

## はじめに

量子アルゴリズムとは、量子力学の原理を使って問題を解く方法である。アルゴリズムは、主に計算機科学で使われており、線形計画法や動的計画法、分岐限定法、局所探索、近似アルゴリズム、ヒューリスティック探索での焼きなまし法、進化的アルゴリズム、群知能などがあった。しかし、ここでは、量子力学という物理を使って、今まで計算が難しかった問題を少ない計算量で解けるアルゴリズムを説明する。

たとえば、量子アルゴリズムがいかに強力かをコイン投げを例にして説明しよう。コイン投げで遊ぶときに、コインが本物か偽物（絵柄が異なるか同じ）かを調べるのに、表と裏の絵柄が異なるか1回ずつ（合計2回）調べる必要があるが、量子アルゴリズムが使えると、どちらかの面を1回見ただけでコインが本物か偽物かを判定できる。この量子アルゴリズムを最初に考えたのは、オックスフォード大学のデイビッド・ドイチ (David Deutsch) で、私がオックスフォード大学にいたときに、隣の部屋にいたようであったが、ドイチ問題として世界で始めて1995年に考案された有名な量子アルゴリズムである。私は、40年ほど前の学生時代に量子力学を勉強したが、問題を解くための計算に使えるとは夢にも思っていなかった。これは、量子状態を使うと、コインの表と裏を同時に調べることができるという量子並列処理の基本原則を使っている。また、関数式に  $n$  個の未知数があるときには、必ず  $n$  個の式が必要であるとか、関数を  $n$  回調べる必要があると学校で習ったが、これは間違いである。量子アルゴリズムでは  $n$  個の未知数があっても関数を1回調べれば、 $n$  個の未知数がすべて求まる。

計算には、現在あるコンピュータで十分ではないかと思われるかもしれないが、従来のコンピュータは、VLSI と呼ばれる集積回路を用いており、その集積度を上げて計算速度を向上させている。さらに、計算高速化のために、コンピュータを葡萄の房のように束ねたクラスター型計算機や電源コンセントから電力資源を取り出すようにネットワーク・コンセントから計算資源を取り出すグリッ

ド・コンピューティング技術による分散並列処理が行われている。インテルの共同創立者であるゴードン・ムーア (Gordan Moore) が 1965 年に予言した「ムーアの経験的法則」によれば、マイクロプロセッサの処理速度は 1 年半ごとに 2 倍になるといわれており、約 40 年間実際にはほぼその通りに開発されている。しかし、この高速化も現在限界に近づいており、マルチコア化によって高速化を図っているが、集積化に大きな問題が発生していると思われる。つまり、VLSI 方式での集積度が今限界に来ており、あと 10~20 年で 1 ビットあたりの原子数が数個の原子レベルに近づいている。また、VLSI の小型化により発熱量もますます増加し、問題となってきている。そのために、もっと高速なコンピュータが必要となるときには、原子レベルでの新しい計算モデルが必要となってきている。

さらに、現在のインターネットでの暗号システムは大きな数字の因数分解の難しさを利用して成り立っているが、量子コンピュータを使えば容易に関数の周期を求めることができ、それを利用して因数分解が容易になるため、インターネットの安全性が危惧される。また、データベース探索が高速になったりする量子アルゴリズムが考案されたり、量子状態を離れたところへ転送する量子テレポーテーションやディコヒーレンスと呼ばれるノイズによって乱される量子状態を修正する量子誤り補正の考え方も出され、より解読されにくい量子暗号も、新しく考案されてきている。一方、この量子コンピュータを実現する方法として、私がオックスフォード大学で行っていた線形イオントラップによる量子コンピュータ実験や光フォント、核磁気共鳴 NMR、量子ドットなどの実験が進められている。

量子アルゴリズムの学習には、物理の量子力学や数学の線形代数、情報工学、計算機工学、電子工学などの基礎が必要であるが、ここでは、それらの一部の知識がなくても、理工学系の学部の講義テキストに利用できることを念頭に作成したので、数学的な厳密さに固守しないで、コインの問題のように非常に直感的にわかりやすく解説した。また、量子アルゴリズムを実際に解くために、Matlab や Mathematica, Java のコード (プログラムそのものの説明は他書を参考にされたい) を随時入れて解説しているので、シミュレーションして確かめることができる。

量子コンピュータに特有な量子アルゴリズムは、新しく出現した分野であり、従来の計算やプログラムでの考え方を、大きく変換させている。これからの情報技術者は、このような量子アルゴリズムのための新しいプログラミング手法を開発することが必要になるかもしれない。いろいろな量子コンピュータの本を読ま

れて、分からなかったことが「この本でやっと分かった!」とさせていただけることが著者の本望である。

2014 年 4 月鹿児島にて

中山 茂

## 量子アルゴリズムでよく出てくる 重要な2つの基本公式の意味を理解しよう

### 【量子アルゴリズム公式1(量子フーリエ変換とアダマール変換)】

$n$  キュービット ( $N=2^n$ ) に対しての量子フーリエ変換は、つぎようになる。

$$|x\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{x \cdot y} |y\rangle \quad \omega = e^{\frac{2\pi i}{N}} \quad |x\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{x \cdot y} |y\rangle$$

これは  $N=2$  のとき、 $\omega = e^{i\pi} = -1$  となり、つぎのようなアダマール変換公式となる。

$$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{x \cdot y} |y\rangle \quad |x\rangle \xrightarrow{H} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{x \cdot y} |y\rangle$$

とくに、量子ビットが  $n=1$  ( $N=2$ ) のとき、つぎのようなアダマール変換となる。

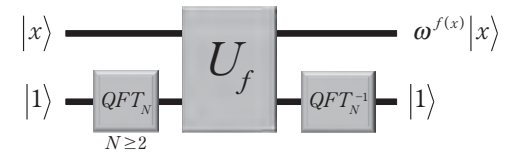
$$|x\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + (-1)^x |1\rangle) = \frac{1}{\sqrt{2}} \sum_{y=0}^1 (-1)^{x \cdot y} |y\rangle$$

### 【量子アルゴリズム公式2(Phase Kickback)】

つぎのような量子オラクルに通せば、関数  $f(x)$  に関する情報が位相項に含まれていることになる。

$$|x\rangle |1\rangle \xrightarrow{I^{\otimes QFT_N}} \frac{|x\rangle}{\sqrt{N}} \sum_{n=0}^{N-1} \omega^n |n\rangle \xrightarrow{U_f} \frac{|x\rangle}{\sqrt{N}} \sum_{n=0}^{N-1} \omega^n |n \oplus f(x)\rangle \xrightarrow{I^{\otimes QFT_N^{-1}}} \omega^{f(x)} |x\rangle |1\rangle$$

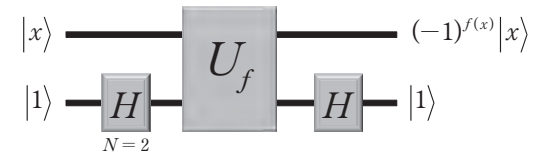
量子アルゴリズム公式2(Phase Kickback)



ここで、 $N=2$  のとき、 $\omega = e^{i\pi} = -1$  となり、

$$|x\rangle |1\rangle \xrightarrow{I^{\otimes H}} \frac{|x\rangle}{\sqrt{2}} (|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{|x\rangle}{\sqrt{2}} (|f(x)\rangle - |\overline{f(x)}\rangle) \xrightarrow{I^{\otimes H}} (-1)^{f(x)} |x\rangle |1\rangle$$

量子アルゴリズム公式2(Phase Kickback)



## 第 1 章

# 量子コンピュータの 基礎

ここでは、量子コンピュータの基礎的な考え方を説明しよう。なぜ量子コンピュータが古典的コンピュータよりも高速計算が可能なのか？ 0と1との重ね合わせとは何なのか？ 量子ビットはなぜコピーできないのか？

## 1.1 古典的コンピュータから量子コンピュータへ

### 1.1.1 古典的コンピュータの発展

1946年に、真空管を用いて世界で初めてのコンピュータが米国のペンシルバニア大学で開発された。J.P.EckertとJ.W.Mauchlyが中心となり、米軍の砲弾軌道計算のために、ENIAC(エニアック, Electric Numerical Integrater and Calculator)を開発した。このコンピュータは、平和的利用として天気予報にも利用された。しかし、このコンピュータは、配線によってプログラムされていたために、計算内容を変更するときには、多くの配線を接続しなおす必要があった。そこで、1948年にプリンストン大学のフォン・ノイマン(J.von Neumann)は、コンピュータのメモリ中にプログラムをソフトウェアとして内蔵させることを提案し、1949年に世界で初めてのプログラム内蔵方式のコンピュータEDSAC(エドサック, Electronic Delay Storage Automatic Calculator)が、M.V.Wilkesによって英国ケンブリッジ大学で開発された。これは、発案者フォン・ノイマンの名前をとって、ノイマン型コンピュータと呼ばれる。これが第1世代のコンピュータであった。

第2世代のコンピュータは、1947年にトランジスタが発明され、真空管を使わないトランジスタ方式のコンピュータであった。最初のトランジスタ方式コンピュータETL MARK IIIが、1956年に電子技術総合研究所で開発され、1959年にIBMは、トランジスタ方式コンピュータIBM7070を発売した。第3世代のコンピュータは、トランジスタが集積回路IC化されたためにIC方式のコンピュータとなり、1964年に最初のIC方式コンピュータIBM360がIBMによって開発された。

第4世代のコンピュータは、VLSI方式のコンピュータで、1970年にIBMによってIBM370が開発された。第5世代のコンピュータは、並列処理が可能で人工知能を盛り込んだ非ノイマン型のコンピュータが開発された。また、計算速度の高速化において、クラスタ型計算機やグリッド・コンピューティング技術を用いて、分散並列処理、CPUのマルチコア化でチップ並列性やチップ内並列性が行われている。ソフトウェアでは、最適化コンパイラや並列・分散アルゴリズムが考案されている。

つまり、従来のコンピュータは、VLSIの集積回路を用いており、その集積度

を上げて計算速度を向上させ、さらに、計算速度の高速化のために、コンピュータを葡萄の房(クラスタ)のように束ねたクラスタ型計算機や電源コンセントから電力資源を取り出すようにネットワーク・コンセントから計算資源を取り出すグリッド・コンピューティング技術による分散並列処理が行われている。実用的には、 $2^n - 1$ が素数であるメルセンヌ素数を発見するためのユーザ参加型の分散コンピューティングによるGIMPS(Great Internet Mersenne Prime Search)プロジェクトが有名で、これにより多くの**完全数**(その数がそれ自身の数を除く約数の和と等しい自然数で、 $6=1+2+3$ ,  $28=1+2+4+7+14$ ,  $496$ )も発見されている。

ゴードン・ムーア(Gordon E. Moore)が1960年代に予言した「ムーアの経験的法則」によれば、マイクロプロセッサの演算速度は1年半ごとに2倍になるといわれており、十数年前までは実際にほぼその通りに開発されてきた。しかし、この高速化もほぼ限界に近づいており、集積化に大きな問題が発生してきていると思われる。十数年前までは、コンピュータは毎年のように新しいCPUが出てきてコンピュータが速くなったように思われたが、CPUの高速化に限界が来て、携帯電話のCPUもCPUそのものは進化しないでマルチコア化されてきているようにも思われる。

つまり、VLSI方式での集積度がもうすぐ限界に来ており、VLSI方式の3次元拡張も期待されているが、あと10年、20年で1ビットあたりの原子数が1nmの原子レベルに近づいてくる。プロセッサの最近の制作スケールでは、1電極あたり5つの原子を利用することが可能なほどの集積度が予想され、さらに

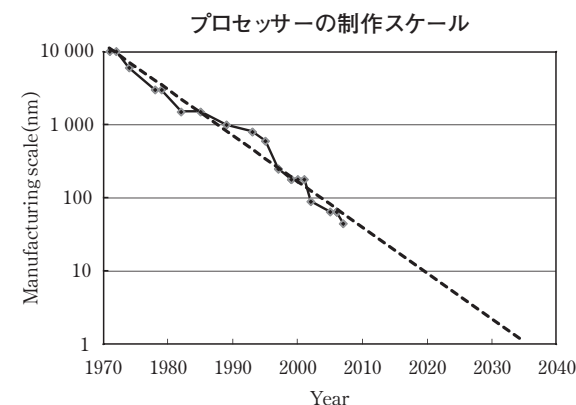


図-1.1

3次元的な集積化も行われている。また、VLSIの小型化により発熱量もますます増加し、問題となってきている。そのために、新しい計算モデルや新しい計算原理が必要で、原子レベルでの新しい量子コンピュータのモデルや分子レベルでのDNAコンピュータが考えられてきている。

危機を煽るわけではないが、たとえば、石油資源に関して「オイルも21世紀には無くなるといったのにまだあるではないか?」と思われる方もいるだろうが、これは、効率的な精練方法や回収率の向上の技術、衛星による油田探索方法の開発により新しい油田の発見が行われたための延命と考えられ、いつかは無くなるものである。そのために、各自動車メーカーは、新しい方式の自動車を開発しており、ハイブリッド・カーや燃料電池、水素電池の自動車を開発している。コンピュータも同様で、さらなる高速化が必要なときには、新しい計算モデルや新しい計算原理を考える必要がある。

### 1.1.2 量子アルゴリズムの発展

量子コンピュータの始まりは、1981年にArgonne National Laboratoryのポール・ベニオフ(Paul Benioff)が、古典的なチューリング機械(Classical Turing Machine)にできることは量子システム(Quantum System)でも可能であると考えたことからである。そして、1982年にCalifornia Institute of Technology(Caltech)のリチャード・ファイマン(Richard P. Feynmann)は、従来のコンピュータを用いて量子力学的現象をシミュレーションすると指数関数的時間がかかり、逆に量子システムを用いた計算には古典的なチューリング機械よりももっと優れた計算能力があるのではないかと考えた。1985年にオックスフォード大学クラレンドン研究所(図-1.2)にいたデイビッド・ドイチ(David Deutsch)は、量子チューリング機械(Quantum Turing Machine)の基本的な考え方を初めて示し、量子計算機モデルの定式化を行った。さらに、現在ドイチ問題として知られている、重ね合わせができる量子状態を用いて古典的な方法では実現できない量子並列(Quantum Parallel)の考え方を示した。

その後、この量子並列を利用した量子アルゴリズムはしばらくの間発見されなかったが、1994年にAT&Tベル研究所のピーター・ショア(Peter Shor)は、関数の周期性を利用して、大きな整数の因数分解を多項式的時間で効率的に計算する量子アルゴリズムを発見した。この発見は、現在広く用いられているRSA暗号が因数分解の難しさを利用しているために、世の中に大きな衝撃を与えた。



図-1.2 オックスフォード大学クラレンドン研究所

たとえば、多くの電子商取引では、公開鍵暗号(RSA)を用いてデータを暗号化してやり取りするSSL(Secure Socket Layer)と呼ばれる安全な通信を使っているが、クラッカーが量子コンピュータを持つとこの安全性が大変なことになる予想された。しかし、量子コンピュータも量子暗号というもっと強固な暗号システムを考案しているのだから、その危険性も回避されようである。1995年にデイビッド・ドイチは、2種類の基本的な量子ゲートがあれば、どのような量子コンピュータも作成できることを示した。さらに、1996年にベル研究所のグローバー(Lov K. Grover)は、量子並列を用いた振幅増幅手法を利用して、データベースでのより高速な検索アルゴリズムを発見した。

### 1.1.3 なぜ量子コンピュータが必要なのか?

論理回路が原子レベルに近づくと、オームの法則は成立せず、原子の世界を支配する法則として、20世紀に確立した理論体系である量子力学(Quantum Mechanics)が必要となる。そこで、原子や光、核スピンにおける量子状態を計算や通信に用いる量子コンピュータが、注目されてきている。

そもそも量子(Quantum)とは、物質のミクロな世界で見られる実体であり、つぎのような性質を持っている。

#### 【量子の性質】

□二重性——量子は波と粒子との2つの性質を同時に持つ

波が角周波数 $\omega$ を持つとすると、波を粒子として量子化されると、粒子は

エネルギー $\hbar\omega$ を持つ ( $\hbar$ はプランク定数  $h$  を  $2\pi$  で割ったもの)。この2つを同時に持ち、それらの性質が顕著に表れる状態が量子である。

□**離散性**——量子は連続的なエネルギーでなく飛び飛びのエネルギーを持つ

マクロな世界ではエネルギーは連続的であるが、ミクロな世界においては、電子が原子核の電磁力で引っ張られているような束縛力があるような場合には、エネルギーは離散的になり、飛び飛びなエネルギー準位しか持たなくなる。

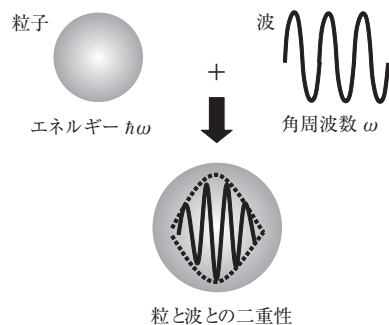


図-1.3 二重性

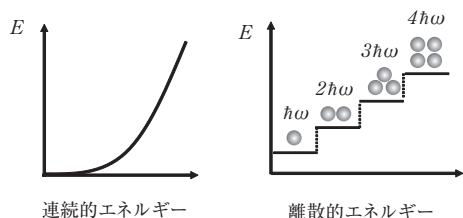


図-1.4 離散性

□**不確定性**——運動量(速度)がわかれば位置が不明、位置がわかれば運動量(速度)が不明になる

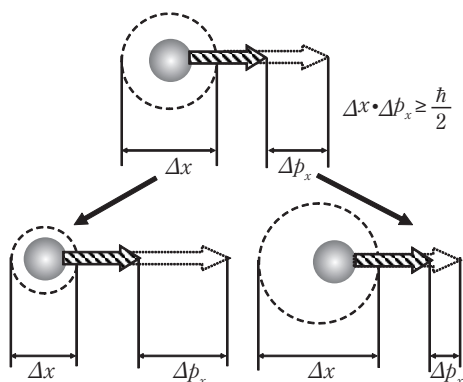


図-1.5 不確定性

位置の不確定性を  $\Delta x$ 、運動量の不確定性を  $\Delta p_x$  とすれば、つぎのような不等式での制約がある。つまり、電子の運動量(速度)と位置とを同時に正確に知ることができない。

$$\Delta x \cdot \Delta p_x \geq \frac{\hbar}{2}$$

図-1.3のように、二重性では、光は干渉するように電磁波の波としての性質もあり、光電効果に見られるように光子としての粒子の性質もあり、また、電子は電子質量があるように粒子としての性質もあり、光学顕微鏡のように電子顕微鏡があるようにド・ブロイ (de Broglie) の電子波としての波の性質もある。これらの量子は、観測の仕方によって、粒子のような状態にも波束として波のような状態にもなる。

離散性とは、図-1.4のように量子の持つエネルギーは連続的なエネルギーでなく、階段のように飛び飛びの離散的なエネルギーを持つことである。例えば、光の角振動数が  $\omega$  である光のエネルギーは、連続的に変化するのではなく  $\hbar\omega$  の整数倍しか取れない。また、原子において原子核の周りを回る電子も、連続的なエネルギー状態にあるのではなく、離散的なエネルギー準位に束縛されている。束縛力は、離散的なエネルギー準位となることが証明されている。

不確定性は、ドイツの物理学者ハイゼンベルグ (Werner Heisenberg) によって提案された**不確定性原理 (uncertainty principle)** と呼ばれ、図-1.5のように位置の不確定性を  $\Delta x$ 、運動量の不確定性を  $\Delta p_x$  とすれば、つぎのような不等式で制約されることになる。

$$\Delta x \cdot \Delta p_x \geq \frac{\hbar}{2}$$

つまり、電子の運動量(速度)と位置とを同時に正確に知ることができず、運動量(速度)がわかれば ( $\Delta p_x = 0$ )、位置が不明 ( $\Delta x = \infty$ )、一方、位置がわかれば ( $\Delta x = 0$ )、運動量(速度)が不明になる ( $\Delta p_x = \infty$ )。

量子コンピュータは、このような量子の性質を持った力学系を利用した情報処理の研究である。従来のコンピュータで使われていた0と1との2つの異なったビットを用いた**ブール論理 (Boolean logic)**とは異なり、量子コンピュータでは、つぎのような特徴を用いて超並列処理が可能となる0と1との**重ね合わせ状態 (superposition state)**を用いている。

【量子状態の3つの特徴】

□量子重ね合わせ状態——離散的な状態が混ざり合った状態で、観測によりどれかの状態に収縮し、重ね合わせ状態が壊れる

図-1.6 立方体のワイヤースケッチを見ると、上面が見えているような見方(0の状態とする)と下面が見えているような見方(1の状態とする)の2つの見方があり、1つの実体でも2つの見方が混在している場合があることがわかる。これが2つの見方の重ね合わせ状態である。

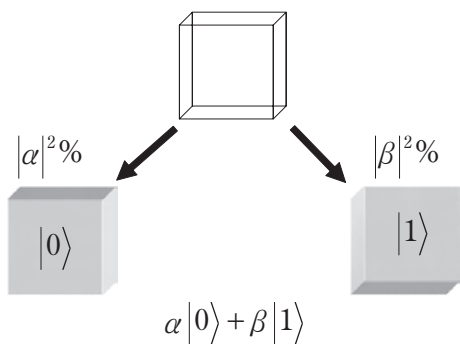


図-1.6 量子重ね合わせ状態

また、図-1.7の絵は騙し絵で有名なRubinの壺であるが、見方により、1枚の絵が壺に見えたり、対面した顔に見えたりする。これが、重ね合わせ状態の例えで、絵の見え方は観測者次第となる。



図-1.7 Rubinの壺

□量子干渉効果——いろいろな状態が強め合ったり弱め合ったりすること

図-1.8のように、量子状態には波の性質があり、2つの波が山と山でぶつくと更に大きな山の波ができる(強め合う干渉, constructive interference), 一方、山と谷の状態の波がぶつくと、波は打ち消し合い、ほとんど消えてしまう(弱め合う干渉, destructive interference)。

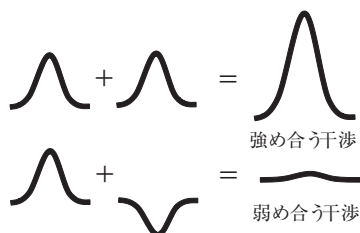


図-1.8 量子干渉効果

□量子もつれ状態——いろいろな状態間で相関関係があり分離できない

量子もつれ状態とは、図-1.9の右のように量子同士が別々な状態に存在しているのではなく、量子間に相関関係が発生し、それぞれの量子の状態を分離することができない状態である。個々の量子状態だけを記述することはできず、一方の観測結果によって他方が影響を受けることになる。

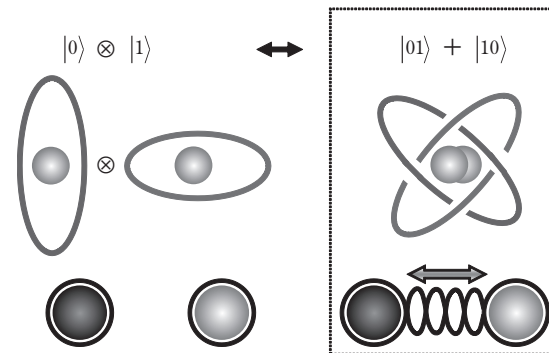


図-1.9 量子もつれ状態

量子重ね合わせ状態は、離散的な状態が混ざり合った状態で、原子の中の電子がいろいろな軌道を取り得るが、1つの電子がいくつかの軌道を持率的に同時に取り得る共存した状態である。このような重ね合わせ状態を観測すると、どれかの状態に収縮し、重ね合わせ状態が壊れる性質がある。量子干渉効果は、池に落ちた2つの石がおこす波紋が干渉するように、いろいろな状態がお互いに強め合ったり弱め合ったりする。量子もつれ状態は、いくつかの状態間で相関関係があり分離できない状態、一方の状態を調べるとその量子状態は壊れてしまい、他方の量子状態が決まってしまうようなお互いに絡み合った状態で、それぞれ個々の量子状態に分離できない。

量子コンピュータでは、重ね合わせ状態は、量子ビット(qubit:キュービット)と呼ばれる。キュービットの実現方法には、原子やイオンを用いたり、光やスピン、量子ドットなどを用いたいろいろな方法がある。

キュービットにおける重ね合わせ状態を、量子力学を学習していない読者に簡単に説明すると、図-1.6のような立方体のワイヤースケッチを見ると、上面が見えているような見方(0の状態とする)と下面が見えているような見方(1の状態とする)の2つの見方があり、1つの実体でも2つの見方が混在している場合



## 2.1 ヒルベルト空間とベクトル空間

### 2.1.1 ヒルベルト空間

ヒルベルト空間 (Hilbert space) とは、ノルムに関して完備な内積が定義された複素数上でのベクトル空間である。つまり、内積空間が完備性を持つとき、「ヒルベルト空間」という。完備性とは、コーシー列が収束することをいう。ヒルベルトは、ユークリッド空間を一般化し、内積が定義された距離空間を考えた。彼は、現代数学の巨峰とも父ともいわれ、「数学に人種の差別はない」という言葉がある。

量子力学での波動関数は、無限次元複素ヒルベルト空間内のベクトルとなり、ヒルベルト空間で議論する必要がある。しかし、量子コンピュータで出てくる有限次元の複素ベクトル空間では、ヒルベルト空間は正確に複素内積空間と同じである。そのために、量子コンピュータでは、ヒルベルト空間を使ってもよいが、内積が定義されたベクトル空間で議論できることにもなる。

### 2.1.2 ベクトル空間

ベクトル空間 (vector space) として、ベクトル (vector) の組  $|x\rangle, |y\rangle, |z\rangle, \dots$  から構成される空間を考えてみよう。そして、複素数  $a, b, c, \dots$  を、この空間のスカラー (scalar) としよう。そうすれば、ベクトル空間とは、2つのベクトルに対して和 (sum) と、ベクトルに複素数を掛けたスカラー倍 (scalar multiplication) との計算が定義できることであり、そのとき、可換法則と結合法則が成り立ち、零ベクトルと逆ベクトルが存在するとき、この要素の集合をベクトル空間という。

#### 【ベクトル空間の定義】

■ 2つのベクトルに対してベクトル和 (sum) が定義  $|x\rangle + |y\rangle$

■ ベクトルに複素数を掛けたスカラー倍 (scalar multiplication) が定義  $a|x\rangle$

□ 可換法則が成立  $|x\rangle + |y\rangle = |y\rangle + |x\rangle$

□ 結合法則が成立  $(|x\rangle + |y\rangle) + |z\rangle = |x\rangle + (|y\rangle + |z\rangle)$

□ 零ベクトルが存在  $|x\rangle + |\emptyset\rangle = |x\rangle$

□ 逆ベクトルが存在  $|x\rangle + |-x\rangle = |\emptyset\rangle$

$|x\rangle + |y\rangle$  をベクトル  $|x\rangle$  とベクトル  $|y\rangle$  とのベクトル和と呼び、ベクトル和は、つぎのようにいかなる2つのベクトルに対して、別なベクトルとなる。

$$|x\rangle + |y\rangle = |z\rangle$$

また、ベクトル和は、順序を入れ替えても同じで、可換 (commutative) であり、

$$|x\rangle + |y\rangle = |y\rangle + |x\rangle$$

和演算の順番を前後しても同じで、結合 (associative) 則が成り立つ。

$$(|x\rangle + |y\rangle) + |z\rangle = |x\rangle + (|y\rangle + |z\rangle)$$

また、つぎのような性質を持つ、任意のベクトルに対して、零ベクトル  $|\emptyset\rangle$  が存在し、

$$|x\rangle + |\emptyset\rangle = |x\rangle$$

つぎのような逆ベクトル  $|-x\rangle$  も存在する。

$$|x\rangle + |-x\rangle = |\emptyset\rangle$$

また、いかなるベクトルに対しても、スカラー  $a$  との積 (product) は、別なベクトルとなる。

$$a|x\rangle = |z\rangle$$

スカラー倍は、ベクトル和に対してもスカラー和に対しても、分配 (distributive) 則が成り立つ。

$$a(|x\rangle + |y\rangle) = a|x\rangle + a|y\rangle \quad (a+b)|x\rangle = a|x\rangle + b|x\rangle$$

また、スカラー倍に関しても、つぎのように可換である。

$$a(b|x\rangle) = ab|x\rangle$$

0 や 1, -1 のスカラーに対して、つぎのように計算できる。

$$0|x\rangle = |\emptyset\rangle \quad 1|x\rangle = |x\rangle \quad (-1)|x\rangle = |-x\rangle$$

## 3.1 量子状態の表現方法

量子状態を表現するには、つぎのようなシュレディンガー描像とハイゼンベルグ描像の2つの方法があり、その方程式の表現も異なる。また、ケットベクトル表現での係数  $c_i$  は複素数のスカラーで確率振幅を表し、密度行列表現の係数  $p_i$  は確率を表す。

### 【量子状態の表現方法と方程式】

#### □シュレディンガー描像

ケットベクトル表現： $|\psi\rangle = c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + \dots + c_{N-1}|N-1\rangle$

シュレディンガー方程式： $i\hbar \frac{\partial |\psi(t)\rangle}{\partial t} = H|\psi(t)\rangle$

#### □ハイゼンベルグ描像

密度行列表現： $\rho = p_1|\psi_1\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2| + \dots + p_N|\psi_N\rangle\langle\psi_N|$

ハイゼンベルグ方程式： $i\hbar \frac{\partial \rho(t)}{\partial t} = [H, \rho(t)] = H\rho(t) - \rho(t)H$

このように、ケットベクトルで表現される量子状態は純粋状態と呼ばれ、ケットベクトルでは表現できない混合状態と呼ばれる量子状態がある。純粋状態での密度行列は  $\rho^\dagger = \rho$  となる性質があり、射影演算子の形になっている。

量子力学では、観測量 (オブザーバブル, observable) はヒルベルト空間でのエルミート演算子 (Hermitian operator) となり、観測可能な物理量はエルミート行列で表されることになる。このエルミート行列とは自己随伴 (self-adjoint) 行列  $H^\dagger = H$  で、転置共役をとっても同じ行列であった。

シュレディンガー方程式に見られるように、ケットベクトルで表現されるシュレディンガー描像では、状態ベクトル  $|\psi(t)\rangle$  は時間とともに変わり、一方、密度行列で表現されるハイゼンベルグ描像では、密度演算子  $\rho(t)$  が時間とともに変わることになる。ここでは、純粋状態の時間発展を支配するシュレディンガー方程式を主に扱うことにしよう。

## 3.2 シュレディンガー方程式

### 3.2.1 シュレディンガー方程式と波動関数

シュレディンガー描像では、量子状態の時間発展はシュレディンガー方程式によって支配され、量子コンピュータはユニタリ変換で制御されるが、量子力学と量子コンピュータとの関係を述べよう。

量子力学におけるシュレディンガー方程式は、考えている系全体のエネルギーを表すハミルトニアン  $H$  によって、系の状態を表す波動関数がどのように時間発展していくかを記述したもので、波動関数の時間微分が含まれていて、時間に依存している。量子力学では実際の波動関数は複雑な特殊関数で表されるが、量子コンピュータでは簡単に状態ベクトル  $|\psi\rangle$  で表す。

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = H|\psi\rangle$$

ここで、プランク定数  $\hbar = h / 2\pi = 1.0545887 \times 10^{-34} [\text{J} \cdot \text{s}]$  で、状態ベクトル  $|\psi\rangle$  が時間に依存しない定常状態でのシュレディンガー方程式は、

$$H|\psi\rangle = E|\psi\rangle$$

となり、ハミルトニアン演算子  $H$  に対して、 $|\psi\rangle$  は固有関数と呼ばれ、 $E$  はその固有値と呼ばれ、その系のエネルギーになっている。

そこで、この系の状態は、内積  $\langle\psi|\psi\rangle$  を調べると、量子状態の確率  $P$  が求められる。

$$P = \langle\psi|\psi\rangle$$

また、状態ベクトル  $|\psi\rangle$  における、ある演算子  $A$  の期待値は

$$\langle A \rangle = \langle\psi|A|\psi\rangle$$

で定義する。たとえば、全エネルギー  $E$  の期待値は

$$\langle E \rangle = \left\langle \psi \left| i\hbar \frac{\partial}{\partial t} \right| \psi \right\rangle$$

となる。

そこで、シュレディンガー方程式を解いてみよう。状態ベクトル  $|\psi\rangle$  は時間と