素因数分解だけではない量子計算の魅力 ——量子探索技術の可能性を探る

量子コンピュータは，量子力学独特の性質を積極的に利用して計算を行うコンピュータです．実用レベルに達するには，まだ長い年月がかかるといわれていますが，現在のコンピュータでは解けない問題を，超高速に解くことが期待されています．本稿では，現在知られている量子アルゴリズムの中でも特に応用範囲が広いとされる量子探索を取り上げ，量子コンピュータの可能性について考えていきます．

たに　せいいちろう
谷　誠一郎

NTTコミュニケーション科学基礎研究所

量子アルゴリズムの必要性

英国の数学者Alan M. Turingにより計算機モデルが考案されて以来，コンピュータは著しい発展をとげました．現在のコンピュータも原理的にはTuringのモデルと同じです．現在のコンピュータばかりでなく，今後開発されるものも含め，このモデルに基づくコンピュータを「古典コンピュータ」と呼び，そのうえでの計算を「古典計算」と呼びます．

一方，「量子コンピュータ」は量子力学的な性質を積極的に利用した，Turingのモデルとは原理的に異なるコンピュータです（**表**）．このため，古典コンピュータでは解くことが難しい問題でも，高速に解くことが期待され，世界中で研究が進められています．量子コンピュータを動かすためには，現在のコンピュータと同様に，ハードウェアを動かす手順（アルゴリズム）が必要です．そして，アルゴリズムの善し悪しが計算速度を大きく左右することも，現在のコンピュータと同じです．このため，量子コンピュータのハードウェアが完成したとしても，それを用いて難しい問題を高速に解くためには，優れた量子アルゴリズムが欠かせません．

ShorとGroverによる高速量子アルゴリズム

量子アルゴリズムの代表例が，素因数分解を現在のコンピュータよりも指数倍高速に行う量子アルゴリズムです．これは，1994年にPeter W. Shor[(1)]によって発見されました．素因数分解は，長年の研究にもかかわらず，Turingのモデル上で高速に解く方法がいまだ見つかっていない難しい問題です．実際，インターネットなどで使用されているRSA暗号は，素因数分解の困難性を安全性の根拠としています．このため，Shorの発見は，量子コンピュータが完成したら，現在使用されている暗号が役に立たなくなるという意味でも非常に大きなインパクトがありました．

しかし，よく考えてみると，便利に使われている暗号が破られてしまうことは，うれしくないことです．専門的には，Shorの量子アルゴリズムの拡張もよく研究されており，素因数分解を含むもっと広範な問題群（隠れ部分群問題*）も高速に解けることが知られています．これらの量子アルゴリズムは，理論的には非常に重要ですが，現時点では，身近な問題との関連は薄く，そのメリットを理解するのは難しいかもしれません．

一方，Shorのアルゴリズムと並んで有名な量子探索アルゴリズム（量子探索）は，1996年にLov K. Grover[(2)]により発見されました．このアルゴリズムが解く探索問題とは，N個のデータの中から所望のデータを探す問題です．古典コンピュータであれば，最悪

表　古典コンピュータと量子コンピュータの比較

	古典コンピュータ	量子コンピュータ
情報の単位	ビット（bit）	量子ビット（qubit）
情報の数学表現	ブール値	複素ベクトル
基本演算	ブール演算 （AND, OR, NOT）	一次変換 （ユニタリ変換）
計算モデル	Turing 機械，論理回路	量子 Turing 機械，量子回路

＊隠れ部分群問題：数学の群論に関する問題．特別な場合として，素因数分解を解く際にキーとなる問題を含みます．

N回程度のデータアクセスが必要です．しかし，量子探索は，$\sqrt{N}$回程度のデータアクセスで済ますことができます．これは，素因数分解の場合のように指数倍のスピードアップではありませんが，それでもNが巨大であれば，著しいスピードアップにつながります．探索問題の最大の特徴は，問題設定の単純さと，それゆえの応用範囲の広さにあります．実際，探索問題は，さまざまな問題の部分問題として現れます．この部分問題を発見し，量子探索を適用することにより，元の問題を極めて高速に，効率良く解くことが期待できます．ただし多くの場合，探索問題を切り出すことは難しく，切り出せたとしても探索アルゴリズム自体にさまざまな工夫をこらす必要が出てきます．このため，Groverのアルゴリズムが発見されてから20年近く経た現在でも，量子探索のさまざまな改良や一般化が研究されています（**図1**）．

量子ビットと重合せ

量子コンピュータが扱う情報の単位を量子ビットと呼びます（**図2**）．1つの量子ビットで，「0または1」ばかりでなく，それらの重合せを表現することができます．同様に，2つの量子ビットでは，00, 01, 10, 11の重合せを表すことができ，さらにn個の量子ビットでは，0…0から1…1までの2^n通りのビット列の重合せを表すことができます．数学の言葉を使うと，次のようになります．0-軸と1-軸を持つ2次元複素ベクトル空間において，0-軸上の単位ベクトル$\vec{0}$が「0」を意味し，1-軸上の単位ベクトル$\vec{1}$が「1」を意味することとします．このとき，「0と1の重合せ」とは，これらのベクトルの合成$\alpha\vec{0}+\beta\vec{1}$のことです（係数$\alpha$，$\beta$は複素数）．同様に，n個の量子ビットは，$2^n$本の軸がある$2^n$次元複素ベクトル空間上のベクトルを表します．量子ビットはベクトルで

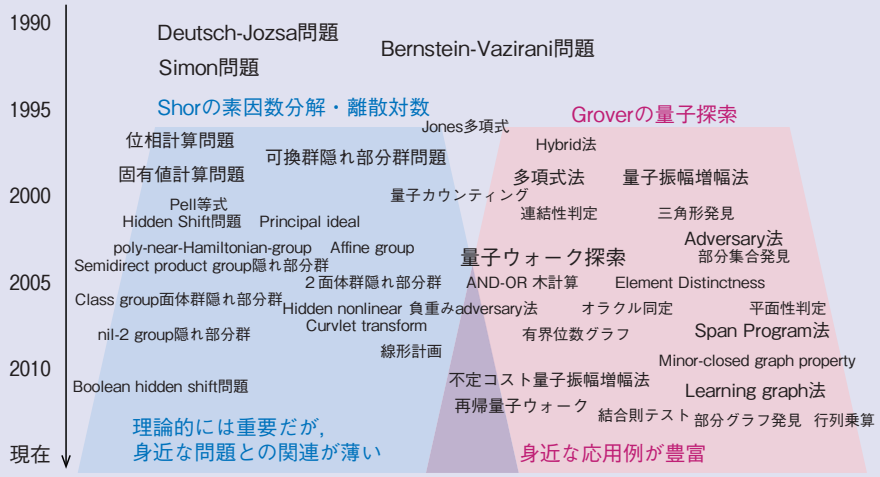


図1　量子アルゴリズム研究の流れ

	重合せ	数学表現
1量子ビット	{0, 1}の重合せ	2次元空間のベクトル
2量子ビット	{00, 01, 10, 11}の重合せ	4次元空間のベクトル
n量子ビット	{0…00, 0…01, …, 1…11}（2^n個のビット列）の重合せ	2^n次元空間のベクトル

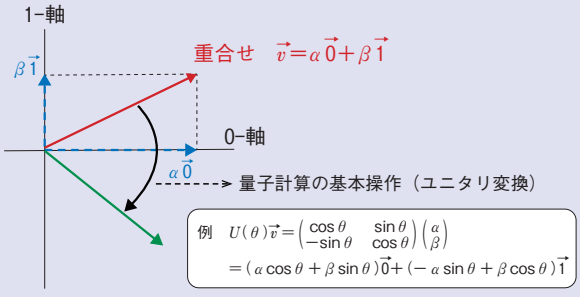


図2　量子ビットと重合せ

あったわけですから，量子ビット上の演算はベクトルに対する演算（ユニタリ変換[*1]）になります．

探索問題と量子アルゴリズム

探索問題に限らず，N個の入力データ$X_1,\cdots,X_N$に依存する問題を解く際には，入力データにアクセスしなければなりません．その際，形式的にはインデックスkでアクセスすると，入力データX_kが得られると考えられます．量子コンピュータでは，このインデックスを量子ビットで記述するので，重ね合わされたインデックスでアクセスし，それに対応して，重ね合わされた入力データを得ることができます．このような重合せによるデータアクセスを認めると，量子探索を次のように述べることができます（簡単のためデータの種類を0または1にしますが，本質的ではありません）．

定理（量子探索）：N個の入力データ$X_1,\cdots,X_N\in\{0,1\}$が与えられたときに，量子探索アルゴリズムは，$\sqrt{N}$回程度のデータアクセスにより，$X_i=1$であるインデックスiを高確率で見つけ出すことができる．

一般に，問題を解くために必要なステップ数は，このデータアクセス回数のほか，得られた入力データを処理するためのステップ数も考慮に入れなければなりません．しかし，探索問題を含め，本稿で扱う問題は，データアクセスのためのステップ数のほうが支配的なので，以下ではデータアクセス回数に着目します．

この定理の応用例としてグラフの平面性を判定する問題を考えてみましょう．

グラフの平面性判定

グラフの平面性とは，枝を交差させずに平面上にそのグラフを描画できる性質です（**図3**）．グラフが平面性を持つならば，一般のグラフでは計算困難な多くの問題を高速に解けることが分かっており，グラフの平面性を判定する問題は重要な問題としてよく知られています．さて，Gをn頂点からなる無向グラフ[*2]とします．問題の入力として，Gの頂点の各組(i,j)間に枝があるかどうかのデータが次のように与えられたとします

・各$i=1,\cdots,n$，各$j=1,\cdots,n$（ただし，$i<j$）に対して，(i,j)間に枝があれば$X_{ij}=1$，なければ$X_{ij}=0$（すなわち，X_{ij}はGの隣接行列[*3]の要素）．

問題は，この$\frac{1}{2}n(n-1)$個の入力データX_{ij}が表すグラフGの平面性を高確率で判定することです．探索問題を部分問題として切り出すために，キーとなるのは，18世紀にオイラーによって発見された基本的な定理です．

定理：n頂点からなるグラフが平面性を持つならば，枝の数は高々$3n-6$本である．

この定理を使って次のように問題を分割します（**図4**）．

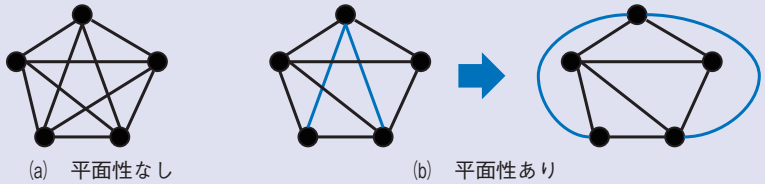
① $n(n-1)/2$個所の枝候補の中から，$3n-5$本の枝を特定する（グラフの枝の数が$3n-5$本よりも少ない場合は全枝を特定することになる）

② $3n-5$本の枝が見つかればオイラーの定理により平面性はない（$3n-5>3n-6$なので）

③ $3n-5$本未満の枝しか見つからなければ，それが全枝であるので，さらなるデータアクセスなしに，高速に平面性を判定

ここで入力データへのアクセスに関係しているのは①だけです．少し考えると，①を行うためには，1本の枝を探す探索問題を$3n-5$回解けば良いことが分かります．したがって，①の部分を量子で高速化できます．結果として，量子コンピュータでは$n^{1.5}$回程度のアクセスで十分であるのに対して，古典コンピュータではn^2回程度のアクセスが必要であることを我々は数学的に証明しました[(3)]．この例でのポイントは，グラフ理論の既存知識を用いることで初めて探索問題を切り出すことに成功した点です．量子で高速に判

枝を交差させずに平面上に描画可能な性質．
例：(a) は平面性がない．(b) は (a) から1本だけ枝を除いたグラフである．
この場合，矢印右の図のように描けるので，(b) は平面性がある．



(a) 平面性なし　　(b) 平面性あり

図3　グラフの平面性

＊1　ユニタリ変換：任意の2つのベクトルの内積を変えない線形変換．直感的には，2つのベクトルの角度とそれぞれの長さを変えない変換．
＊2　無向グラフ：向きを持たない枝からなるグラフ．
＊3　隣接行列：n頂点グラフGの隣接行列Aとは，n行n列の行列で，要素A［i,j］で頂点i，j間の枝の有無を表したもの．

定できるグラフの重要な性質は，ほかにも多数知られており，例えば，連結性*4の判定やハミルトンパス*5の存在判定などがあります．

量子探索の一般化

古典コンピュータ上で，ランダム抽出することを考えます．すなわち，入力データ$X_1,\cdots,X_N$の中からランダムに1つ選択してアセクスします．N個のデータの中に所望のデータがちょうど1つだけある場合，この方法の成功確率は，わずかにN分の1です．量子探索を大雑把に表現すると，このランダム抽出を「重合せ」で$\sqrt{N}$回程度繰り返していることと同じなのです．古典コンピュータでは，成功確率N分の1のランダム抽出をN回程度繰り返さないと，成功確率を1近くまで増幅できないわけですから，量子探索は，ランダム抽出の成功確率を，ずっと少ない繰り返し回数で，1近くにまで増幅しているとみることができます．この考え方を以下のように一般化できることが知られています．

定理（量子振幅増幅）：入力へのアクセス回数がcで，かつ，成功確率がpの古典アルゴリズムがあれば，アクセス回数が$c/\sqrt{p}$程度で，かつ，成功確率が1に近い量子アルゴリズムをつくることができる．さらに，pの値が正確に分かっていれば，成功確率を1にすることができる．

探索問題に対するランダム抽出の場合，$c=1$，$p=1/N$であるので，対応する量子アルゴリズムのアクセス回数は，$c/\sqrt{p}=\sqrt{N}$となります．つまり，特別な場合が，Groverの量子アルゴリズムになっています．直感的に，上記の定理は，元となる古典アルゴリズムを重合せで$1/\sqrt{p}$回程度繰り返すことで成功確率を1近くまで増幅できるといっています．同じアイデアを用いると，1台の量子コンピュータ上でのアルゴリズムだけでなく，複数の量子コンピュータからなる量子ネットワーク*6上での分散計算アルゴリズムなどにも適用することができます．

リーダ選挙問題

リーダ選挙問題とは，ネットワーク上のノードどうしで自律的にリーダを決定するという分散計算の本質的な問題です（**図5**）．この問題は，分散計算のさまざまな問題を解く際に，部分問題として出現します．しかしながら，各ノードが識別子をあらかじめ持っていることを仮定しない一般的な条件下において，古典通信（通常のビットの送受信）と古典計算では，有限時間内に確率1では解けないことが数学的に証明されています．ところが，量子計算と量子通信を使えば，有限時間内に確率1で解けることを我々は証明しました(4)．これは，量子計算と古典計算が質的に異なることを示しています．なお，この結果の最初の証明は，量子振幅増幅を用いていませんでしたが，後に量子振幅増幅を用いた別証明を与えました．以下にそのアイデアを述べます．

*4　連結性：任意の2頂点に対して，1本または複数の枝をたどることによって，一方の頂点から他方に到達できるようなグラフの性質．
*5　ハミルトンパス：グラフの枝をたどることによって，すべての頂点をちょうど1回だけ訪れることができるとき，その経路のことをハミルトンパスといいます．
*6　：量子ネットワーク上では，量子ビットを送受信する量子通信が行われます．量子通信は，光子に量子ビットを載せて光ファイバで通信することにより，すでに量子鍵配送で実用化されています．

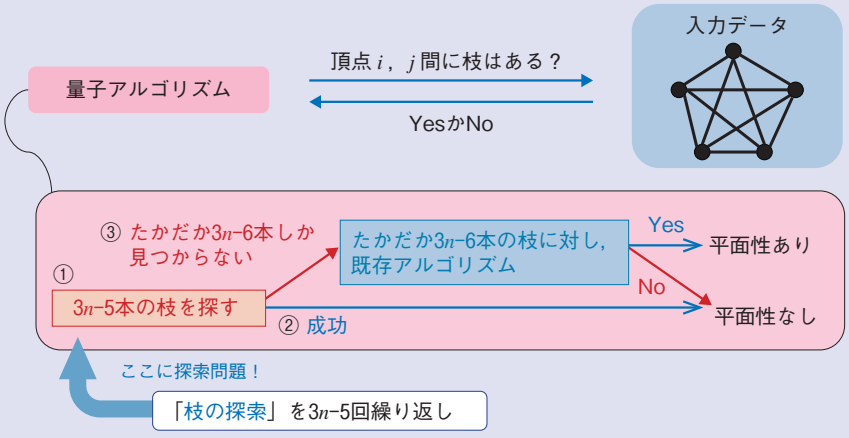


図4　グラフの平面性を判定する量子アルゴリズム

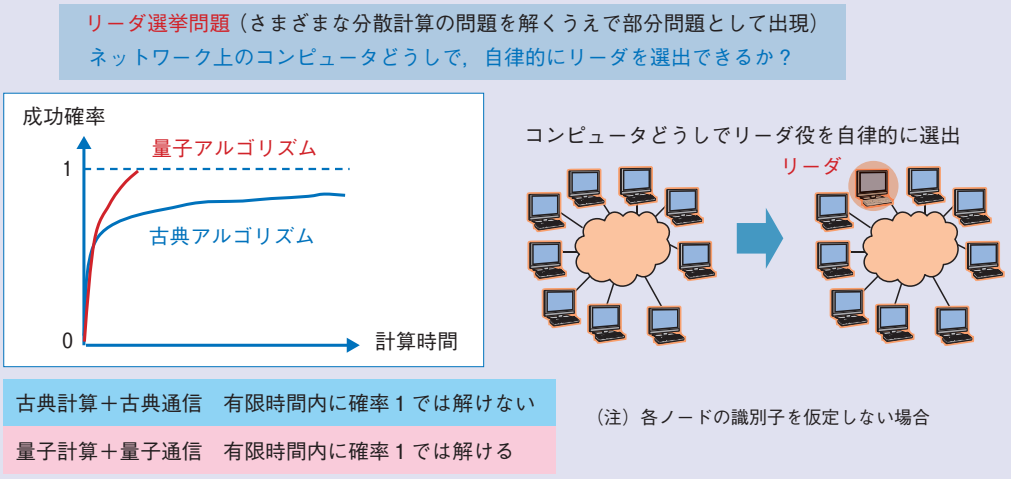


図５　リーダ選挙問題を解く量子アルゴリズム

まず最初に，次のような単純な古典アルゴリズムを考えます．①各ノードがコインを投げ，コインの表を出したノードがただ１つのときに，そのノードをリーダと決定する．②ノード数をnとすると，このアルゴリズムの成功確率は，$p=n/2^n$であることは簡単に分かる．③成功確率の値が正確に分かっているので，量子振幅増幅を使って，コイン投げを$1/\sqrt{p}=\sqrt{2^n/n}$回程度繰り返すことで成功確率を１にすることができる．

さらに，この①～③のアイデアを洗練させると，コイン投げはn回程度に減らすことができます．

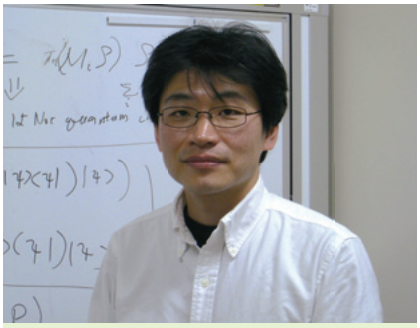
今後の展望

これまでの20年間の膨大な研究を通して，量子計算理論は高度に発展してきました．最近では，ランダムウォーク*7の量子版（量子ウォーク）や，ある種の半正定値計画法*8を基にした量子アルゴリズムなども盛んに研究され，数学や計算機科学のさまざまな分野との関連が知られるようになっています．また，アルゴリズムを量子回路に落とし込む部分の効率化に関する研究も着実に進歩しています(5)．しかし，未解明な問題は今なお数多くあり，まだまだ発展途上といえます．これらの問題を解決するためには，数学・物理・計算機科学の最新の知識を結集して，新たな技術を開発していく必要があるのです．

*7　ランダムウォーク：グラフの隣接頂点間を確率的に移動することにより，グラフの頂点をたどる確率モデル．
*8　半正定値計画法：半正定値行列を用いて記述できる，最適化手法の一種．線形計画法を特殊な場合として含みます．

■参考文献

(1) P. W. Shor: “Algorithms for quantum computation: Discrete logarithms and factoring,” Proc. FOCS1994, pp.124–134, Santa Fe, U.S.A., Nov. 1994.
(2) L. K. Grover: “A fast quantum mechanical algorithm for database search,” Proc. STOC1996, pp.212–219, Philadelphia, U.S.A., May 1996.
(3) A. Ambainis, K. Iwama, M. Nakanishi, H. Nishimura, R. Raymond, S. Tani, and S. Yamashita: “Quantum Query Complexity of Boolean Functions with Small On-Sets,” Lecture Notes in Computer Science, Vol. 5369, pp.907–918, 2008.
(4) S. Tani, H. Kobayashi, and K. Matsumoto: “Exact quantum algorithms for the leader election problem,” ACM Transactions on Computation Theory, Vol.4, No.1, pp.1-24, March 2012.
(5) Y. Takahashi and S. Tani: “Collapse of the Hierarchy of Constant-Depth Exact Quantum Circuits,” Proc. CCC2013, pp.168–178, Stanford, U.S.A., June 2013.



谷　誠一郎

私たちは，量子情報科学の研究をさらに推進し，量子コンピュータの能力を最大限に活かすことを目指します．

◆問い合わせ先
NTTコミュニケーション科学基礎研究所
メディア情報研究部
情報基礎理論研究グループ
TEL　046-240-3658
FAX　046-240-4709
E-mail　tani.seiichiro@lab.ntt.co.jp