年日本電信電話（株）入社．平成 16 年から 17 年にかけて科学技術振興機構（JST）ERATO 今井量子計算機構プロジェクト研究員兼任．平成 17 年から科学技術振興機構（JST）ERATO-SORST 量子情報システムアーキテクチャ研究員兼任．情報理工学博士．電子情報通信学会，IEEE，ACM 各会員．