量子コンピュータに基づく計算量理論とその周辺

西村治道（大阪府立大学理学系研究科）

1　序

量子コンピュータは，従来のコンピュータと異なり，その計算原理が量子力学に基づいている．始まりは 1985 年に Deutsch [7] が，量子力学の基本原理の 1 つである「重ね合わせの原理」によりある種の並列計算を行うことで高速な計算ができるのではないか，というアイデアをもとに，量子コンピュータの計算モデルを提唱したことにある．量子コンピュータが一躍注目を集めることとなったのは，1994 年の Shor のアルゴリズム [20] である．Shor は，従来のコンピュータでは高速に解くことは困難であると考えられている整数の素因数分解問題や離散対数問題が，量子コンピュータを用いたアルゴリズムによって高速に解けることを証明した．これらの問題の計算量的困難性は，RSA 暗号など現在のインターネットで実装されている暗号系の安全性の基盤となっているため，量子コンピュータが実現すれば，Shor のアルゴリズムが実用化し，現在の多くの暗号系は崩壊する，という流れのもと量子コンピュータの研究は理論・実験とも急速に盛んになった．現在ではプレプリントサーバー arXiv (http://arxiv.org/archive/quant-ph) に毎日のように量子コンピュータがらみの論文が投稿されている．

一方で，量子コンピュータは計算機科学の世界にも新しい潮流を作った．量子コンピュータを利用した更なるアルゴリズムの開発や量子コンピュータの存在下でも安全性が保証される暗号系の提案などのために，量子計算の計算能力とその限界を理論的に研究する分野が生まれ，総称的に量子計算量理論と呼ばれている．量子計算量理論は当初，時間計算量に関する計算モデルをベースに語られるものを指していたが，（従来からの計算量理論 [3] がそうであるように）今日では，通信量など他の計算資源を扱うモデルも含め，量子情報理論や量子アルゴリズムなど周辺領域でも計算量理論的アプローチを取るものを含むようになってきている．本稿では，量子計算量理論およびその周辺の理論の中でも盛んに研究されていて，かつ比較的シンプルな計算モデルとして，量子回路，量子通信計算量を取り上げ，その計算量理論を紹介する．

2　量子状態と測定

量子コンピュータが処理する情報は，多くの場合，量子ビット (qubit, quantum bit の略語) と呼ばれる 2 状態系で数学的に表現され，その状態はビット 0 に対応するベクトル

$|0\rangle$ とビット 1 に対応するベクトル $|1\rangle$ によって張られる 2 次元複素内積空間 $\mathcal{H}_2$ 上の単位ベクトル $\alpha|0\rangle+\beta|1\rangle$ の形で表される．m 個の量子ビットからなる量子状態系は，$\mathcal{H}_2$ のテンソル空間 $\mathcal{H}_2^{\otimes m}$ によって表現され，その状態は m ビット列 $x=x_1x_2\cdots x_m\in\{0,1\}^m$ に対応するベクトル $|x\rangle=|x_1\rangle\otimes|x_2\rangle\otimes\cdots\otimes|x_m\rangle$ の線型結合

$$|\psi\rangle=\sum_{x\in\{0,1\}^m}\alpha_x|x\rangle$$

によって表される．$|\psi\rangle$ は 2^m 個という指数オーダのビット列を重ね合わせで表現しており，これらを一度に操作できることが量子コンピュータの能力の源となっている．

状態から情報を得るには測定が必要である．量子コンピュータにおける測定は，標準的には射影測定と呼ばれる測定が用いられる．射影測定は数学的には文字通り射影作用素を使って定義される．量子力学の測定の公理により，次の事実が知られている．

測定の公理（射影測定）　$\sum_i E_i=I$（I は $\mathcal{H}_2^{\otimes m}$ 上の恒等作用素）をみたす射影作用素の族 $\{E_i\}_i$ で表される測定を状態 $|\psi\rangle$ に施すと，測定値 i を確率 $||E_i|\psi\rangle||^2$ で得て，測定後の状態は $E_i|\psi\rangle/||E_i|\psi\rangle||$ となる．

$m=1$ の場合，つまり量子ビット $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ に対する測定として，計算基底における測定を考えよう．計算基底における測定とは，E_b を $|b\rangle$ で張られる $\mathcal{H}_2$ の 1 次元部分空間 $\mathrm{span}\{|b\rangle\}$ への射影作用素としたとき，$\{E_0,E_1\}$ で表される測定を意味する．$|\phi\rangle$ を計算基底で測定すると，$|\alpha|^2$ の確率で測定値 0 が得られ，$|\beta|^2$ の確率で測定値 1 が得られる．計算基底における測定は，一般の m にも拡張される．それは各量子ビットを計算基底で測定することを意味し，$\mathcal{H}_2^{\otimes m}$ の部分空間 $\mathrm{span}\{|x\rangle\}$ への射影作用素 E_x の族 $\{E_x\}_x$ で定義される．測定の公理より，$|\psi\rangle$ が計算基底のもとで測定されると，確率 $|\alpha_x|^2$ でビット列 x が測定結果として得られ，測定後の状態は $|x\rangle$ となる．より一般に，$|\psi\rangle$ をなす量子ビットの一部からの情報が必要なときは，それらの量子ビットのみを測定結果の対象とする．$|\psi\rangle$ の量子ビットのうち $j_1,\ldots,j_k$ 番目だけを測定することは，$\mathcal{H}_2^{\otimes m}$ の部分空間

$$\mathrm{span}\{|x\rangle\mid x\text{ の }j_1,\ldots,j_k\text{ 番目からなる }k\text{ ビット列が }y\}$$

への射影作用素 E_y の族 $\{E_y\}_y$ で定義される．これは，$j_1,\ldots,j_k$ 番目の量子ビットにのみ計算基底のもとでの測定を行っていることに等しい．

(例) 3 量子ビットからなる状態 $\frac{1}{\sqrt{3}}(|100\rangle+|010\rangle+|001\rangle)$ の第 1 量子ビットを計算基底のもとで測定すると，確率 2/3 で 0 が得られ，このとき測定後の状態は $\frac{1}{\sqrt{2}}(|010\rangle+|001\rangle)$ となる．確率 1/3 で 1 が得られ，このとき測定後の状態は $|100\rangle$ となる．

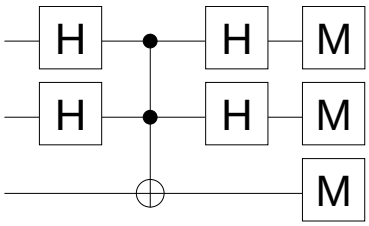

図 1　量子回路の例

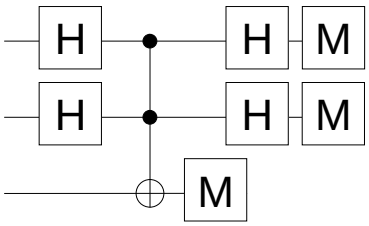

図 2　第 3 量子ビットを先に測定する量子回路

3　量子回路と計算量

3.1　定義と例

量子コンピュータの最も代表的な計算モデルは，Deutsch が導入した量子回路 [8] である．量子回路は，複数の量子ビット上からなる複素内積空間 $\mathcal{H}$ 上の作用の列であり，量子ゲートと呼ばれる決められた次元以下のユニタリ作用素の列によって表現される．その際，各量子ビットは（量子）ワイヤと呼ばれる．量子回路を構成するゲート数を量子回路のサイズと呼ぶ．量子回路 C による計算は次のように進められる．まず，計算したい入力，例えばビット列 x，に対して初期状態 $|\phi\rangle = |x\rangle \otimes |0^m\rangle$ を準備する．$|0^m\rangle$ は C での計算に必要な補助の量子ビットの列でアンシラ (ancilla) とよばれる．次に，C を構成する各量子ゲート $G_1, \ldots, G_k$ を順に作用させていく．各 G_i は量子回路の全てのワイヤのうち決められた有限個のワイヤ上でのみ作用するため，$\mathcal{H}$ 上の作用としては $G'_i = G_i \otimes I$ という形のユニタリ作用素となる（I は G_i が作用しないワイヤ上の恒等作用素である）．結果，C の作用後の状態は $|\phi'\rangle = G'_k G'_{k-1} \cdots G'_1 |\phi\rangle$ となる．最後に，$|\phi'\rangle$ を測定することで量子回路の出力に関する確率分布を得る．

(例) 図 1 は量子回路の例である．横線は量子回路のワイヤを表し，この例は 3 量子ビットからなる量子回路である．回路の演算は図の左から右へ進む．H は

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

で定義される量子ゲートで，アダマールゲート (Hadamard gate) と呼ばれる．黒丸および $\oplus$ のついた縦線は

$$T(|x\rangle \otimes |y\rangle \otimes |z\rangle) = |x\rangle \otimes |y\rangle \otimes |xy \oplus z\rangle$$

（$\oplus$ は排他的論理和）で定義される量子ゲートで，トフォリゲート (Toffoli gate) と呼ばれる．$x = y = 1$ という制御条件のもとで z がフリップされるので，第 1 および第 2 量子

ビットには制御する側を表す黒丸を付け，第 3 量子ビットには制御される側を表す $\oplus$ を付けている．トフォリゲートは古典のゲートとして以前から知られており，T はそれを自然に量子ゲートとして表現したにすぎない．M は各量子ビットに対する（計算基底のもとでの）測定を表している．この量子回路は初期状態として，$|000\rangle = |0\rangle|0\rangle|0\rangle$（3 つの $|0\rangle$ のテンソル積を表す．テンソル記号はしばしば省略される）を入力すると，最初の 2 つの H で

$$|\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle),$$

T の適用後,

$$|\psi_2\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$$

となり，最後の 2 つの H の適用後の状態は,

$$|\psi_3\rangle = \frac{1}{4}(3|000\rangle + |010\rangle + |100\rangle - |110\rangle + |001\rangle - |011\rangle - |101\rangle + |111\rangle)$$

となる．それゆえ，測定によって 000 を確率 9/16 で，$010, 100, 110, 001, 011, 101, 111$ の各々を確率 1/16 で得る．ここで，最初の 2 つの H はどちらを先に適用するかは計算に何の影響も与えないことに注意すべきである．これは第 1 量子ビットにかかる H は $\mathcal{H}_2^{\otimes 3}$ 上のユニタリ演算としては $H \otimes I \otimes I$（I は $\mathcal{H}_2$ 上の恒等作用素）であり，第 2 量子ビットにかかる H は $I \otimes H \otimes I$ で，2 つは互いに可換なので，どちらを先に適用しても得られる状態は同じだからである．同様の理由で，図 2 のように最後の 2 つの H の前に第 3 量子ビットを測定することは，最終的に得られる測定値の確率分布に何の影響も与えない．これもまた最後の 2 つの H を表すユニタリ作用素と第 3 量子ビットの測定を表す射影作用素が可換であることによる．

従来のコンピュータがなす古典的な演算[*1]が AND と NOT など有限個のゲートで表現できることはよく知られている．任意の量子的な演算はユニタリ作用素として表現されるので（複素数値の連続性から）有限個の量子ゲートで正確に表現することはできないが，近似的には表現できる．そのような量子ゲートの集合を万能集合と呼ぶ．近似を許す限り，計算量の観点で多くの場合において，万能集合の種類は重要でない．最も簡素な万能集合の例として，$\{H, T\}$ が知られている [19]．トフォリゲートは任意の古典的な演算を表現できる [13] ので，任意の古典的演算は $\{H, T\}$ からなる量子回路で実行可能である．与えられたユニタリ作用素を近似的に表現する（適当な万能集合を基にした）量子回路のサイズは，近似精度を ϵ とすると，$\log(1/\epsilon)$ の多項式で押えられる [10, 13].

[*1] 量子計算の研究者には従来の計算を（古典力学に基づいた計算のため）古典的な計算と呼ぶ慣習がある．

3.2 計算量クラス

計算すべき問題の多くは，適当な符号化によってビット列全体の集合 $\{0,1\}^*$ 上の関数で表現される．以下では簡単のため関数としてブール関数のみを考慮するものとする．

古典の計算量理論 [3] において，「効率的に計算可能な関数」のクラスとして古くから認識されているのが **P** であり，「効率的に検証可能な関数」のクラスである **NP** とともに計算量理論の代表的なクラスである．その一方で，1970 年代後半に発見された素数判定に対する乱択アルゴリズム（乱数を使って次の動作を決めてもよいアルゴリズム）以降，多くの計算量理論の研究者が「効率的に計算可能な関数」と考えるのは **BPP** と呼ばれるクラスである．**BPP** とは，多項式時間乱択アルゴリズムによって有界誤りで，すなわち確率 $1/2+\epsilon$ （ϵ は入力の長さによらない正の数）以上で正しく計算できる関数のクラスである．アルゴリズムを繰り返して多数決を取ることで，多項式時間のままで誤り確率（$\leq 1/2-\epsilon$）を指数的に減少させることができる．$\mathbf{P}=\mathbf{BPP}$ というのが多くの計算量理論の研究者の予想であるが，現時点で証明はなされていない．一方で，多項式時間乱択アルゴリズムによって非有界誤りで，すなわち $1/2$ より大きな確率で正しく計算できる関数のクラスは **PP** と呼ばれている．この場合，アルゴリズムの成功率は $1/2$ に指数的に近いかも知れず，誤り確率を効率的に減らせるという保証はない．自明な包含関係として $\mathbf{P}\subseteq\mathbf{BPP}\subseteq\mathbf{PP}$ が成立するが，包含関係が真であるかは未解決である．

量子コンピュータで効率的に計算可能な関数のクラスが **BQP** である．固定された量子回路が扱える入力のサイズは有限なので，問題を解くためには有限生成された一様回路の族で考える必要がある．ここで，量子回路の族 $\{C_n\}_n$ が有限生成された一様回路族 [14, 15] であるとは，C_n が（n に依存しない）有限種類の量子ゲートの集合 $\{G_i\}_i$ から構成され，その表現（例えば二進表現）が n の多項式時間で計算可能であることをいう（厳密には G_i の計算基底における行列表現の各成分が多項式時間計算可能という制約を必要とする）．必然的に C_n のサイズは n に関する多項式以下となる．関数 f が有限生成された一様量子回路族 $\{C_n\}_n$ によって有界誤りで計算可能とは，任意の n および任意のビット列 $x\in\{0,1\}^n$ に対して，C_n の入力 x 上での出力が確率 $1/2+\epsilon$（ϵ は入力の長さによらない正の数）以上で $f(x)$ であることをいう．**BQP** は有限生成された一様量子回路族によって有界誤りで計算可能な関数のクラスである．Shor のアルゴリズムが計算量理論的に示すことは，整数の素因数分解問題および離散対数問題（のブール関数版）が **BQP** に含まれるということである．これらの問題は **BPP** に含まれないであろうと考えられているので，$\mathbf{BPP}\subsetneq\mathbf{BQP}$ と予想されている．しかしながら，$\mathbf{BQP}\subseteq\mathbf{PP}$ が示されて

いる [2] ため，何らかの計算量理論的ブレークスルーがない限り，包含関係が真であることを証明することは困難であると考えられる．

3.3 オラクルモデルと量子アルゴリズムの例

これまで開発されてきた量子アルゴリズムの多くは，量子回路をベースとしつつも，オラクルと呼ばれるある種のブラックボックスにアクセスすることで計算を行うタイプの問題である．ここでは初期の量子アルゴリズムとして Simon [21] が与えた量子アルゴリズムを紹介する．Simon が考えた問題は，次のような問題である．

Simon の問題

（オラクルとして与えられる）入力. 任意の $x \in \{0,1\}^n$ に対して，$f(x \oplus a) = f(x)$ をみたすような「2 対 1」関数 $f : \{0,1\}^n \to \{0,1\}^{n-1}$.

出力. 隠された n ビット列 $a \neq 0^n$

Simon の問題に対する量子アルゴリズム（Simon のアルゴリズム）は，以下の様である．

ステップ 1. 初期状態として $|0^n\rangle|0^{n-1}\rangle$（$2n-1$ 個の量子ビット $|0\rangle$）を準備する．最初の n 量子ビットを第 1 レジスタ，残りの $n-1$ 量子ビットを第 2 レジスタと呼ぶ．

ステップ 2. 第 1 レジスタの n 量子ビットの各々に H を施す．このとき，状態は

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

と変化する．

ステップ 3. 各重ね合わせの x に対して，オラクルに質問することで第 2 レジスタ上に値 $f(x)$ を得る．このとき，状態は

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

となる．

ステップ 4. 第 2 レジスタを測定する．測定値として各 $b \in \{0,1\}^{n-1}$ が確率 $1/2^{n-1}$ で得られ，測定後の状態は，

$$\frac{1}{\sqrt{2}}(|x[b]\rangle + |x[b] \oplus a\rangle)|b\rangle$$

となる．ただし，$x[b]$ は $f^{-1}(b) = \{x[b], x[b] \oplus a\}$ なる長さ n のビット列である．

ステップ 5. 第 1 レジスタの n 量子ビットの各々に H を施す．このとき，状態は

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} ((-1)^{z \cdot x[b]} + (-1)^{z \cdot (x[b] \oplus a)})|z\rangle|b\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} (-1)^{z \cdot x[b]}(1 + (-1)^{z \cdot a})|z\rangle|b\rangle$$

となる．$z \cdot w$ は n ビット列 z および w を $\mathbb{Z}_2^n$ の要素とみなしたときの内積である．

ステップ 6. 第 1 レジスタを測定する．このとき，測定値として $z \cdot a = 0$ をみたす n ビット列 z が得られる．

以上より Simon のアルゴリズムから $z \cdot a = 0$ をみたす z を得られるが，このような z は $\{z \mid z \cdot a = 0\}$ からランダムに得られることが確認できる．よって $O(n)$ 回 Simon のアルゴリズムを実行すれば，高確率で（$\mathbb{Z}_2^n$ の要素として）一次独立な $n-1$ 個の要素 $z_1, \ldots, z_{n-1}$ が得られる．このとき，連立方程式 $z_1 \cdot y = 0, \ldots, z_{n-1} \cdot y = 0$ から $y = a$ を求めることができる．Simon のアルゴリズム 1 度当たり 1 回の質問（プラス n の多項式回のゲート操作）を要するので，我々は量子コンピュータにより，n の多項式の計算量で Simon の問題を解くことができる．一方，古典のアルゴリズムでは，直感的には $f(x) = f(x')$ となるような x と x' のペアを見つけるまでオラクルへの質問を行う必要があり，いわゆるバースデーパラドクス的考察から $\Omega(\sqrt{2^n})$ 回の質問が必要となることが証明できる．

Simon のアルゴリズムは量子計算量理論において幾つかの面で重要な役割を果たした．１つ目は，古典では指数的な計算量を必要とするが量子では多項式の計算量で済む問題を初めて提示したということである．ここでいう計算量とはオラクルへのアクセス回数であるが，計算量理論の相対化の概念を用いれば $\mathbf{BPP} \subsetneq \mathbf{BQP}$ という状況証拠を与えていることになる．２つ目のより重要ともいえる貢献は，このアルゴリズムで使用された手法（量子フーリエ変換）が，Shor のアルゴリズムに利用されたということである．この手法はいわゆる「隠れ部分群問題」に一般化される（Simon の問題は $\mathbb{Z}_2^n$ 上の隠された部分群 $\{0^n, a\}$ を発見する問題とみなせる）など代数的構造を持つ問題において非常に相性がよく，今日多くの代数的問題に対する効率的な量子アルゴリズムが発見されている [6].

3.4 量子 Turing 機械

古典の計算量理論において最も標準的な計算モデルは Turing 機械である．それゆえ，Deutsch が最初に導入した量子コンピュータのモデルは量子回路ではなく，Turing 機械の量子版である量子 Turing 機械 [7] であった．量子 Turing 機械は，量子計算量理論を展開するために Bernstein と Vazirani[4] によって最定式化され，**BQP** も量子 Turing 機械をベースに定義されている．量子 Turing 機械と量子回路は，多項式時間量子 Turing 機械と有限生成された一様量子回路族が互いに誤差なく模倣可能である [14, 15] という意味で，多項式計算量として同等である．量子 Turing 機械は，停止問題 [16] など量子 Turing 機械特有の問題があるが，量子回路と違い単一ですべての入力を扱えるという利点があるため，量子状態の Kolmogorov 計算量などを扱う上で便利なモデルである．

4　量子通信計算量

4.1　古典の通信計算量

今日のインターネット時代において，利用可能なデータ量は日々巨大化していて，１つの計算機に全てのデータを保存することは不可能である．それゆえ，何らかの問題を解決する上で，複数の計算機にまたがるデータを必要とすることはそう珍しい話ではない．このような分散されたデータを入力とする問題を解決するために，複数の計算機が行う計算のことを通信プロトコルといい，必要な通信の量（通信計算量）を研究するのが，通信計算量理論 [23, 11] である．例えば，２つのデータ x と y が２台の計算機に分散されていて，それらが等しいかどうかを判定する問題（等価性判定問題）を考える．問題を考える上で計算機１，計算機２とするのでは味気ないので，データ x は Alice が，データ y は Bob が持つものとする．この場合，最も安易な方法は Alice が x そのものを Bob に送ってしまうことである．しかしこの方法は，データそのものを送るという意味で通信量的に非効率的な方法である．ではより良い方法は存在するのか？実は Alice が Bob にデータそのものを送るより通信量を減らす方法はない．さらには２人がお互いに情報のやり取りを行うことで何とかしようとしても，通信量を減らすことはできない [11].

ところが，Alice と Bob が乱数を使った確率的な（つまり，有界誤りを認めた）通信プロトコルを行うと，通信計算量が劇的に減少することがある．等価性判定問題を再考しよう．データの長さが異なる場合は（Alice が x の長さを Bob に送ればよく）あまり通信量を必要としないので，x および y の長さが共に n である場合を考えよう．決定的な（常に正しい答えを出す）通信プロトコルでは，データをそのまま送る以外なく，n の通信計算量が必要である．ところが，確率的通信プロトコルでは $O(\log n)$ という指数的に少ない通信計算量で解くことが可能となる [11].

アイデアは，多少の誤りが認められると，Alice と Bob は自らのデータを少し冗長にすることで，２人のデータ内の対応するどのビットも同じかどうかを高確率で判定できる点にある．具体的には，まず誤り訂正符号 $E : \{0,1\}^n \to \{0,1\}^m$ として，任意の２つの符号語 $E(x)$ と $E(y)$ のハミング距離が $(1-\delta)m$ 以上で $m = cn$（δ と c は適当な定数）となるようなもの（例えば Justesen 符号 [12] など）を考える．Alice は乱数を使ってランダムに選んだ $i \in \{1, 2, \ldots, m\}$ に対して $E(x)$ の i 番目のビット $E_i(x)$ と i そのものを Bob に送る．Bob は $E_i(y)$（これは Alice が i を送るので計算可能）と $E_i(x)$ が等しければ１（等しいという判断），等しくなければ０（等しくないという判断）を出力する．この通信

プロトコルは $x = y$ の場合，どんな i に対しても $E_i(x) = E_i(y)$ なので常に正しい答えを与える．また，$x \neq y$ の場合，誤り訂正符号 E の取り方より $E_i(x) = E_i(y)$ となる確率はせいぜい δ であり，それゆえこの計算の誤り確率は δ である．誤り確率を ϵ まで小さくしたければこの計算を $O(\log \frac{1}{\epsilon})$ 回並列に行えばよく，その場合でも通信量は $O(\log \frac{1}{\epsilon})$ 個のペア $(i, E_i(x))$ を送るためのビット長 $O(\log n)$ （ϵ が定数である限り）で十分となる．

一般的に通信計算量はラウンドの回数，つまり Alice から Bob（または Bob から Alice）への通信を 1 ラウンドとした場合の回数，に依存する．通常のネットワークでは同じ通信量でもラウンド数が多ければより多くの時間がかかることを鑑みると，効率的なのは 1 ラウンドの通信プロトコルであり，一方向であると呼ばれる．例えば，上記の等価性判定問題に関する確率的プロトコルは一方向である．さらに，一方向通信プロトコルの亜種として，次のような 3 者間の一方向通信に限定された場合の通信プロトコル（SMP プロトコル，SMP は Simultaneous Messages Passing の略）がある．Alice と Bob がそれぞれ自分の入力に関するビット列を第 3 者である Referee（彼は自分の入力を持たない）に送って，Bob の代わりに Referee が計算結果を出力する．このような通信プロトコルは，中央集中型ネットワークをイメージしている．興味深いことに，SMP プロトコルのもとでは等価性判定問題に対して指数的な通信計算量の削減を達成することができず，$\Theta(\sqrt{n})$ の通信計算量を必要とすることが知られている [11].

4.2 量子通信プロトコルの例

1979 年の Yao [23] による導入以来，通信計算量は VLSI や回路理論への応用などから計算量理論における重要なトピックであり続けている．そのため，量子情報および量子計算の研究が進むと，自然に量子の力を利用した通信計算量（量子通信計算量）の理論が展開されることとなった．1993 年に Yao [24] は，通信においてビットのような古典情報を用いる代わりに量子ビットのような量子情報を用いる通信計算量モデルを提案した．ここでは，古典に対する劇的な優位性を持ち，かつ比較的シンプルな例として，Buhrman ら [5] の等価性判定問題に対する量子 SMP プロトコルを取り上げる．前節で述べた通り，等価性判定問題は SMP プロトコルのもとでは確率的な計算でさえ各データの長さ n に対して $\Theta(\sqrt{n})$ の通信量を必要とする．ところが，Buhrman らは量子指紋プロトコルという方法で，量子通信を利用すれば SMP プロトコルのもとでさえ $O(\log n)$ の通信量で有界誤りで等価性判定問題を解けることを示したのである．

彼らのプロトコルは，前節の等価性判定問題に対する確率的通信プロトコルのアイデアを利用している．誤り訂正符号 E を前節で与えたものと同一のものとする．このとき，

Alice と Bob は $(\log(m)+1)$ 個の量子ビットからなる状態を表すベクトル $|h_x\rangle$ および $|h_y\rangle$ をそれぞれ Referee に送る．ここで，任意の z に対して $|h_z\rangle$ はペア $(i, E_i(z))$ の量子的重ね合わせ，つまりベクトル $|i\rangle|E_i(x)\rangle$ の各係数が均等であるような線型結合

$$|h_z\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle|E_i(x)\rangle$$

であり，量子指紋 (quantum fingerprinting) と呼ばれる．$x = y$ のとき，$|h_x\rangle = |h_y\rangle$ であり，$x \neq y$ のとき，ベクトル $|h_x\rangle$ とベクトル $|h_y\rangle$ の内積はせいぜい $\delta m/m = \delta$ であることに注目すると，Referee は 2 人から受け取った量子指紋が同じか内積が δ 以下かを高確率で判定する量子回路があれば等価性判定問題を解くことに成功する．そのような量子回路は以下の通りである．(1) Referee は 2 人から得た状態から状態 $|0\rangle|h_x\rangle|h_y\rangle$ を準備し，最初の量子ビット（すなわち $|0\rangle$）にアダマールゲート H を施し，

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|h_x\rangle|h_y\rangle$$

を得る．(2) 最初の量子ビットが $|1\rangle$ の場合，$|h_x\rangle$ と $|h_y\rangle$ の順番を入れ替える（制御スワップと呼ばれる）．このとき，

$$\frac{1}{\sqrt{2}}(|0\rangle|h_x\rangle|h_y\rangle + |1\rangle|h_y\rangle|h_x\rangle)$$

を得る．(3) 最初の量子ビットに H を施してから最初の量子ビットを計算基底で測定する．このとき，測定前の状態は

$$\frac{1}{2}|0\rangle(|h_x\rangle|h_y\rangle + |h_y\rangle|h_x\rangle) + \frac{1}{2}|1\rangle(|h_x\rangle|h_y\rangle - |h_y\rangle|h_x\rangle)$$

であり, この状態の最初の量子ビットから 1 を得る確率は, ベクトル $\frac{1}{2}(|h_x\rangle|h_y\rangle - |h_y\rangle|h_x\rangle)$ の長さの 2 乗，すなわち $\frac{1}{2} - \frac{|\langle h_x|h_y\rangle|^2}{2}$ である．この確率は $x = y$ のとき 0 で，$x \neq y$ のとき $(1-\delta^2)/2$ 以上なので，0 を得たときに Referee は 2 人のデータが等しいと判定すれば，この量子通信プロトコルの誤り確率は 1 より小さい定数 $(1+\delta^2)/2$ である．やはり誤り確率を十分小さな定数 ϵ まで減らすには，このプロトコルを $O(\log \frac{1}{\epsilon})$ 回並列で行えばよい．そのときの通信計算量は $O(\log \frac{1}{\epsilon}) \times (\log(m)+1) = O(\log n)$ である．

この等価性判定問題に対する量子通信プロトコルを古典的な通信プロトコルに変形できないのか，というのは自然な疑問である．ポイントとなっているのは，Alice がペア $(i, E_i(x))$ の全て，そして Bob がペア $(j, E_j(y))$ の全てを量子重ね合わせにして送っている部分であり，それら 2 人からの量子重ね合わせから $i = j$ となるような部分の $E_i(x)$ と

$E_j(y)$ の比較を可能にする方法にある．確率的通信プロトコルでは重ね合わせのまま情報を送れない以上，Alice と Bob は個々にペア $(i, E_i(x))$ と $(j, E_j(x))$ を選択しないといけないが，そのようなペアのインデックス i と j が合致する確率は指数的に小さい．この点で上記の量子通信プロトコルは，量子状態特有の利点を最大に生かしたものといえよう．

Buhrman らのプロトコルは，SMP プロトコルという制約のもとで，量子と古典の通信計算量に関する指数的ギャップを与えている．では通信プロトコルに制約のない場合はどうであろうか？指数的なギャップを与える問題は存在する [17] が，関係として記述される人工的問題である．等価性判定問題のように対象となる問題がブール関数で記述される場合，現時点で知られている最大の量子・古典間のギャップは平方である（Disjointness と呼ばれる関数に対して得られたギャップであり，古典通信計算量 $\Theta(n)$ に対して，量子通信計算量 $\Theta(\sqrt{n})$ [1, 18]）．指数的なギャップが達成可能か否かは，重要な未解決問題として多くの研究者が奮闘中であるが，いまだ解かれていない．一方向通信プロトコルという制約のもとでは，量子・古典間のギャップは高々 2 倍のギャップしか示されていない（等価性判定問題に対して得られたギャップで，古典 $\log n$ に対して量子 $\frac{1}{2}\log n$ [22]）．一方で，プロトコルの誤り確率が有界誤りであるという条件を（計算量クラス **PP** の定義のように）非有界誤りという条件に変更すると，どんなブール関数に対しても古典通信計算量は量子通信計算量のちょうど 2 倍であることが証明されている [9].

参考文献

[1] S. Aaronson and A. Ambainis. Quantum search of spartial regions. *Theory of Computing* **1** (2005) 47–49.

[2] L. M. Adleman, J. DeMarrais, and M. A. Huang. Quantum computability. *SIAM Journal on Computing* **26** (1997) 1524–1540.

[3] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, Cambridge, 2009.

[4] E. Bernstein and U. Vazirani. Quantum complexity theory. *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, pp. 11–20, 1993. Final version appeared in *SIAM Journal on Computing* **26** (1997) 1411–1473.

[5] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting, *Physical Review Letters* **87** (2001) Article no. 167902.

[6] A. M. Childs and W. van Dam. Quantum algorithms for algebraic problems. To appear in *Review of Modern Physics*. arXiv:0812.0380 (2008).

[7] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of Royal Society of London A* **400** (1985) 97–117.

[8] D. Deutsch. Quantum computational networks. *Proceedings of Royal Society of London*

A **425** (1989) 73–90.

[9] K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. Unbounded-error one-way classical and quantum communication complexity. *Lecture Notes in Computer Science* **4596** (2007) 110–121.

[10] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. Graduate Studies in Mathematics, Vol. 47, American Mathematical Society, Rhode Island, 2002.

[11] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, Cambridge, 1997.

[12] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[13] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[14] H. Nishimura and M. Ozawa. Computational complexity of uniform quantum circuit families and quantum Turing machines. *Theoretical Computer Science* **276** (2002) 147–181.

[15] H. Nishimura and M. Ozawa. Perfect computational equivalence between quantum Turing machines and finitely generated uniform quantum circuit families. *Quantum Information Processing* **8** (2009) 13–24.

[16] M. Ozawa. Quantum nondemolition monitoring of universal quantum computers. *Physical Review Letters* **80** (1998) 631–634.

[17] R. Raz. Exponential separation of quantum and classical communication complexity. *Proceedings of 31st ACM Symposium on Theory of Computing*, pp.358–367, 1999.

[18] A. A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya Mathematics* **67** (2003) 145–159.

[19] Y. Shi. Both Toffoli and Controlled-NOT need little help to do universal quantum computation. *Quantum Information and Computation* **3** (2003) 84–92.

[20] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science*, pp.124–134, 1994. Final version appeared in *SIAM Journal on Computing* **26** (1997) 1484–1509.

[21] D. Simon. On the power of quantum computation. *Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science*, pp.116–123, 1994. Final version appeared in *SIAM Journal on Computing* **26** (1997) 1474–1483.

[22] A. Winter. Quantum and classical message protect identification via quantum channels. *Quantum Information and Computation* **4** (2004) 564–578.

[23] A. C.-C. Yao. Some complexity questions related to distributed computing. *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, pp. 209–213, 1979.

[24] A. C.-C. Yao. Quantum circuit complexity. *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, pp. 352–361, 1993.