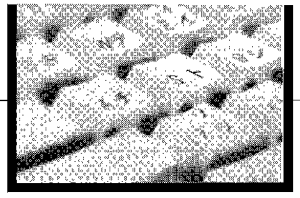


FRONTIERS

「量子計算機」の現状と今後

竹内 繁樹☆1

三菱電機（株）先端技術総合研究所
科学技術振興事業団　さきがけ研究21

量子計算機とは，「1」と「0」の重ね合わせ状態をとることができる「キュビット」を基本単位とする，まったく新しい概念の計算機である．もし実現すれば，因数分解などこれまでの計算機では桁数の増大に伴い計算時間が爆発的に増大するような問題を，桁数に比例する時間で解けることが発見され，注目を集めている．現在その実現に向けて，さまざまな量子計算機のアイディアが提案され，また，単一光子や溶液中の分子を用いた少数規模の量子計算が実際に行われるようになった．本稿では，それらの最新の提案や実験を紹介しながら，量子計算の現状と今後について考える．

最近の量子計算研究の展開

1994年，Shorは因数分解を高速に行う量子アルゴリズムを発見した．この発見によって量子計算は一躍脚光を浴びることになる．因数分解は一見簡単そうにみえるが，対象となる数の桁数の増大とともに計算時間が指数的に増大することが知られている．たとえば，200桁の数の因数分解には，現在最高速の計算機を用いたとしても，数十億年かかる．ところが，量子計算機を用いれば，おおざっぱな試算ではこれが数分で解けてしまうことになる．現在インターネットで使われている公開鍵暗号は，多数桁の因数分解が事実上解けないことを利用しているため，これが解けてしまうという発見は大きなインパクトがあった．その他にも，データベース検索を古典計算機にくらべて$1/\sqrt{N}$の時間で高速に行うアルゴリズムが発見されている．なぜ高速になるかは，本文中で簡単に述べる．

現在の計算機が，「0」または「1」のいずれかの状態をとる「ビット」を基本単位として用いるのに対して，量子計算機は「0」と「1」の重ね合わせ状態をとることができるような「キュビット（qubit, quantum bitの略）」を用いる．重ね合わせ状態とは，ミクロな粒子にみられる量子力学的な性質である．今，電子が1つだけ閉じ込められた箱を用意して，その箱の中央を「しきり」で仕切ったとする．古典力学においては，電子は仕切りの左の部分か右の部分のどちらか一方だけに存在するはずである．しかし，量子力学に従えば，電子はどちらに存在するか観測されるまで，左側，右側のそれぞれの状態の「重ね合わせ状態」として存在する．1985年にDeutschは，そのような量子力学の原理に基づく量子計算機を考案した．その後1992年にDeutsch自身らによって，未知のビット列の判定問題を現在の計算機よりも早く解く量子アルゴリズム（Deutsch-Jozsaアルゴリズム）が発見された．その発見がShorのアルゴリズムに結びつく．

当初は純粋に理論上の概念であった量子計算も，近年，量子の「重ね合わせ状態」を自由に制御する技術が開発され，現実のものとなりつつある．Shorの発見以降，量子計算の実現に向けて，さまざまな量子計算機のアイディアが提案され，また，光子や溶液中の分子を用いた少数規模の量子計算が実際に行われるようになっている．本稿では，まず現在の計算機と対応させながら，量子計算機の基本的な概念を説明する．次に，提案されている実現方法と量子計算実験を紹介し，最後に量子計算の今後の展開について考える．

量子計算機の基礎知識

たとえば「入力を2倍して出力する」という計算を考えよう．これは図-1のように，入力された2進列の最後に0を書き込めばよい．このよ

☆1 現在北海道大学電子科学研究所

うに，計算とはある2進列を別の2進列に置き換える「変換」と捉えることができる．通常の計算機では，「ビット列」に対してNOTやANDなどの「基本ゲート」を適当な順序で作用させることにより，任意の変換を実現する．そのような手順を図示したものが「回路」である．以下これらに相当する量子計算の概念である，「キュビット」「基本量子ゲート」および「量子回路」について説明する．また，提案されている量子計算機を評価する重要な指標として，「緩和時間」や「計算可能回数」にも触れる．

キュビット　古典計算機のビットに対応する概念がキュビットである．キュビットは，|0>と|1>の任意の重ね合わせ状態をとることができる．ここで，|0>，|1>と"|　>"で囲っているのは，これらが量子力学的な状態であることを示すためである．たとえば，あるキュビット|a>を考えると，それが|0>である場合は|a>＝|0>と表す．重ね合わせ状態のキュビットは，たとえば

$$|a\rangle = 1/\sqrt{3}\,|0\rangle + \sqrt{(2/3)}\,|1\rangle \qquad (1)$$

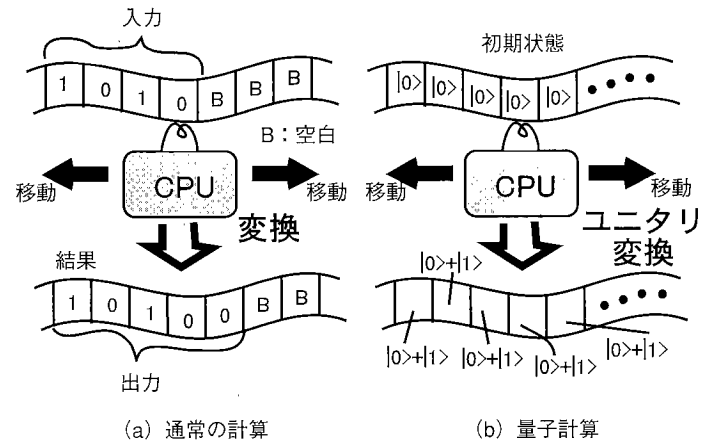
のように表される．|0>や|1>の前についている係数は「振幅」と呼ばれ，これらの自乗は，状態を観測したときに|0>または|1>である確率を与える．たとえば，式(1)のキュビット|a>を観測すると，3分の1の確率で|0>，3分の2の確率で|1>として見出される．一般には，それぞれの確率を足し合わせると1になる．

任意のキュビット|a>の状態は，

$$|a\rangle = \cos(\theta/2)\,|0\rangle + \exp(i\alpha)\sin(\theta/2)\,|1\rangle \qquad (2)$$

と表すことができる．ここで，iは虚数単位，θは|0>と|1>の重みづけに，αは位相に関するパラメータである．この位相αは，2つの状態の干渉を考える際に重要で，たとえば，(|0>＋|1>)/2と(|0>－|1>)/2の2つの状態を足し合わせると，それらの位相差による干渉の結果，|0>の状態だけが残る☆2．

式(2)で表されるキュビット|a>は，図-2に示されるような単位球面上の1点を指すベクトル(ブロッホベクトル)として表現すると便利である．この場合，|0>の状態は北極を指す，|1>の状態は南極を指すベクトルとして，また$(|0\rangle + |1\rangle)/\sqrt{2}$はXY平面上の1点を指すベクトルとして表される．位相は，XY平面内でのX軸からの角度に対応する．



(a) 通常の計算　　(b) 量子計算

図-1　通常の計算機と量子計算機：通常の計算機における計算とは，与えられたビット列を中央処理装置(CPU)が保持する一定の規則に従い別のビット列に書き換える「変換」である．同様に量子計算機における計算は，与えられたキュビットの列を別のキュビットの列に書き換える「ユニタリ変換」である．例では，最初|00000>であった状態が，|00000>(=|0>)から|11111>(=|31>)までの32通りの状態の一様な重ね合わせに変換されている．

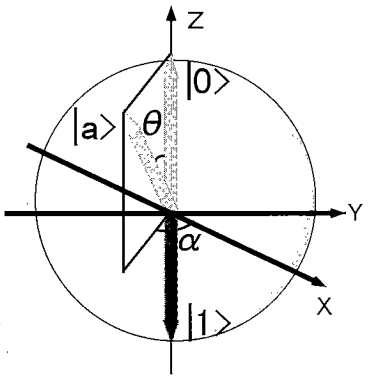
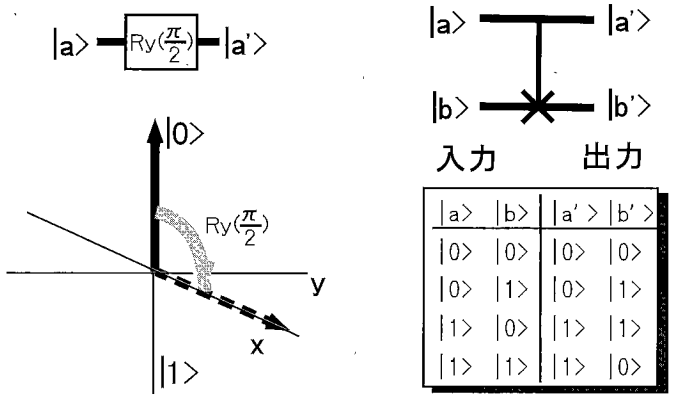


図-2　キュビット：|0>と|1>の任意の重ね合わせ状態をとることができる．単位球面上の1点を指すベクトル(ブロッホベクトル)として表すことができ，|0>と|1>の割合はθによって，また|0>と|1>の間の位相はαによって定められる．

基本量子ゲートと量子回路　Deutschらによって，次の2つの基本ゲートをキュビットに作用させることで，任意の量子回路を構成できることが明らかにされている(図-3)．1つ目は，回転ゲートと呼ばれ，通常の計算機のNOTゲートに対応する．これは，1つのキュビットに対して作用し，キュビットのパラメータθや位相αを，ある特定の値変化させる．キュビットをブロッホベクトルで表現した場合，回転ゲー

☆2 $1/\sqrt{2}\,(1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle) + 1/\sqrt{2}\,(1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle) = |0\rangle$．それぞれの括弧に係数$1/\sqrt{2}$がついているのは，もともと1つの量子が，括弧で表されるそれぞれの状態を同じ割合でとっているため．



(a) 回転ゲート　　(b) 制御ノット

図-3 基本量子ゲート：回転ゲートはキュビットをある方向に一定角度回転する操作である．180度θを回転する回転ゲートは，通常のNOTに対応する．制御ノットは，通常の排他的論理和に相当する．これらは，|0>と|1>の「重ね合わせ状態」を入出力できる点に注意．

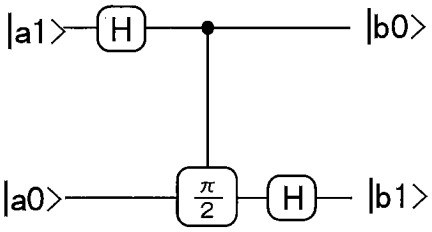


図-4 2キュビットの離散フーリエ変換の量子回路：|a1>|a0>で表される状態を|a>，|b1>|b0>を|b>とすると，この回路は|a>→Σ_{a,b} exp(2πi a b/4) |b>へと変換する．図中，H は図-3における Ry(π/2) を，π/2 は，制御キュビットが1のときのみ信号キュビットの位相をπ/2変化させるようなゲートを表している．

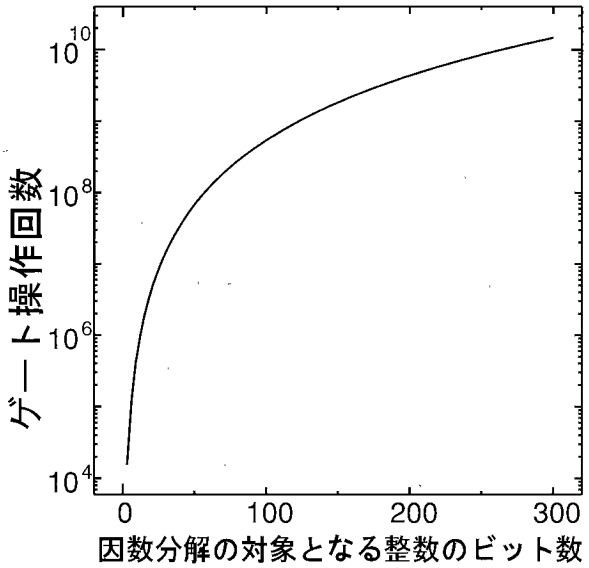


図-5 因数分解に必要な計算ステップ数．

トの働きはベクトルをある方向へ一定角度回転させることに相当する．たとえばθを180度回転させる回転ゲートは，NOTゲートと類似している．

もう1つは制御ノットと呼ばれる．これは，2つのキュビットに対するゲートである．便宜上，一方を制御ビット，他方を信号ビットと呼ぶと，制御ビットが|0>のときには信号ビットは変化を受けないが，制御ビットが|1>のときのみ信号ビットの|0>と|1>が入れ替えられる．図-3において，入力|a>，|b>および出力|b'>に注目すると，排他的論理和(exclusive-or)と類似している．ただし，入出力に「重ね合わせ状態」を許す点が大きく異なる．

適当な物理的なキュビットの列に対して，これらの基本量子ゲートを構築することさえできれば，量子計算を実現できる．ここで量子回路の一例として，2キュビットの離散フーリエ変換を行う量子回路を図-4に示す．ここで注意するのは，量子回路が実際の配線図を示しているのではなく，キュビットの列に対する操作手順を示していることである．たとえば後述するイオントラップ量子計算機では，量子回路はイオンにどのような手順でレーザーを照射すればよいかを表している．

図-4の回路では，2ビットから2ビットへの離散フーリエ変換を3回の操作で実現している．同様にして，NビットからNビットへの離散フーリエ変換を，N (N+1)/2回程度の操作で2^N通りの入力に対して一度に実行することができる．このフーリエ変換を直接計算すると2^{2N}回程度の計算が必要になることを考えれば，量子計算によるフーリエ変換は圧倒的に速いことが分かる．この量子高速フーリエ変換は，Shorの因数分解アルゴリズムの鍵になっている．このように量子計算が高速なのは，2^Nの大きさの状態空間に対する演算を，N個のキュビットに対する少数個の量子ゲートの組合せで実現できるからである．

緩和時間，ゲート時間と計算可能回数

このように，キュビットに対して前述の量子ゲートを実現することができれば，量子計算が原理的には可能になる．しかし，実際の物理系で量子計算を実現するにはいくつかの問題とそ

れに関する指標が存在する．

まず重要な指標が「緩和時間」である．量子計算では重ね合わせ状態を用いて計算を行うため，計算の間はその状態が保たれている必要がある．しかし，実際の物理系においては，重ね合わせ状態は一定の時間しか保つことができない．この重ね合わせ状態が保たれている時間を緩和時間と呼ぶ．多数のキュビットを用いる場合には，重ね合わせの崩れる要因が増えるため，緩和時間はさらに短くなる．単独のキュビットの緩和時間（τ）は，それを用いる量子計算機の計算時間の上限を与える．

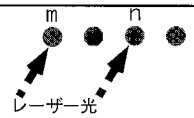
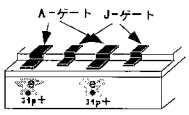
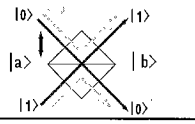
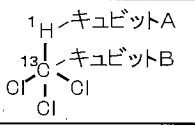
方式	概念図	キュビット	緩和時間，計算可能回数 実験現状
イオントラップ		イオンの電子準位	10^8(s), 10^{13} 制御ノット
シリコン		シリコン中に埋め込まれたリン，イオンの核スピン	10^6(s), 10^{12} アイディアのみ
線形光学素子		光子の光路および偏光	10^{-4}(s), 10^6 3キュビットのアルゴリズム実現
NMR		^{1}H，^{13}Cなどの核スピン	10^2(s), 10^5 3キュビットのアルゴリズム実現

表-1 提案されている量子計算機の一覧．

先に述べた量子ゲート操作は，実際にはレーザーの照射などで，一定時間を必要とする．これがゲート時間（Tg）である．たとえば，因数分解可能な数の桁数は，キュビットにゲート操作を何度行えるかによって決まる．これを計算可能回数（Nmax）と呼ぶ．単純には，Nmaxはτ/Tgで見積もることができる．現在の計算機を超える量子計算機の実現を目指す場合，最も重要なのはこの計算可能回数である．

図-5に，因数分解アルゴリズムを実行するのに必要な物理的な回数のグラフを示す[1]．この操作回数はほぼ必要な計算可能回数とみなすことができる．この図から，たとえば今の計算機では事実上解けないとされる200ビットの整数を因数分解するには，約10^{10}の計算回数が必要であること，それよりさらに入力ビット数が増大しても，必要なステップ数はそれほど増えないことが分かる．10^{10}の計算可能回数を実現するには，ゲート時間を10^{-12}秒としても，最低でも10^{-2}秒以上の緩和時間が必要になる．このように，キュビットが長い緩和時間を持つように物理系を選定，構築することが非常に重要である．

量子計算機のアイディア

重ね合わせ状態をとることが可能な量子力学的な状態は，すべてキュビットとしての候補になり得る．これまで，電子やイオン，核スピン，光子の偏光やモードなど，さまざまなキュビットを候補とする量子計算機が提案されている．また，単一光子や溶液中の分子を用いた少数規模の量子計算が実際に行われるようになった．ここでは**表-1**に挙げたそれらのうちの一部について，簡単に仕組みを紹介する．なお，諸提案のより詳しい動作原理については，文献2)を参照してほしい．

イオントラップ量子計算機　長い緩和時間を人工的に作り出す手段として，イオントラップがある．これは，電磁ポテンシャルによってイオンを真空中に浮かせることにより，外界との相互作用を裁ち切り，長い緩和時間を実現する．1995年にZurekらにより，直線上にトラップしたイオンの電子状態をキュビットとし，それらにレーザー光を照射することでゲート操作を行う量子計算機が提案された[3]．その後，単一イオンを用いた制御ノット実験が行われている．

この提案は，予想される計算可能回数が10^{13}回と大きいため，現在の計算機を凌駕する量子計算機の有力候補の1つである．現在NIST，ロスアラモス国立研究所などで複数のキュビットを用いた量子計算機の実現を目指している．しかし，キュビットの数が増えた場合にいかに系全体を安定に保つかが課題で，今のところイオン2つによる量子ゲート実験には成功していない．

シリコン量子計算機　諸提案の中でも，現在のシリコンチップによる計算機に最も近いのが，シリコン中にドープされたリン原子の核スピンをキュビットとして用いるアイディアである[4]．この提案の鍵は，リン原子を埋め込む基板には，「核スピンを持たないシリコン同位体（^{28}Si, ^{30}Si）」だけを用いる点である．こうすることでリン原子の核スピンは，回りに相互作用す

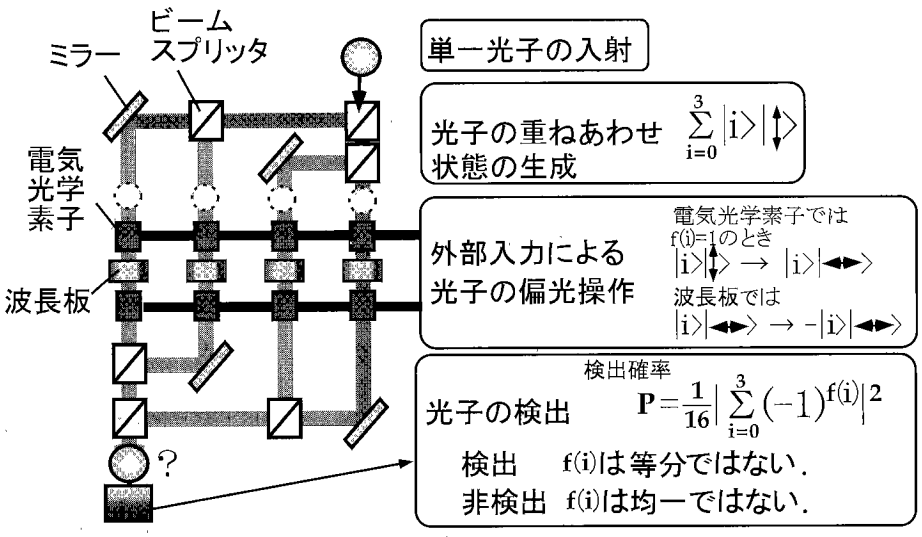


図-6 4ビットの「0」「1」列を判別する線形光学素子量子計算機．4桁の2進数を電気光学素子への電圧として計算機に与えておき，その後，入力ポートから縦偏光の単一光子を入射する．出力ポートに設置された検出機が光子を検出すると，「0」と「1」の数が同数（等分）ではなかったことが，検出しなければ，すべて0やすべて1の状態（均一）ではなかったことが一度の実験で分かる．

る相手のいない，いわば真空中に隔離されたのと同じような状態になる．この工夫によって，絶対温度0.1度に冷却した場合10^6秒程度の緩和時間が達成できると考えられている．この長い緩和時間の結果，予想される計算可能回数は，10^{12}が予想されている．回転ゲートや制御ノットの操作は，リン原子の上部や間に設けられた電極に電圧をかけながら，電磁波を照射することによって行う．

このアイディアは，キュビットの数が増大した場合も装置が複雑にならずに済む点も大変魅力的である．しかし，この構造の実現には，現在の半導体加工技術にさらに進展が求められる．ほかに固体素子で量子計算を実現するアイディアとして，超伝導トンネル接合を用いるもの，電子スピンを用いるものなどが提案されている．

線形光学素子量子計算　この方法は，既存の線形光学素子を用いて，量子計算の回路を組み立てるものである[5]．キュビットとしては，単一光子の偏光や光路を用いる．それに対するゲート操作は，ビームスプリッタや偏光回転板といった，線形光学素子によって行う．この方法で任意の量子計算の実験を行うことができることが分かっている．**図-6**に3キュビットのDeutsch-Jozsaアルゴリズムを実現した例を示す．

注意を要するのは，この方法では，N個のキュビットで記述されるアルゴリズムを実行するには，2のN乗個の光路が必要になるという点である．そのため，たとえば200ビットの数の因数分解などは，必要な光路の数が2^{200}乗と莫大になってしまい，実現不可能である．しかし，この方法は，単一の量子計算の出力など，後述の核磁気共鳴量子計算では検証できない実験を行うことができる．10キュビット程度までで記述されたアルゴリズムを実験的に調べる有力な試験台として，相補的に用いられていくと思われる．

核磁気共鳴量子計算　核磁気共鳴（NMR）法は，大きな磁場の印加されている状態で，物質中の原子核スピンを高周波電磁波を用いて制御，測定する方法で，材料分析や医療診断に広く応用されている技術である．NMR量子計算では，適当な溶媒に溶かし込まれた，10^{20}個程度の分子1つ1つが「量子計算機」として働く[6]．

キュビットとしては，分子中の原子核の核スピンを用いる．核スピンが磁場と同じ方向を向いている状態を$|0\rangle$，反対方向の状態を$|1\rangle$とする．核スピンに対するゲート操作は，適当な高周波パルスを試料に印加することにより行う．核スピンの状態の読み出しは，逆に試料から発生される電磁波を，コイルでピックアップすることで行う．その結果は溶液中のすべての分子の平均値で与えられるため，いわば，10^{20}回の量子計算の結果の平均値を読み出すことになる．

核磁気共鳴量子計算機は量子計算のテストベッドの主力として用いられ，現在3キュビットの計算が実現されている．ただし，大量の量子計算の平均値しか与えられないため，NMR量子計算での検証には向かない量子計算アルゴリズムや仕組みも存在する．現状技術では，キュ

ビットの増大と共にS/Nが指数的に減少するため，10キュビット程度が限界だと考えられている．

量子計算機の今後

以上，本稿では現在提案されている量子計算機を概覧した．最後に簡単に，本文で触れられなかった最近の理論面の進展，および量子計算機の今後の展開について触れる．理論的な展開についてのより詳しい内容は，文献7)～9)を参照してほしい．

理論的な展開　当初，量子計算の実現に対して，いくつかの本質的な疑念が呈された．1つはエラー蓄積の問題である．ディジタル計算機では，微小なエラーが存在してもしきい値を超えない限りはその都度消去され，蓄積することがない．一方，量子計算では，位相や振幅などの連続量を扱うため，そのままではエラーが蓄積してしまうことが指摘されていた．しかし，Shorらによる量子誤り訂正符号の発見により，このエラーを訂正可能であることが示された．この方法では，5つの実キュビットの組合せで1つの論理キュビットを構成する．実キュビットのうち1つにエラーが生じた場合は，それを検出し，訂正することができる．このように，量子計算の実現に対する本質的な疑問は，理論的には解決しつつある．

量子計算を他の並列計算のアイディアと比較した場合，最も大きな違いは，計算要素の数，すなわちキュビットの数に対して指数的に大きな計算レジスタを確保できることであろう．量子計算によってどのような計算が効率的に解けるかの研究も活発に行われている．量子計算によってNP完全問題を解けるかどうかは，まだ分かっていない．

ところで，「量子力学は確率の学問だから，量子計算機は確率的にしか正しい答えを与えないのではないか」という質問をいただくことがある．これに対する答えはノーである．量子計算の中で行われる「変換」とそれに伴って変換されたキュビットの状態は一意に定まっており，常に正しい答えが得られるアルゴリズムも設計可能である．

量子計算の実現に向けて　最後に，量子計算機の今後の展開を考える．いつ頃どのような形で，現在の計算機を上回る性能を持つ量子計算機は実現するのだろうか．本文で述べたように，量子計算機が現在の計算機を上回るための目標スペックは，1000個のキュビットに対して，10^{10}回のゲート操作が実行可能であることである．

事実上1994年に始まった実験的な研究からわずか5年で，3キュビットのアルゴリズム実験がNMR量子計算機と線形光学素子量子計算機によって実現している．これらの方法による10キュビット程度の量子計算は，10年を待たずに実現するだろう．今後は，これらの計算機による量子計算アルゴリズムや誤り訂正の実験的な検証を通じて，実現に向けた問題点の抽出や理論へのフィードバックがなされるだろう．

現在提案されている方法の中で，将来そのスペックを達成可能かもしれないのは，イオントラップ量子計算機とシリコン量子計算機である．特にシリコン量子計算機は，基本的な2キュビットのゲート操作が実現した場合，それを2から10へ，10から1000へと集積化することは，それほど困難ではないかもしれない．

また，これらの提案はここ数年に出されたものである．この1年の間にも，格子状に干渉させたレーザー光で閉じ込め中性イオンを用いるアイディアや，結晶中の核スピンを用いるアイディアなど，次々と新しいアイディアが提案されている．今後も活発な提案が引き続き行われることは間違いない．量子計算機の研究は，これらのさまざまな提案のそれぞれが抱える問題点を1つ1つ解決しながら，同時により良い方式が探求される段階にあると思われる．

謝辞　本稿にコメントを寄せてくださった，三菱電機先端技術総合研究所の山田訓氏，同産業システム研究所の吉田実氏に感謝します．

参考文献
1) Hughes, R.J., James, D.F., Knill, H.J., Laflamme, R. and Petschek, A.G.: Phys. Rev. Lett., Vol.77, p.3240 (1996).
2) 竹内繁樹: 21世紀，量子猫は計算をするか？，日本物理学会誌, Vol.54, No.4, pp.263-273 (1999).
3) Cirac, J.I. and Zoller, P.: Phys. Rev. Lett., Vol.74, No.20, p.4091 (1995).
4) Kane, B.E.: A Silicon-based Nuclear Spin Quantum Computer, Nature, Vol.393, p.133 (1998).
5) 竹内繁樹: 電子情報通信学会論文誌 A, Vol.J81-A, No.12, p.1644 (1998).
6) Chuang, I.L., Vandersypen, L.M.K., Zhou, X., Leung, D W. and Lloyd, S.: Nature, Vol.393, p.143 (1998).
7) 西野哲朗: 量子コンピュータ入門，東京電機大学出版局，東京 (1997).
8) 大矢雅則: 量子コンピュータの数理，丸善(株)，東京 (1999).
9) 数理科学「特集　量子コンピューター」, Vol.424, 10月号 (1998).

(平成11年8月30日受付)