特集 量子コンピュータ

基般

量子計算の基礎

西村治道（名古屋大学大学院情報科学研究科）

量子計算

我々が日常的に用いているパソコンも限られた人しか利用できない高価なスパコンも，現在のコンピュータはすべて物理としては，マクロ系が従う古典力学を基礎原理とする．一方で，原子などのミクロ系は量子力学に従うとされ，不確定性原理やエンタングルメントなど量子力学特有の現象が生じる．コンピュータの高速化を目的として基本素子が微細化するにつれ，量子力学的効果が計算に及ぼす影響を抑えることが重要と考えられてきたが，1982 年に Feynman [6] はまったく逆の発想で量子計算という考え方を発表した．彼はどんなにコンピュータの基本素子を微細化したところで，量子力学系のコンピュータによるシミュレーションは系のサイズが大きくなるにつれて指数的に計算時間が爆発してしまうこと，そして効率的なシミュレーションを行うにはコンピュータの計算機構も量子力学系を採用すべきであることを指摘した．

1985 年，Deutsch [5] によって今日の量子計算の基礎となる量子並列計算の概念が提案された．彼は Feynman の考えを一歩押し進め，計算の高速化の観点で鍵となる量子力学の特性として重ね合わせの原理に目をつけ，重ね合わせの原理によって一種の並列計算（量子並列計算）が可能となることを明らかにした．量子並列計算のアイディアは，量子計算が量子力学系のシミュレーションなど量子力学に関係する問題のみならず，さまざまな問題に対する効率的なアルゴリズム（量子アルゴリズム）を成し遂げるという新たな可能性を示唆するものであった．

Deutsch の提案後しばらく注目されなかった量子計算であるが，今から 20 年前の 1994 年に Shor[7] の開発したアルゴリズムが量子計算を一躍スターダムに押し上げた．彼は，現在オンラインショッピング等で日常的に用いられている暗号が安全性の根拠とする整数の素因数分解を，多項式時間で行う量子アルゴリズムを発見したのである．Shor 以降の量子計算は，量子力学を用いた情報処理全般を扱う量子情報科学という，より広範な分野における中心的話題として，現在に至るまで理論と実験の双方で多岐にわたる研究が続けられている．

本稿では，量子計算の基礎と題して量子計算が何かを理解する上で必要最低限の理論的基礎を紹介する．量子計算に必要な量子力学の基本事項を紹介し，Deutsch が提案した量子回路（最も標準的な量子計算モデル）を使って，量子計算の進め方や量子アルゴリズムの例を詳細に記述するとともに古典計算との違いについて説明する．最後に，計算量理論の量子版である量子計算量理論の現状について簡単に触れる．なお本稿では，（多くの量子計算の論文がそうであるように）古典力学に基づく従来の計算，回路，アルゴリズムを量子との対比から古典と呼ぶ．

ここで本稿における量子力学の扱いについて述べておきたい．本稿では，（ノイマン型コンピュータで有名な）von Neumann による量子力学の公理に基づいて，量子力学を数学的に表現し，その表現をもとに議論を展開していく（これは社会現象を数学的にモデル化し，その上で議論を展開する計算機科学のやり方と同じである）．

量子計算に必要な量子力学の基礎

量子計算に必要な量子力学の基礎事項として，情報を保存すべき量子力学系および系が取り得る状態，より多くの情報を保存するために必要な 2 つ以上の

系の合成系，情報を読み出す測定，状態を変化させる上での系の時間発展，の 4 つの概念の数学的扱いがある．以下ではこれらを量子回路による量子計算の場合について順次説明していく．

量子ビット

情報の基本単位はビットであるが，量子計算における情報の基本単位は量子ビットである．量子ビットは物理的には（光子の偏光や電子のスピンなどの）2 準位系であり，量子力学の公理によると数学的には

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},\quad |1\rangle=\begin{bmatrix}0\\1\end{bmatrix} \tag{1}$$

を基底（この基底は計算基底と呼ばれる）とする 2 次元線形空間 $\mathbf{C}^2$ によって記述される．状態 $|0\rangle$ は論理的な 0 に対応し，状態 $|1\rangle$ は論理的な 1 に対応する．$|0\rangle$, $|1\rangle$ という記法はケットと呼ばれ，量子力学で用いられる．標準的なベクトル記法でなくケットを本稿では用いるが，理由の 1 つとしてビットとの対応が明示的であることが挙げられる．量子ビットの状態は $\mathbf{C}^2$ の単位ベクトル，すなわち

$$|\psi\rangle=a|0\rangle+b|1\rangle=\begin{bmatrix}a\\b\end{bmatrix} \tag{2}$$

（ただし，a, b は $|a|^2+|b|^2=1$ をみたす複素数）と表現される．係数 a, b は（確率）振幅と呼ばれる．

なぜ量子ビットの状態の数学的表現が式 (2) なのか．量子力学が扱う微細な系では，人間は測定という行為によってその姿を推測するしかない．測定が異なる結果を示す 2 つの状態を異なると考え，同じ結果を示すなら同一視する．そうやって試行錯誤した結果，式 (2) を量子ビットが取る状態の数学的表現とするとうまくいったので，公理として採用されているのである．

では式 (2) に対応する量子ビットの状態を測定すると何が起きるのかというと，(量子力学の公理によって) 確率 $|a|^2$ で測定値 0 が得られ，確率 $|b|^2$ で測定値 1 が得られることになる．これは 0 を表，1 を裏としたときに表が確率 $|a|^2$，裏が確率 $|b|^2$ で出現するコインのようにも思えるが，実際はもっと変である．コインの場合，一度投げられれば人間が測定するか否かに関係なく表か裏か決まっている．しかし信じがたいことに量子ビットの場合，測定する前は 0 とも 1 とも決まってない，つまり 0 が $|a|^2$，1 が $|b|^2$ の割合で「重なっている」と考えたほうが矛盾がないのである．そんなわけで，量子ビットが式 (2) で表現される状態にあるとき，「0 と 1 が振幅 a および b で重なり合っている（重ね合わせにある）」と呼ばれ，多くの物理学者は直観的描像として「0 と 1 が振幅の絶対値の 2 乗の割合で共存している」と考えるのである．

もう 1 つ奇妙なのは，式 (2) の中の振幅が負の数や複素数を取り得ることである．これは実際必要で，たとえば

$$|\phi_0\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle,\quad |\phi_\pi\rangle=\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$$

はともに測定すると確率 1/2 で 0 と 1 が出現するが，(後で見るように) 測定の前に前処理をすると，この 2 つは違う測定値を与えることになる．それゆえ 2 つは違う状態として考えるべきなのである．さらには同様の理由で $|\phi_\theta\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}e^{i\theta}|1\rangle$ は θ が $[0, 2\pi)$ の範囲で異なればすべて違う状態と考えるのが自然となる（θ は位相と呼ばれる）．状態表現に複素数が出てくるのは，量子力学が人間に馴染みのある古典力学の現象とは大きく異なることの表れとも取れる．

複数の量子ビット

次に 2 つの量子ビットからなる量子力学系を考える．そのため，ベクトルのテンソル積の概念を導入する．たとえば，2 つの 2 次元ベクトル

$$|\psi\rangle=\begin{bmatrix}a\\b\end{bmatrix}=a|0\rangle+b|1\rangle,\quad |\phi\rangle=\begin{bmatrix}c\\d\end{bmatrix}=c|0\rangle+d|1\rangle$$

のテンソル積は 4 次元ベクトル

$$|\psi\rangle\otimes|\phi\rangle=\begin{bmatrix}ac\\ad\\bc\\bd\end{bmatrix}=ac|00\rangle+ad|01\rangle+bc|10\rangle+bd|11\rangle$$

と定義される．テンソル積の記号 $\otimes$ はしばしば省略され，単に $|\psi\rangle|\phi\rangle$ と書かれることも多い．m 次元ベクトルと n 次元ベクトルのテンソル積も同様にして mn 次元のベクトルとして定義されることになる．量子力学の公理によると，2 量子ビットは

$|00\rangle := |0\rangle\,|0\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ を基底とする 4 次元空間 $\mathbf{C}^4$ で表現され，取り得る状態は単位ベクトル $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$（2 ビットの重ね合わせ）として表現される．同様に 3 量子ビットは $|000\rangle$（$|00\rangle$ と $|0\rangle$ のテンソル積と考えられる）から $|111\rangle$ までの 3 ビットの重ね合わせ，そして n 量子ビットは $|0^n\rangle$ から $|1^n\rangle$ までの n ビットの重ね合わせ

$$\left|\psi\right\rangle = \sum_{x\in\{0,1\}^n} \alpha_x \left|x\right\rangle = \alpha_{0^n}\left|0^n\right\rangle + \cdots + \alpha_{1^n}\left|1^n\right\rangle \quad (3)$$

（$\sum_{x\in\{0,1\}^n}\left|\alpha_x\right|^2 = 1$ であり，$\{|x\rangle\}_{x\in\{0,1\}^n}$ はやはり計算基底と呼ばれる）として表現される．物理的には n 個の量子ビットで，2^n 個もある n ビットを重ね合わせて表現できることは，量子ビットの有用な特性である（ただし，後で注意するようにむやみに重ね合わせればいいというわけでもない）．

上記の重ね合わせとともに，通常のビットと量子ビットの違いを表す特性としてエンタングルメントがある．量子ビット A が状態 $|\psi\rangle = a|0\rangle + b|1\rangle$，量子ビット B が状態 $|\phi\rangle = c|0\rangle + d|1\rangle$ にあるとき，A, B の 2 量子ビットの状態はテンソル積

$$|\psi\rangle \otimes |\phi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \quad (4)$$

で表現される．一方，2 量子ビットは $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$ のような状態も取ることができる．係数比較から分かるように $|\Phi^+\rangle$ は式 (4) の形で表現できない．このようなとき A と B はエンタングルしていると呼ばれ，A と B は古典力学で説明できない相関を持ち得ることが知られている．エンタングルメントの概念は 3 つ以上の量子ビットにも拡張され，量子状態の表現能力として大きな意味を持つ．実際，式 (3) の状態は 2^n 個のパラメータ $\boldsymbol{\alpha}_x$ を持つ一方，n 個の量子ビットがすべて互いにエンタングルしてないような状態は i 番目の量子ビットが $a_i|0\rangle + b_i|1\rangle$ と表現できるため，合成系の量子状態は高々 $2n$ 個のパラメータしか含まない．つまり，n 量子ビットの状態に（実際に引き出せるかどうかはさておき）指数的な情報を保存したければ量子ビットはエンタングルさせる必要がある．

測定

量子ビットを測定したとき測定値がどのような確率で出現するかについてはすでに述べた．以下では，測定後の状態がどうなるかや複数の量子ビットも含めて測定を定義する．扱うのは最も基本的な測定である計算基底による測定だけである．量子力学の公理によると，n 量子ビットの状態が式 (3) にあるとき，すべての量子ビットを計算基底で測定すると，測定結果 x が確率 $|\boldsymbol{\alpha}_x|^2$（振幅の絶対値の 2 乗）で得られ，測定後の状態は計算基底の状態 $|x\rangle$ となる．たとえば $\frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle$ を計算基底で測定すれば，確率 1/2 で測定結果 00 が得られて状態は $|00\rangle$ になり，確率 1/2 で測定結果 11 が得られて状態は $|11\rangle$ になる．一度測定すると状態が計算基底のどれかの状態になってしまうので，むやみに多くのビット列を重ね合わせてもそれら全部が測定で引き出せるわけではない．目的の情報を引き出すためには状態の加工（系の時間発展）が必要となる．

目的の情報を得る上で必ずしも n 量子ビットすべてを測定する必要はない．たとえば答えが Yes か No かを判定したい場合，最初の量子ビットのみ測定して 1 なら Yes，0 なら No と判断することもできる．n 量子ビットの状態 $|\phi\rangle$ が

$$\left|\phi\right\rangle = \sum_{y\in\{0,1\}^m} \alpha_y \left|y\right\rangle\left|\phi_y\right\rangle$$

（各 $|\phi_y\rangle$ は n 量子ビットのうち前半 m 量子ビットの状態が $|y\rangle$ のときの後半 n-m 量子ビットの状態）であるとき，前半 m ビットを計算基底で測定すると，確率 $|\boldsymbol{\alpha}_y|^2$ で y を得ることになり，測定後の状態は $|y\rangle\,|\phi_y\rangle$ になる．たとえば 3 量子ビットの状態が

$$\left|\phi\right\rangle = \sqrt{\frac{1}{6}}\left|000\right\rangle + \sqrt{\frac{2}{6}}\left|011\right\rangle + \sqrt{\frac{3}{6}}\left|111\right\rangle$$

であるとき，テンソル積の線形性より

$$\left|\phi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left(\sqrt{\frac{1}{3}}\left|00\right\rangle + \sqrt{\frac{2}{3}}\left|11\right\rangle\right)\right) + \frac{1}{\sqrt{2}}\left|1\right\rangle\left|11\right\rangle$$

と書き直せるので，最初の量子ビットを測定したとき，確率 1/2 で 0 を得て測定後の状態は $\left|0\right\rangle\left(\frac{1}{\sqrt{3}}\left|00\right\rangle + \sqrt{\frac{2}{3}}\left|11\right\rangle\right)$ となり，確率 1/2 で 1 を得て測定後の状態は $|1\rangle\,|11\rangle$ となる．

時間発展：量子回路，量子ゲート

量子力学の公理によると，量子力学系の時間発展はユニタリ変換と呼ばれる可逆な線形変換で表現される．つまり n 量子ビットの場合，その時間発展は（ユニタリ行列と呼ばれる）2^n 次正則行列で表現できることになる．

量子計算においては，n 量子ビットの状態を何らかのユニタリ変換で望ましい状態に加工することが計算となる．しかし，2^n という指数サイズの次数の行列に対応する変換を直接的に実現することは一般に困難である．そこで必要となるのは，n 量子ビットのうちのいくつかの量子ビットに的を絞って局所的なユニタリ変換で時間発展させる操作を逐次的に行うことで，所望のユニタリ変換を実現するという作業になる．これはまさに古典の計算において，n 変数のブール関数の計算が直接的には困難なので，何個かのビットに簡単なゲート（たとえば2個のビットに AND）を逐次的に施していくことと同じ考え方である．そのための基本素子となるユニタリ変換が量子ゲートであり，どの量子ビットにどの量子ゲートを施すかを示す設計図が量子回路である．以下では，重要な量子ゲートをいくつか紹介する．

1量子ビットゲート

1量子ビットゲートは2次のユニタリ行列で表現される．式(1)を思い出すとユニタリ行列[☆1]

$$U=\begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

は $|0\rangle$ を $U|0\rangle = a|0\rangle + b|1\rangle$ に移し，$|1\rangle$ を $U|1\rangle = c|0\rangle + d|1\rangle$ に移す線形変換である．逆に，$U|0\rangle$，$U|1\rangle$ を互いに直交する単位ベクトルに取れば対応する行列 U はユニタリ行列になることが知られているので，計算基底の各状態の移り先を指定することでも1量子ビットゲートを定義できる．

よく用いられる1量子ビットゲートとして，

$$X=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\quad Z=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\quad H=\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

がある．X は $|0\rangle$ を $|1\rangle$ に，$|1\rangle$ を $|0\rangle$ に移すので自然に古典の NOT ゲートに対応するが，重ね合わせ $|\psi\rangle = a|0\rangle + b|1\rangle$ にも適用できて $X|\psi\rangle = a|1\rangle + b|0\rangle$ となる．Z は $|0\rangle$ を $|0\rangle$ に，$|1\rangle$ を $-|1\rangle$ に移すので，状態 $a|0\rangle + b|1\rangle$ を $a|0\rangle - b|1\rangle$ に移す．H は Hadamard ゲートと呼ばれ，一様な重ね合わせを作る上で用いられる．実際，$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ なので，$|0\rangle$ と $|1\rangle$ が均等に重ね合わさった状態を作ることができる．n 量子ビットの状態 $|0^n\rangle$ の各量子ビットに H が適用されれば，

$$\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right)^{\otimes n} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\cdots\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

（n 個の $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ のテンソル積）となり，展開すると

$$\left(H|0\rangle\right)^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle = \frac{1}{\sqrt{2^n}}\left(|0^n\rangle + \cdots + |1^n\rangle\right)$$

（2^n 個の計算基底の状態 $|x\rangle$ の一様な重ね合わせ）を得る．たとえば，$n=2$ の場合，

$$\begin{aligned}\left(H|0\rangle\right)^{\otimes 2} &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\\ &= \frac{1}{\sqrt{2^2}}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)\end{aligned}$$

となる．

ここで量子ビットの位相の情報を取り出す方法を紹介する．量子ビットの状態が $|\phi_\theta\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)$ であるとする．このとき，$|\phi_\theta\rangle$ に H を施してから計算基底で測定すると，

$$\begin{aligned}H|\phi_\theta\rangle &= \frac{1}{\sqrt{2}}\left(H|0\rangle + e^{i\theta}H|1\rangle\right)\\ &= \frac{1}{2}\left(\left(1+e^{i\theta}\right)|0\rangle + \left(1-e^{i\theta}\right)|1\rangle\right)\end{aligned}$$

となるため計算基底で0を得る確率は $|(1+e^{i\theta})/2|^2 = (1+\cos\theta)/2$ となり，確率の違いからある程度は θ に関する情報が得られる．特に $|\phi_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ の場合は H を施すと常に0が得られ，$|\phi_\pi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ の場合は H を施すと常に1が得られるので，$|\phi_0\rangle$ と $|\phi_\pi\rangle$ は確実に識別可能である．この例のように，目的の情報を取り出すには重ね合わせをそのまま測定するだけでなく，時間発展による適切な加工が必要である．

☆1 ユニタリ行列の定義から $UU^\dagger = U^\dagger U = I$ をみたす．$U^\dagger$ は U の転置共役で I は単位行列．

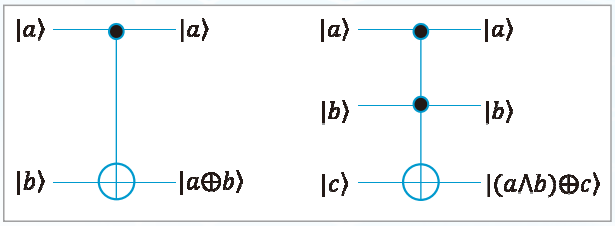

図 -1　CNOT と Toffoli．左が CNOT ゲートで右が Toffoli ゲート．黒丸は制御部を表し，⊕ は標的部を表す

CNOT ゲート，Toffoli ゲート

2 つ以上の量子ビットにまたがる量子ゲートとしてよく用いられるのが，CNOT ゲート（Controlled-NOT ゲート）と Toffoli ゲートである（ゲートの図式は**図 -1**）．CNOT は $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ をそれぞれ $|00\rangle, |01\rangle, |11\rangle, |10\rangle$ に移す 2 量子ビットゲートであり，まとめると $\mathrm{CNOT}|a\rangle|b\rangle = |a\rangle|a \oplus b\rangle$（$a, b \in \{0, 1\}$，⊕は排他的論理和）と書ける．$a=1$ のときに b に NOT が適用されるとみなせることが CNOT の名前の由来であり，前半の量子ビットは制御部，後半の量子ビットは標的部と呼ばれる．行列表示は

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

となる．Toffoli ゲートは $|a\rangle|b\rangle|c\rangle$（$a, b, c \in \{0, 1\}$）を $|a\rangle|b\rangle|(a \wedge b) \oplus c\rangle$（$a \wedge b$ は a, b の AND）に移す 3 量子ビットゲートである．$a=b=1$ のときに c に NOT が適用されるとみなせるので，CNOT の一般化ともいえる．CNOT ゲートも Toffoli ゲートも計算基底の状態を置換しているだけなので，その意味では NOT ゲート同様に古典ゲートに対応物が存在する．Toffoli ゲートはその定義から分かるように，AND ゲートおよび NOT ゲートの代用品として用いることができるため，任意の古典回路は Toffoli ゲートだけで模倣可能である．

量子計算の例：量子並列計算と干渉効果

量子回路による量子計算の進め方は以下のようになる．

初期状態の準備　計算の入力が $x \in \{0, 1\}^n$ のとき，n 量子ビットの状態 $|x\rangle$ とともに，補助量子ビットと呼ばれる $m-n$ 個の量子ビットの状態 $|0^{m-n}\rangle$ を，m 量子ビット上の量子回路の初期状態とする．

量子回路の実行　初期状態 $|x\rangle|0^{m-n}\rangle$ に対して，量子回路で指定された量子ビットに，指定された量子ゲートを逐次的に適用していく．

出力の読み出し　指定された量子ビット（たとえば最初からの k 量子ビット）を計算基底で測定する．

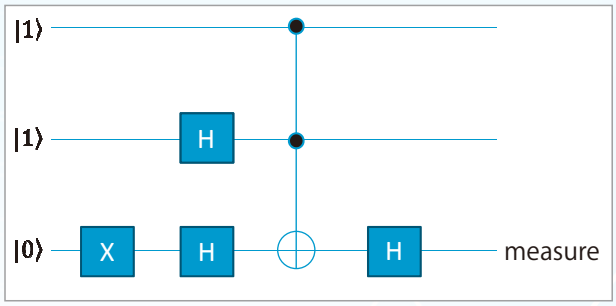

図 -2　量子回路による計算の例

図 -2 は実際に上記の進め方を見るための例である．計算の入力が $x=11$ のときの例で，$|11\rangle$ は 3 量子ビット上の量子回路の最初の 2 量子ビットに，補助量子ビット $|0\rangle$ は最後の量子ビットに準備されている．量子回路の実行ではまず第 3 量子ビットに NOT ゲート X が施される．この結果，初期状態 $|11\rangle|0\rangle = |110\rangle$ は $|111\rangle$ に変化する．次に第 2 および第 3 量子ビットに H が施されるため，状態は

$$\begin{aligned} |\psi_1\rangle &= |1\rangle\big(H|1\rangle\big)\big(H|1\rangle\big) \\ &= |1\rangle\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \\ &= \frac{1}{2}\big(|100\rangle - |101\rangle - |110\rangle + |111\rangle\big) \end{aligned}$$

となる．次に第 1 および第 2 量子ビットを制御部とする Toffoli ゲートが適用される．その結果，状態は

$$|\psi_2\rangle = \frac{1}{2}\big(|100\rangle - |101\rangle - |111\rangle + |110\rangle\big)$$

になる．次に第 3 量子ビットに H が施される．その結果，測定前の状態は

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{2}\big(|10\rangle H|0\rangle - |10\rangle H|1\rangle - |11\rangle H|1\rangle + |11\rangle H|0\rangle\big) \\ &= \frac{1}{2\sqrt{2}}\big(|100\rangle + |101\rangle - |100\rangle + |101\rangle\big) \\ &\quad + \frac{1}{2\sqrt{2}}\big(-|110\rangle + |111\rangle + |110\rangle + |111\rangle\big) \\ &= \frac{1}{\sqrt{2}}\big(|101\rangle + |111\rangle\big) \end{aligned}$$

となる．最後に第3量子ビットを測定すると確率1で結果1が得られることとなる．

上記の例で注目すべき最初の点は量子並列計算の威力である．通常の回路同様に基本となるゲートが固定されればゲートの総数が計算にかかるコストと思ってよい．上記例では，Toffoli, H, X が基本ゲートとして認められていれば，コスト5とカウントする．我々が手計算で $|\psi_1\rangle$ から $|\psi_2\rangle$ への変化を記述するときは（我々の手計算は量子計算の古典計算による模倣なので），計算基底の各状態に対して Toffoli ゲートが適用される（例の場合，$|\psi_1\rangle$ が4個の計算基底の状態の和なので計4回）が，量子計算ではこれがたった Toffoli ゲート1回の適用でできる．これが量子並列計算の威力であり，古典計算に対する計算時間の優位性を生み出し得る．

次に注目すべき点は干渉効果である．$|\psi_2\rangle$ に至るまでの変化では重ね合わさっている計算基底の状態の個数が増えるか現状維持かである．ところが $|\psi_2\rangle$ から $|\psi_3\rangle$ に変化すると，その個数は4個から2個に減少している．$|\psi_3\rangle$ に関する上記の手計算から見られるように，これは $|100\rangle$ と $|110\rangle$ の振幅が $1/2\sqrt{2}$ と $-1/2\sqrt{2}$ で打ち消しあったためである．このような効果を干渉効果という．干渉効果により，欲しい情報を持つ状態だけが残るように量子回路を設計することが量子計算の威力を発揮する術である．

量子アルゴリズムの例

Bernstein-Vazirani のアルゴリズム[2] は Shor のアルゴリズム以前に発見された量子アルゴリズムで，初等的であるが量子並列計算と干渉効果が有効な形で表れているよい実例である．以下の問題を考えよう．

問題 BV　入力 $s=s_1\cdots s_n\in\{0,1\}^n$ は，$x=x_1\cdots x_n\in\{0,1\}^n$ に対して $\mathbf{Z}_2^n$ 上の内積

$$f_s(x)=\sum_{i=1}^{n}s_ix_i\pmod 2$$

を返すようなブラックボックス回路の隠されたパラメータである．このとき s を正確に推定せよ．

古典計算ではどのように s を推定すればよいだろうか．隠された s の第 i ビット s_i を知りたければ i ビット目のみが1のビット列を x として $f_s(x)$ を評価すればよい．つまり，n 回の f_s の評価で問題 BV は解けることになる．しかし f_s は1回あたり1ビットの情報しか返さないことを鑑みると，情報理論的にこれが古典計算にできるベストである．

一方，量子計算ではどうか．驚くことに Bernstein-Vazirani アルゴリズムは，以下で見るようにわずか2回の f_s の評価で s を推定することができる．

量子アルゴリズム $\mathcal{A}_{BV}$

(i) $n+1$ 量子ビットの状態 $|0^n\rangle|0\rangle$ を準備する．
(ii) 最初の n 個の各量子ビットに H を施す．
(iii) f_s を呼び出し，前半 n 量子ビットが $|x\rangle$ であるときの評価値 $f_s(x)$ を最後の量子ビットに足し込む．
(iv) 最後の量子ビットに Z を適用する．
(v) f_s を呼び出し，前半 n 量子ビットが $|x\rangle$ であるときの評価値 $f_s(x)$ を最後の量子ビットに足し込む．
(vi) 最初の n 個の各量子ビットに H を施す．
(vii) 最初の n 量子ビットを計算基底で測定する．

以下で量子状態がどのように変遷するかを記す．

まず，$\left(H|0\rangle\right)^{\otimes n}=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$ だったので (ii) の後の状態は

$$|\psi_2\rangle=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle$$

となる．

(iii) が量子並列計算の効果を発揮するところで，状態は

$$|\psi_3\rangle=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f_s(x)\rangle$$

となる．手計算なら 2^n 回も f_s の評価が必要な一方で量子計算では1回の評価でよい点が要所である．

(iv) は得られた情報を振幅に移すことを行う．Z ゲートは $b\in\{0,1\}$ に対して $Z|b\rangle=(-1)^b|b\rangle$ である変換だといえるので，状態は

$$|\psi_4\rangle=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle(-1)^{f_s(x)}|f_s(x)\rangle$$

$$=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f_s(x)}|x\rangle|f_s(x)\rangle$$

となる．最後の1量子ビットの振幅に乗せた情報が全量子ビットの振幅の情報となるのが味噌である．

(v) で再び f_s の評価を最後の量子ビットに書き込むが $f_s(x) + f_s(x) = 0 \pmod 2$ より状態は，

$$|\psi_5\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f_s(x)} |x\rangle |0\rangle$$

となる．

(vi) が干渉効果を発揮するところで最も非自明である．(vi) によって $|\psi_5\rangle$ は状態

$$|\psi_6\rangle = |s\rangle\,|0\rangle$$

となる．このことを示すには，$|\psi_5\rangle$ の最初の n 量子ビットの状態 $|\chi_s\rangle := \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f_s(x)} |x\rangle$ が $|s\rangle$ になることを示せばよい．そのために鍵となるのは，($H = H^{-1}$ ゆえに)「H を n 個の量子ビットにそれぞれ施す」というユニタリ変換がその逆変換に等しい事実であり，この事実から $|s\rangle$ の各量子ビットに H を適用して $|\chi_s\rangle$ になることを示せば十分となる (どう示すか興味のある方はぜひご自身の手でご確認いただければと思う)．

結局 (vi) が終わると状態は $|\psi_6\rangle$ になることが分かり，そうなれば (vii) で s を確率1で得ることは明らかである．

$\mathcal{A}_{BV}$ は f_s の評価2回以外に $2n$ 回の H の適用，1回の Z の適用を行う．ブラックボックスとして与えられる f_s の評価は通常 (外部アクセスであるなどさまざまな理由で) 他のコストが無視できるほど高コストとされるため，このコストが2になったことは古典計算に対する量子計算の計算量的優位性を示していると考えられる．

量子計算量理論

最後に，Bernstein-Vazirani や Shor のアルゴリズムを生み出した量子計算に対する計算量理論からの研究 (量子計算量理論) について，簡単に現状を紹介する．

重要な課題はやはり Deutsch に端を発する方向性，つまり量子計算の古典計算に対する計算量的優位性およびその計算限界の解明である．Shor のアルゴリズムに代表される通り，代数的な問題に量子アルゴリズムは強く，多くの効率的量子アルゴリズムが開発されている[3]．その一方で NP 完全問題などについては，多項式時間量子アルゴリズムに対する否定的な証拠が示されている．

もう1人の量子計算の創始者 Feynman に端を発する方向性は，近年量子物理学の問題を計算量的枠組みで再検討するという趣旨のもと精力的に研究が進められている．量子物理系を記述するハミルトニアンの最小エネルギーを求める問題がどういう条件のもとで古典計算で効率的に計算できるかや，逆に NP の量子版においてさえ困難な問題であるかなどはまさにその典型である[1]．また，計算量理論の対話型証明モデルを用いてエンタングルメントを計算量理論的に解明するという研究なども興味深い話題である．

最後に触れておきたいのが量子的手法である．これは量子計算の概念や考え方を用いて古典の計算量理論や数学の問題を解くという手法であり，まだ適用例は多くないが量子計算の新しい存在意義として注目を集めている[4]．

参考文献

1) Aharonov, D., Arad, I. and Vidick, T. : The Quantum PCP Conjecture, *ACM SIGACT News* 44, pp.47–79 , arXiv:1309.7495 (2013).
2) Bernstein, E. and Vazirani, U. : Quantum Complexity Theory, in *Proceedings of the 25th Annual Symposium on Theory of Computing*, pp.11–20, ACM (1993).
3) Childs, A. M. and van Dam, W. : Quantum Algorithms for Algebraic Problems, *Reviews of Modern Physics* 82, pp.1–52 (2010).
4) Drucker, A. and de Wolf, R. : Quantum Proofs for Classical Theorems, *Theory of Computing, Graduate Survey* 2, pp.1–54 (2011).
5) Deutsch, D. : Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proceedings of Royal Society London Ser.* A 400, pp.97–117 (1985).
6) Feynman, R. : Simulating Physics with Computers, *International Journal of Theoretical Physics* 21, pp.467–488 (1982).
7) Shor, P. : Algorithms for Quantum Computation : Discrete log and Factoring, in *Proceedings of 35th Annual IEEE Symposium on Foundations of Computer Science*, pp.124–134, IEEE (1994).

(2014年3月20日受付)

西村治道 hnishimura@is.nagoya-u.ac.jp

1971年生．2001年名古屋大学大学院人間情報学研究科博士課程了．学術博士．2006年大阪府立大学講師．2012年名古屋大学准教授．量子計算量理論の研究に従事．