7 量子通信計算量理論 ―花子から太郎へ

西村 治道〔大阪府立大学理学系研究科〕
レイモンド ルディ〔日本 IBM 東京基礎研究所〕

1993 年の Yao による導入以降，量子通信計算量理論は量子計算量理論における重要なトピックの 1 つであり続けている．特に，ラウンド数制限のもとでの量子通信計算量理論は近年多くの興味深い結果が生み出されている．本稿では，量子通信計算量理論に関する近年の成果のいくつかを紹介する．

通信計算量理論とは

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 つの計算機にすべ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．そのような状況において，問題を高速に解決する上で鍵となるのは，いかに計算機間の通信量を削減できるかにある．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[6] である．最も分かりやすい例として，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)を考えよう．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 は花子が，データ y は太郎が持つものとする☆1．この場合，最も安易な方法は花子が x そのものを太郎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非常に通信量的には非効率的な方法である．ではよりよい方法は存在するのか？　もし太郎のデータ y が x と違う長さであるなら，花子が彼女の x の長さを表すビット列を送ることで，指数的に少ない通信量で正しく等価性判定問題を解ける．しかし，この手は彼らのデータが同じ長さである場合は使えない．実は，この一見非常に簡単そうな問題でさえ花子が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，花子と太郎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，結局通信量を減らすことはできないことが知られている[6]．

このように書くと，通信プロトコルは大抵の問題で少なくともどちらかの入力の長さ分だけの通信量を必要とし，あまり面白みのあることができないのではないかと考えられるかもしれない．実際，通信計算量理論は通信量の下限を回路計算量の下限のような計算量理論などに応用することがより重要な一側面である．では，通信計算量の上限はほとんど自明で研究意義がないのか，というとそうではない．特に，確率的通信プロトコル，つまり乱数（ランダムな数）の使用のもとで少しの誤りを認めた通信プロトコルでは通信計算量が劇的に減少する場合がある．たとえば前述の等価性判定問題を再考しよう．前述の観察よりデータの長さが異なる場合は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（つまり $|x| = |y| = n$）である場合を考えよう．通常の誤りのない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．アイディアは，多少の誤りが認められると，花子と太郎は自らのデータを少し冗長にすることで，花子と太郎のどのデータ内の対応する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，誤り訂正符号 $E : \{0, 1\}^n \to \{0, 1\}^m$ として，任意

☆1 量子情報では Alice と Bob がお馴染みだが，本稿は日本語なので日本人に登場していただくことにしよう．

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（たとえば Justesen 符号）があるので，花子はランダムに選んだ $i \in [m] = \{1, 2, \ldots, m\}$ に対して $E(x)$ の i 番目のビット $E_i(x)$ と i そのものを太郎に送る．太郎は $E_i(y)$（これは花子が 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，それゆえこの通信プロトコルの誤り確率は 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，つまり花子から太郎（または太郎から花子）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，一方向通信プロトコルと呼ばれる．たとえば上記の等価性判定問題に関する確率的通信プロトコルは一方向通信プロトコルである．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（以下，通常の一方向通信プロトコルと区別するために SMP[☆2] プロトコルと呼ぶ）に限定された場合の通信プロトコルがある．花子と太郎がそれぞれ自分の入力に関するビット列を第三者である次郎（彼は自分の入力を持たない）に送って，太郎の代わりに次郎が計算結果を出力する（**図 -1**）．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．ところが興味深いことに，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 [6]．

その誕生以来，通信計算量理論は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理論（量子通信計算量理論）が展開されることとなった．以下では，量子通信計算量理論に関する 4 つのトピックを紹介したい．第 1 に SMP プロトコルにおける量子通信利用の優位性を紹介する．第 2 に，一方向通信プロトコルにおける量子通信の優位性を紹介する．第 3 に，通信プロトコルにおける異なる量子的方法の利用とその優位性を紹介する．最後に，量子通信計算量理論における重要な基礎技術である量子ランダムアクセス符号を紹介する．

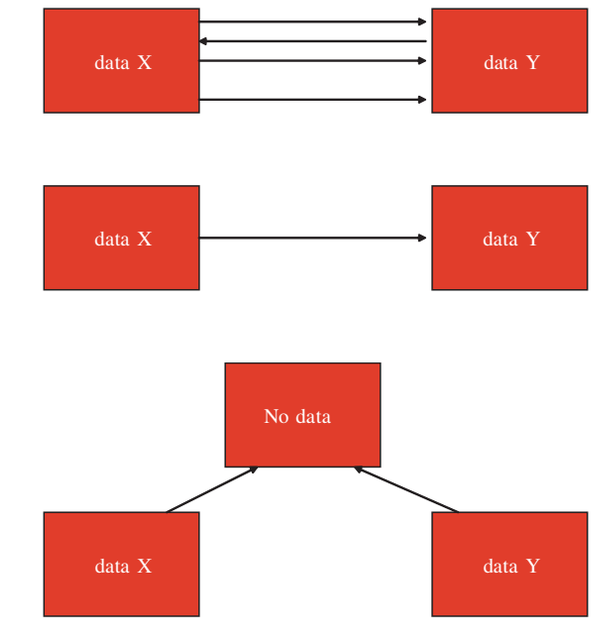

図 -1　通信プロトコルにおける通信の流れ．上から順にラウンド数に制限のない通信プロトコル，一方向通信プロトコル，SMP プロトコル．

SMP プロトコルにおける量子通信の優位性

1993 年に Yao 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プロトコルの概念を提案した．量子通信を用いたプロトコルでの通信計算量は量子通信路を通じて送られる量子ビットの数であり，量子通信計算量と呼ばれる．その比較上しばしば従来の通信計算量は古典通信計算量と呼ばれる．Yao の提案後，1998 年の Buhrman-Cleve-Wigderson による平方的な通信量削減を与える問題や 1999 年の Raz による指数的な通信計算量の削減を与える問題の発見によって，量子通信の通信プロトコルにおける有用性が明らかになった．そしてこれらの結果に劣らないインパクトを与えたのが，2001 年の Buhrman ら [3] の等価性判定問題に対する通信プロトコルである．前章で述べたとおり，等価性判定問題は SMP プロトコルのもとでは確率的プロトコルでさえ通信計算量 $\Theta(\sqrt{n})$ である．ところが Buhrman らは，量子通信を利用すれば SMP プロトコルのもとでさえ量子通信計算量 $O(\log$

☆2　SMP は Simultaneous Message Passing の略である．

n) により高確率で等価性判定問題を解けることを示した．彼らの通信プロトコルは比較的シンプルだが，Shor のアルゴリズムとも Grover のアルゴリズムともまったく異なる．ここでは簡単に彼らの通信プロトコルを紹介したい．

彼らの通信プロトコルは，前章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ィアを利用している．誤り訂正符号 E を前章で与えたものと同一のものとする．このとき，花子と太郎は $(\log(m)+1)$ 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 $|h_y\rangle$ をそれぞれ次郎に量子通信路を通じて送る．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 $|i\rangle|E_i(x)\rangle = |i\rangle \otimes |E_i(x)\rangle$ 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，次郎は 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的手続きがあれば等価性判定問題を解くことに成功する．そのような量子手続きは以下の通りである．(1) 次郎は 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 $|0\rangle$）にアダマール変換 H を施す．このとき H は $|0\rangle$ を $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$，$|1\rangle$ を $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ に変換するので，

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

を得る．(2) 次郎は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）．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標準基底 $\{|0\rangle, |1\rangle\}$ 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 を得たときに次郎は 2 人のデータが等しいと判定すればこの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，この通信プロトコルを $O(\log \frac{1}{\epsilon})$ 回並列で行えばよい．そのときの量子通信計算量は $O(\log \frac{1}{\epsilon}) \times (\log(m) + 1) = O(\log n)$ である．

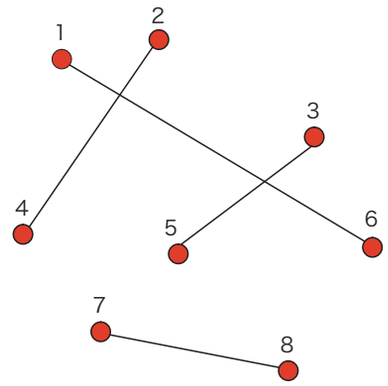

図-2　完全マッチング M の例：$n = 8$ の場合で $M = \{(1, 6),(2, 4),(3, 5),(7, 8)\}$.

この等価性判定問題に対する通信プロトコルを確率的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．実際，ポイントとなっているのは花子はペア $(i, E_i(x))$ のすべてを，太郎はペア $(j, E_j(y))$ のすべ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花子と太郎は個々にペア $(i, E_i(x))$ 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．この点において上記の通信プロトコルは量子状態特有の利点を最大に活かしたものである．

一方向通信プロトコルにおける量子通信の優位性

前章では，SMP プロトコルに関する量子通信利用の優位性を紹介したが，一方向通信プロトコルに関して古典と量子の指数的ギャップを示すことは近年まで未解決であった．2004 年に Bar-Yossef ら [2] は以下の問題 HM_n (Hidden Matching) において，一方向通信プロトコルの通信計算量は量子のそれが古典よりも指数的に小さいことを示した．

問題 HM_n

花子のデータ：$x \in \{0, 1\}^n$

太郎のデータ：$[n]$（で番号付けられた頂点）上の完全マッチング M（**図 -2** 参照のこと）

出力：$b = x_i \oplus x_j$ かつ $(i, j) \in M$ であるような組 (i, j, b)

問題 HM_n を解く通信プロトコルは，以下のとおり非常にシンプルであるが，やはり量子重ね合わせという量子特有の性質をうまく利用したプロトコルである．

HM_n に対する通信プロトコル

(1) 花子は量子状態 $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_i (-1)^{x_i} |i\rangle$ を太郎に送る．

(2) 太郎は量子状態 $|\psi\rangle$ を基底 $\left\{\frac{1}{\sqrt{2}}(|s\rangle \pm |t\rangle) \mid (s, t) \in M\right\}$ のもとで測定し，状態 $\frac{1}{\sqrt{2}}(|s\rangle + |t\rangle)$（に対応する測定値）を得た場合，$(s, t, 0)$ を出力する．状態 $\frac{1}{\sqrt{2}}(|s\rangle - |t\rangle)$ を得た場合，$(s, t, 1)$ を出力する．

上記の通信プロトコルの成功確率が 1 であることは，以下のように簡単に確かめられる．ある $(i, j) \in M$ に対して $|\psi\rangle$ は (1) $x_i = x_j$ の場合，ベクトル $\frac{1}{\sqrt{n}}(|i\rangle + |j\rangle)$ を含み，(2) $x_i \neq x_j$ の場合，ベクトル $\frac{1}{\sqrt{n}}(|i\rangle - |j\rangle)$ を含むことから，測定によって 1 つの枝 (i, j) に対して正しい組 $(i, j, x_i \oplus x_j)$ を得る確率はそれらのベクトルの長さの 2 乗，すなわち $2/n$ である．M は $[n]$ 上の完全マッチングであるため枝の数は $n/2$ であり，それゆえ正しい組を得る確率は $2/n \times n/2 = 1$ となる．また，この通信プロトコルの量子通信計算量は明らかに $\log n$ である．一方，HM_n に関する古典通信計算量の下界は $\Omega(\sqrt{n})$ であり，これは上界と一致することが示されている [2]．この下界のアイディアのポイントとなっているのは，次のような直感にある．太郎は彼が持つ完全マッチングの中の 1 つ (i, j) に対して，花子のデータの情報 $x_i \oplus x_j$ を見つけたい．しかし，花子はどのような組を太郎が持つか知らない．よって，いわゆるバースデーパラドックスを当てに，$O(\sqrt{n})$ 個の組 (i', j') に対する $x_{i'} \oplus x_{j'}$ をランダムに選んで送るしかない．この直感は，情報理論的手法と完全マッチングのグラフ構造を利用して証明されている．

量子通信以外の量子的方法の優位性

最初の章では確率的通信プロトコルを用いると，等価性判定問題の通信計算量が誤りのない通信プロトコルに比べ指数的に小さくできることを紹介した．その通信プロトコルでは花子と太郎はお互い自らの乱数を個々に用いていた．その一方で，彼らが共通の（つまり 2 人が参照できるような）乱数を用いる通信プロトコルも提唱されている．このような事前共有の乱数を認めた通信プロトコルは，ラウンド数に制限のない通信プロトコルや一方向通信プロトコルでは，個々にしか乱数を使用できない場合に比べあまり優位性を持たない．ところが，SMP プロトコルでは大きな優位性を持つ．再び等価性判定問題を考えよう．花子と太郎が事前に乱数を共有していればペアのインデックス i を共同で選択できる．このとき，前述の誤り訂正符号 E のもと $E_i(x)$ と $E_i(y)$ を次郎に送り，次郎はそれらが等しいかどうかをチェックすれば $x = y$ かどうかを一定の確率で判定できる．よって，それを定数回並列的に繰り返せば高確率で等価性判定問題を解ける．この場合の通信計算量はたかだか $O(1)$ であり，事前共有された乱数がない場合の通信計算量 $\Theta(\sqrt{n})$ に比べはるかに優れていることが分かる．

このように考えると，量子的に興味深いのは事前共有しているものが量子状態である場合である．1997 年に Cleve と Buhrman は，花子と太郎があらかじめ量子状態を共有するが使用可能な通信路は古典通信路である（つまりビットしか送信できない）という設定のもと，その量子状態のエンタングルメントを利用した通信プロトコルの概念を考案した．それ以来，事前共有された量子状態を持つ通信プロトコルは，エンタングルメントを研究する 1 つの方向として計算機科学の研究者だけでなく，量子情報理論の研究者からも注目を集めてきた．しかしながら，事前共有された量子状態を持つことがそのような状態を持たない通信プロトコルに比べて大きな優位性を持つ問題の例は，なかなか見つからないままであった．この歴史はまさに，エンタングルメントという量子力学特有の概念が情報理論的にも計算理論的にも未知な部分が多いことを如実に示す一例であった．そんな中，2006 年に Gavinsky ら [4] は SMP プロトコルにおいて，次の事実を示した．ある問題において，量子状態が事前共有された場合における通信プロトコルは，量子状態を事前共有しない通信プロトコルよりも，指数的に通信計算量を減らすことができる．この問題 HP_n (Hidden Parity) は，以下のようであり HM_n にヒントを得ている．

問題 HP_n

花子のデータ：$x \in \{0, 1\}^{n/2}$ および $[n]$ 上の完全マッチングの集合 M

太郎のデータ：$y \in \{0, 1\}^n$

出力：$b_1 = x_{(i,j)}$ および $b_2 = y_i \oplus y_j$ であるような組 (i, j, b_1, b_2)．ただし，$x_{(i,j)}$ は (i, j) に対応する番号を $k = k_{i,j} \in [n/2]$ としたときのビット x_k を表す．

実際，この問題は事前共有された量子状態 $|\phi\rangle = \frac{1}{\sqrt{2}} \sum_{i \in \{0,1\}^{\log n}} |i\rangle |i\rangle$ を使って，以下の通信プロトコルにより古典通信計算量 $O(\log n)$，成功確率 1 で解ける（解析は彼らの論文 [4] を参照していただきたい）．

HP_n に対する通信プロトコル

(1) 太郎は $|\phi\rangle$ を $\frac{1}{\sqrt{n}}\sum_i |i\rangle(-1)^{y_i}|i\rangle$ に変換する．
(2) 花子は各枝 $(i, j) \in M$ に対応する射影作用素 $E_{ij} = |i\rangle\langle i| + |j\rangle\langle j|$ からなる測定を行い，測定結果（仮に (i, j) とする）を得る．
(3) 花子と太郎はそれぞれの $\log n$ 個の量子ビット上でアダマール変換を行い，標準基底のもと測定を行う（花子と太郎の測定結果を仮に k, l とする）．
(4) 花子は $i, j, k, x_{(i,j)}$ を，太郎は l を次郎に送る．
(5) 次郎は $(i, j, x_{(i,j)}, (k + l) \cdot (i + j))$ を出力する．ここで $i, j \in [n]$ に対し，$i \cdot j$ は i と j を $\log n$ ビットと見なしたときのドット積を表す．

一方，Gavinsky らは HP_n に対して，事前共有された量子状態を持たない場合，乱数を事前共有しても，量子通信を利用できても，高確率で解くために通信計算量が少なくとも $\Omega((n/\log n)^{1/3})$ であることを示した．この証明は次章で紹介するランダムアクセス符号の概念や半正定値計画法による状態識別の困難性の量的特徴付けを利用しており本稿では紹介しない．しかし，上記の通信プロトコルにおいて事前共有された量子状態 $|\phi\rangle$ が存在しない場合に同じようなことが可能かを考えてみると，通信計算量が指数的に増えそうなことは感じていただけるのではないかと思う．

量子ランダムアクセス符号（QRAC）

量子通信計算量理論で幅広く使われている手法の 1 つは量子ランダムアクセス符号（以下，QRAC．Quantum Random Access Coding の略）[1] である．たとえば，量子通信計算量の下限については量子通信計算量と VC 次元の関係や前章の Gavinsky らの結果などに使用されている．また，上限については直接の関係がないものの，問題 HM_n のアイディアは局所的復号可能符号 (Locally Decodable Codes) に由来するものであり，この局所的復号可能符号の結果も QRAC に深く関係する．そのほかに，QRAC はアドバイス付き量子計算の解析や量子オートマトンなどにも幅広い応用を持っている☆3．

量子情報理論で有名な Holevo 限界により，n ビットを伝送するのに n 個の量子ビットが必要と知られている．よって，その事実だけを鑑みると量子通信路の使用による利得はないように思える．しかし，Ambainis ら [1] は，受信者の必要な 1 ビットのみが伝送されればよいという条件なら，量子ビットは古典ビットにできないことを実現できるかもしれないと考え，QRAC の概念を導入した．(n, m, p)–QRAC とは，以下のように $x \in \{0, 1\}^n$ を m 個の量子ビットの量子状態 ρ_x に写す関数である．任意の $i \in [n]$ に対して，ρ_x から x_i を確率 p 以上で得るような測定が存在する．その定義から QRAC は n ビットの文字列を m 個の量子ビットに埋め込む符号であると考えられるが，Holevo 限界とは矛盾しない．なぜなら，第 i ビットを取り出す観測による復号では，取り出せるビットの数が 1 個しか保証されないからである．

さて，(n, m, p)–QRAC の存在に関する条件はどのようなものであろうか．Ambainis らの論文 [1] では，以下の m に関する次の下限が与えられている．任意の $p > 1/2$ に対して，(n, m, p)–QRAC が存在すれば $m \geq (1 - H(p))n$ が成立する．ここで，$H(p) = -p \log p - (1 - p) \log(1 - p)$ である．逆に，$m \geq (1 - H(p))n + O(\log n)$ のもと，(n, m, p)–QRAC が存在することが知られており [1]，特にそのような QRAC は古典的符号および復号で達成可能である．このため，漸近的には古典通信でも量子通信でも QRAC を実現する上での差はない．

一方，m が小さい場合に関しては量子通信は古典通信にはできないことを可能にする．$m = 1$ に対しては Ambainis らは $(2, 1, 0.85)$–QRAC が可能なことを観察し，さらにこの事実は Chuang によって $(3, 1, 0.79)$–QRAC の構築へと拡張された．これらは 2 つないし 3 つの基底に関する測定を各ビットに対する復号プロセスとして用意し，量子ビットに対する幾何的描像である Bloch 球の中にそれらの復号プロセスのどれからも正しい値が復号できるように均等に符号を配置することによって得られている．$(2, 1, 0.85)$–QRAC は**図 -3** によって与え

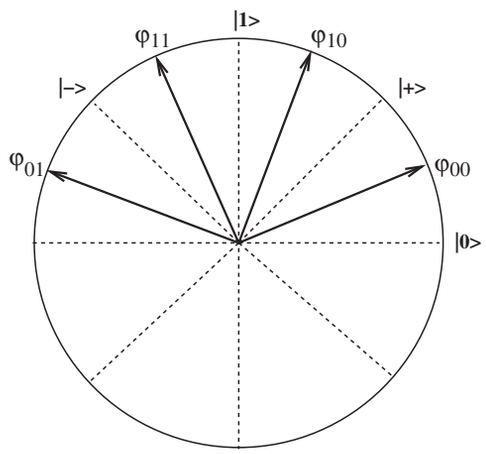

図 -3　(2, 1, 0.85)–QRAC の符号化．量子状態 $\varphi x_1 x_2$ は $x_1 x_2$ の符号化である．復号は第 1, 2 ビットに対してそれぞれ基底 $\{|0\rangle, |1\rangle\}$ および $\{|+\rangle, |-\rangle\}$ に関する測定によってなされる．

☆3　Google によれば，QRAC[1] を参照する論文の合計数は 2006 年 9 月の段階で 43 本である．

られる．たとえば 10 の符号化 φ_{10} は $|1\rangle$ と $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ の中間にあり，第 1 ビット 1 を得るためには標準基底 $\{|0\rangle, |1\rangle\}$ で測定することで $\cos^2 \frac{\pi}{8} \approx 0.85$ の確率で 1 を得る．同様に第 2 ビット 0 を得るには基底 $\{|+\rangle, |-\rangle\}$ で測定すればよい（ただし，$|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ である）．1 ビットによる古典的な符号では 0.5 を超える成功確率さえ不可能であるため，これらの符号化は量子通信のこのタスクにおける優位性を示している．

では，1 個の量子ビットで何ビットの QRAC まで可能であろうか？　このことに関して以前の下限[1]は，十分小さい $\epsilon > 0$ に対しての $(n, 1, 1/2 + \epsilon)$–QRAC に対する限界が自明なものとなって，有意な限界を得ることはできない．しかし，最近の研究によって $\epsilon > 0$ がどんなに小さくても 4 ビットの QRAC は不可能なことが明らかになった：任意の $p > 1/2$ に対して，$(4, 1, p)$–QRAC は存在しない[5]．この結果は (2, 1, 0.85)–QRAC や (3, 1, 0.79)–QRAC の存在を考えると意外なものであるといえる．さらに文献 5)では一般の m に対しても同様に $(m, n, > 1/2)$–QRAC が不可能となるような m が存在することを示している．その m の値は n に関して指数的であるため $(m = 2^{2n})$，実際には n の多項式程度ですでに不可能となるのではないかと考えるかもしれないが，逆に $(2^{\Omega(n)}, n, > 1/2)$–QRAC の存在は通信計算量理論との関連より示されている．

今後残された課題

本稿では量子通信計算量理論について一方向通信プロトコルと SMP プロトコルを中心に近年得られた研究成果のいくつかを紹介した．**表 -1** は本稿で主に取り扱った等価性判定問題の通信計算量を表している．最後に，量子通信計算量理論における今後の研究テーマ・未解決問題について述べる．

(1) 等価性判定問題のようにデータに対して解が常に一意に存在するような問題は全域関数と呼ばれ，理論的興味としても他の理論への応用としても重要視されている．しかし，全域関数における量子通信計算量と古典通信計算量の違いに関して現時点では，複数ラウンドの通信プロトコルの場合さえ量子と古典通信計算量の最大のギャップは平方的でしかない．一方向通信プロトコルに限ると有意なギャップは与えられていない．全域関数においてこれらを超えるギャップが存在するか？

(2) 本稿で述べた通り，事前共有された量子状態によるエンタングルメントの量子計算における有用性は，量子計算量理論において重要な課題の 1 つである．一方向通信プロトコルに関する通信計算量に関して，SMP プロトコルに対する Gavinsky らの結果のようなギャップが可能か？　またラウンド数に制限がない場合はどうか？

	ラウンド制限なし	一方向通信	SMP
誤りなし	n	n	$2n$
確率的	$\Theta(\log n)$	$\Theta(\log n)$	$\Theta(\sqrt{n})$
量子的	$\Theta(\log n)$	$\Theta(\log n)$	$\Theta(\log n)$

表 -1　等価性判定問題に対する通信計算量．n は花子と太郎のデータの長さを表す．いずれも 2 人は乱数または量子状態を事前共有しないものとする．量子的は量子通信を使った場合の量子通信計算量を意味する．

参考文献

1) Ambainis, A., Nayak, A., Ta-shma, A. and Vazirani, U. : Dense Quantum Coding and a Lower Bound for 1-way Quantum Automata, Proc. 31st STOC, pp.376-383 (1999). Journal version appeared in J. ACM, Vol.49, pp.496-511 (2002).
2) Bar-Yossef, Z., Jayram, T. S. and Kerenidis, I. : Exponential Separation of Quantum and Classical One-way Communication Complexity, Proc. 38th STOC, pp.128-137 (2004).
3) Buhrman, H., Cleve, R., Watrous, J. and de Wolf., R. : Quantum Fingerprinting, Phys. Rev. Lett., Vol.87, Article No.167902 (2001).
4) Gavinsky, D., Kempe, J., Regev, O. and de Wolf, R. : Bounded-error Quantum State Identification and Exponential Separations in Communication Complexity, Proc. 40th STOC, pp.594-603 (2006).
5) Hayashi, M., Iwama, K., Nishimura, H., Raymond, R. and Yamashita, S. : (4, 1)-quantum Random Access Coding Does Not Exist — One Qubit Is Not Enough to Recover One of Four Bits, New J. Phys., Vol.8, Article No.129 (2006).
6) Kushilevitz, E. and Nisan, N. : Communication Complexity, Cambridge University Press (1997).

（平成 18 年 10 月 30 日受付）

西村 治道
hnishimura@mi.s.osakafu-u.ac.jp
2001 年名古屋大学大学院人間情報学研究科博士課程修了．2006 年より大阪府立大学理学系研究科講師．量子計算および計算量理論の研究に従事．学術博士．

レイモンド ルディ
raymond@jp.ibm.com
2006 年京都大学大学院情報学研究科博士課程修了．同年より日本 IBM 東京基礎研究所（TRL）の研究員．量子計算とアルゴリズムの研究に従事．情報学博士．