■6 群（コンピュータ‐基礎理論とハードウェア）- 2 編（計算論とオートマトン）

6 章 様々な計算モデルにおける計算複雑さ

（執筆者：河内亮周）［2010 年 4 月 受領］

■概要■

5 章で解説した決定性，非決定性計算以外にも計算量理論やアルゴリズム理論において様々な計算モデル上で理論的解析が進められている．例えば，乱数を使ったアルゴリズムは決定性，非決定性計算の枠組みでは計算量の評価が与えられないため，確率計算のためのモデルで評価しなければならない．また，複数台の計算機が互いに通信を行う計算過程に対しても通信付き計算のためのモデルを用意する必要がある．計算量理論やアルゴリズム理論においては，そのような計算モデル上での計算量の理論的解析も古くから重要視されている．

【本章の構成】

本章では様々な計算モデル及びそのモデル上での計算量に関する重要な結果について解説を行う．（6-1）節では，古くから研究がなされている論理回路を計算モデルとした計算量解析，（6-2）節では二者間の通信による計算モデルにおける計算量，（6-3）節では乱数を用いたアルゴリズムの計算量について，（6-4）節では量子力学の原理を計算機に応用した量子計算機での計算量，（6-5）節では，能力の異なる二者間が対話することで計算を行う対話型証明系と呼ばれるモデルでの計算量について，それぞれ紹介する．

■6 群 - 2 編 - 6 章

6-1 回路計算量

（執筆者：森住大樹）[2008 年 12 月 受領]

本節では，論理回路を計算モデルとする計算複雑さを取り扱う．論理回路の**サイズ**とは，その論理回路に含まれる素子数であり，論理回路の**深さ**とは，その論理回路の段数である．チューリング機械においては計算時間や計算領域が計算複雑さを議論する代表的な指標であるが，論理回路ではサイズや深さがそれに相当する．論理回路のサイズはチューリング機械の計算時間と関連が深く，論理回路におけるサイズの下界を示すことでチューリング機械においての計算時間の下界を示すことが可能であることが知られている．

6-1-1 論理回路と回路計算量

本節では特に言及しない場合，論理回路は図 6･1 のような 2 入力の AND 素子，OR 素子と NOT 素子で構成されるループのない回路とする．論理関数 f の**回路計算量**（circuit complexity）とは，f を計算する最小な回路のサイズである．回路計算量の対象となる回路は様々なものがある．2 変数 1 出力論理関数すべてについて，それを計算する素子を使用可能とする場合も多いが，すべての 2 変数 1 出力関数は AND，OR，NOT 素子をたかだか定数個用いて計算することが可能であるので，両者の回路モデルでの回路計算量はたかだか定数倍しか違わない．この例では該当しないが，回路モデルによっては回路計算量が大きく異なる場合も多数存在する．以降では，主に回路計算量の下界について概説する．

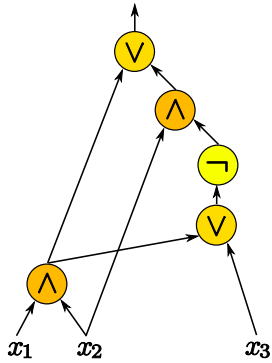

図 6･1　論理回路

6-1-2 非明示的な下界

n 変数論理関数 $f:\{0,1\}^n \to \{0,1\}$ はすべてで 2^{2^n} 通り存在する．この数と，サイズが一定の値以下である回路が何通り存在するかの組み合わせの数を比較することで，回路計算量の下界を得ることが可能である．この証明手法はシャノン（Shannon）の**数え上げ論法**（counting argument）と呼ばれ，その論法に基づき次の定理が得られる．

定理　ほとんどすべての n 変数論理関数の回路計算量は $\Omega(2^n/n)$ である．

定理のような下界は，具体的に回路計算量が $\Omega(2^n/n)$ である関数は特定できていないため，

非明示的な（nonexplicit）下界と呼ばれる．一方，上界については，すべての n 変数論理関数に対して回路計算量は $O(2^n/n)$ であるので，定理の下界は定数係数を除いて最適である．

6-1-3 明示的な下界

本節の冒頭に述べたように，論理回路におけるサイズの下界，つまり回路計算量の下界を示すことでチューリング機械においての計算時間の下界を示すことが可能であることが知られている．特に，NP に関連するある種の論理関数*の回路計算量に対して多項式を超える下界を示したならば P≠NP を証明したこととなり，重要な未解決問題である P 対 NP 問題が解決される．既に述べた非明示的な下界は多項式を十分に超えているが，すべての論理関数を議論の対象としているため P≠NP の証明には不十分である．そこで，明示的に定義された関数に対して回路計算量の下界を示すことが重要となるのだが，現在のところ，最も良い下界でも線形に止まっている．

制限を加えた回路モデルを考えて大きな下界を証明し，制限のない回路に対する下界につなげようとする一つの流れがあり，1980 年代に二つの回路モデルにおいて指数の下界が証明されている．**単調回路**（monotone circuit）とは，AND，OR 素子から構成され NOT 素子を含まない回路である．単調回路でのクリーク関数の回路計算量に対し，指数の下界が証明されている．**定数深さ回路**（constant depth circuit）とは，深さを定数に制限した回路である．ただし，各素子のファンインは無制限とする†．定数深さ回路でのパリティ関数の回路計算量に対し，指数の下界が証明されている．

6-1-4 その他の回路モデル

既に述べた以外に重要な回路モデルには，**論理式**（formula）がある．論理式は，すべての素子のファンアウトが 1 である回路のことである．論理式のサイズは制限なしの回路の深さと密接に関係している．ほかにも様々な回路モデルが存在し，例えば，定数深さ回路において使用可能な素子の種類を増やしたモデル，単調回路の制限を緩めたものに相当する，使用可能な NOT 素子の数を制限した否定数限定回路などがある．最近では，論理回路ではなく各素子が加算または乗算を行う算術回路の研究も盛んである．

表 6･1　主な回路モデルと下界

回路モデル	特徴	回路計算量の下界
一般の回路	制限なし	線形
単調回路	AND，OR 素子のみ	指数
定数深さ回路	深さを定数に制限	指数
論理式	ファンアウトを 1 に制限	$\Omega(n^{3-o(1)})$

表 6･1 に主な回路モデルと証明されている回路計算量の下界について簡単にまとめた．詳しくは参考文献に記述がある．文献 1, 2) はともに執筆当時までの回路計算量に関する主要な結果を網羅しており，回路計算量に関する代表的な文献である．文献 3) は文献 2) の日本語訳である．

* 論理回路はチューリング機械と異なり入力の長さが固定であるため正確に述べるには準備を要する
† ファンインが 2 で深さが定数では，定数個の入力に依存する関数しか計算できない

■参考文献

1) I. Wegener, “The Complexity of Boolean Functions,” Teubner/Wiley, 1987.
2) R. Boppana and M. Sipser, “The complexity of finite functions,” in Handbook of Theoretical Computer Science, Vol.A: Algorithms and Complexity, ed. by J. van Leeuwen, pp.757-804, Elsevier Science Publishers, 1990.
3) R. Boppana and M. Sipser 著, 西野哲朗 訳, “有限関数の複雑さ,” in コンピュータ基礎理論ハンドブック　アルゴリズムと複雑さ, 廣瀬健, 野崎昭弘, 小林孝次郎 監訳, pp.755-802, 丸善, 1994.

■6 群 - 2 編 - 6 章

6-2 通信計算量

（執筆者：西村治道）［2008 年 12 月 受領］

通信計算量（communication complexity）は，複数の参加者で協調的な計算を行うために必要な通信の量を理論的に研究するための計算モデルであり，その下界は多くの応用をもつ．本節では，通信計算量のモデルとその理論について最新の動向も含めて概観する．

6-2-1 通信計算量のモデル

通信計算量の概念は 1979 年にヤオ（Yao）によって導入された．ここでは，最も基本的なモデルとして 2 者間でのブール関数の計算を取り上げる．アリスとボブはそれぞれの入力として n ビット x，y を与えられ，$\{0,1\}^n \times \{0,1\}^n$ 上のブール関数 f に関しての値 $f(x,y)$ を計算したい．アリスとボブは個々の計算能力に全く制限はなく，関数 f も（関数 f の表をもつなどして）完全に知っている．任意の $(x,y) \in \{0,1\}^n \times \{0,1\}^n$ に対して $f(x,y)$ を正しく計算するためにアリスとボブが通信すべきビット数を f の（決定性）通信計算量といい，$D(f)$ で表す．アリスが x をそのまま送り，ボブが $f(x,y)$ を計算してその値をアリスに教えれば 2 者は $f(x,y)$ を知ることになるので，任意の f に対して $D(f) \le n+1$ が成り立つ．一方で，2 者は相手の入力情報を知る必要は必ずしもないので，通信計算量が $n+1$ より小さいような多くの関数が考えられる．例えば，x と y が含む 1 の数の和のパリティ（偶数か奇数か）を出力とする関数の通信計算量は 2 である．通常，$\log n$ の多項式で押えられる通信計算量をもつ関数が効率的に計算可能な関数とされている．

通信計算量において応用上重要なことは，下界を求めることである．$D(f)$ の下界を求める方法として代表的なものに通信行列のランクがある．f の通信行列とは，x を行，y を列のインデックスとして (x,y) 成分に $f(x,y)$ をもつような 2^n 次正方行列 $M_f = (f(x,y))$ である．基本的事実として，$D(f) \ge \log_2(2\mathrm{rank}(M_f)-1)$ が知られている．例えば，関数 $EQ(x,y) = 1$（$x = y$ のとき），0（$x \ne y$ のとき）は通信行列が 2^n 次単位行列となるため，$D(EQ) \ge \log_2(2\cdot 2^n - 1) \ge n$ が示される．通信行列のランクは（EQ のように）多くの関数に対して緊密な下界を導出するが，$D(f)$ を完全に特徴づけるわけではない．実際に，$\log_2 \mathrm{rank}(M_f) = O(n^{1/\log_2 3})$ であるが，$D(f) = \Omega(n)$ であるような関数の存在が知られている．その一方で，任意の f に対して，$D(f) = (\log_2 \mathrm{rank}(f))^{O(1)}$ であることが予想されているが，現在も未解決のままである．

通信計算量のモデルは，その応用に応じて関数以外の問題への拡張，通信形態，計算への参加人数など様々なバリエーションがあり，詳細はこの分野の代表的テキスト[1)]に委ねる．本節では，回路計算量の下界の研究において重要な応用をもつ多者間の通信計算量（NOF モデル）について触れておく．k 人の参加者は共通に見ることのできる黒板を介して通信することにより，協調して $(\{0,1\}^n)^k$ 上のブール関数 $f(x_1, x_2, \ldots, x_k)$ を計算したい．ただし，i 番目の参加者は入力 $x_i \in \{0,1\}^n$ だけを見ることができない．状況としては x_i が書かれた紙が i 番目の参加者の額にはってあることを想像するとわかりやすい．この多者間での通信計算量のモデルは NOF モデル（Number-On-the-Forehead）と呼ばれ，複数の参加者が多くの入力を共有していることが下界を得ることを驚くほど難しくしている．$k = (\log n)^{\Omega(1)}$ のもとで通信計算量が $(\log n)^{\omega(1)}$ であるような関数は，回路計算量クラス ACC^0 に属さない明示的な関数の発見に繋がるため，$k \ge \log n$ における非自明な通信計算量をもつ可能性のある関数は，

近年も変わらず精力的な研究がなされている．

6-2-2 乱択及び量子通信計算量

ほかの計算モデルの例に漏れず，通信計算量も決定性，非決定性をはじめとして様々な計算の様相が考えられている．特に乱択通信計算量と量子通信計算量は近年における研究の盛んな様相である．乱択通信計算量ではアリスとボブは乱数を使って計算を行うことが認められている．関数 f の誤り ϵ での乱択通信計算量 $R_\epsilon(f)$ は，f を誤り確率 $< \epsilon$ で計算するために必要な通信ビット数を表す．例えば，関数 EQ は入力を有限体上の多項式を用いて符号化することで，$O(\log n)$ ビットの通信で高確率（例えば確率 2/3）で計算できるため，$R_{1/3}(EQ) = O(\log n)$ である．ゆえに，チューリング機械を基とする計算量クラスと異なり，効率的な乱択通信計算量をもつ関数のクラスと効率的な決定的通信計算量をもつ関数のクラスの差異は明示的である．$R_{1/3}(f)$ も通信行列を近似する行列に関するランク（近似ランク）を使って下界を与えることができるが，決定性の場合同様に完全な特徴づけを与えるには至っていない．一方で，$R_{1/2}(f)$ は（しばしば学習理論で出現する）サインランクと呼ばれる行列のランクに関する指標と値がほぼ完全に一致することが知られている．

量子通信計算量では量子通信，すなわち通信にキュビット（量子ビット）を利用することが認められる．$Q_\epsilon(f)$ は関数 f を誤り確率 $< \epsilon$ で計算するために必要なキュビット数とする．量子通信計算量は通信媒体自体がビットからキュビットに代わるため，より効率的な計算が可能となることが期待される．確かに，f が部分関数である場合は $Q_{1/3}(f)$ が $R_{1/3}(f)$ より指数的に小さいような関数が発見されている．しかし，f が全域関数の場合は，2 乗のギャップをもつ関数しか発見されておらず，超多項式のギャップをもつか否かは未解決である．一方で，$Q_{1/2}(f)$ は $R_{1/2}(f)$ の約 1/2 であることが知られている[2)]．

乱択通信計算量 $R_{1/3}(f)$ では，アリスとボブで乱数を個々に使用するか共有の乱数を用いるかで大きな差はないことが知られている．一方，量子通信計算量では，アリスとボブが共有の量子状態を利用することを認めた量子通信計算量 $Q^*_{1/3}(f)$ が $Q_{1/3}(f)$ とほとんど差がないか否かは未解決である．加えて $Q^*_\epsilon(f)$ はその下界を与えることが $Q_\epsilon(f)$ に比べて困難である．近年，$Q^*_\epsilon(f)$ の下界を与える新しい証明法が開発され，それらの手法は NOF モデルにおける乱択通信計算量など量子でない通信計算量の下界にも応用されている[3)]．

6-2-3 通信計算量の応用

そもそも通信計算量は，計算における情報のやり取りで不可避なボトルネックを量的に評価するための抽象的計算モデルとして導入された．それゆえ通信計算量の下界は，VLSI のサイズのような導入初期の応用をはじめとして，チューリング機械，オートマトン，各種回路の計算量，決定木やデータ構造，果ては疑似乱数に至るまで非常に幅広い応用がある[1)]．近年では，1990 年代後半に端を発するストリームアルゴリズム[4)]の限界を証明する上で，通信計算量の下界が幅広く用いられている．

■参考文献

1) E. Kushilevitz and N. Nisan, “Communication Complexity,” Cambridge University Press, Cambridge, 1997.
2) K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, “Unbounded-error classical and quantum communication complexity,” in Proc. 18th International Symposium on Algorithms and Computation, Lecture Notes in Comput. Sci., vol.4835, pp.100-111, 2007.
3) A.A. Sherstov, “Communication lower bounds using dual polynomials,” Bull. Eur. Association Theoretical Comput. Sci., vol.95, pp.59-93, 2008.
4) 徳山豪, “オンラインアルゴリズムとストリームアルゴリズム,” 共立出版, 2007.

■6 群 - 2 編 - 6 章

6-3 乱択計算

（執筆者：渡辺　治）[2009 年 3 月 受領]

乱択計算とは，計算過程にランダム性が入ってくる計算である．具体的には乱数を利用して計算を行う乱択アルゴリズムが表す計算である．通常の計算は，入力が定まれば計算過程が一意に定まる決定性計算である．それに対し，計算の途中で乱数を使用すると計算過程が一意に決まらない．そのことで，計算が不安定になる可能性もあるが，通常の決定性計算では得られない効率や効果が得られる場合がある．本節では，乱択計算の意義を議論し，乱択計算に関する計算の複雑さの研究について述べる．

6-3-1 乱択計算の意義

乱択アルゴリズムを例示しながら，乱択計算の効果と重要性について述べる（乱択アルゴリズムについては文献 1, 2) 参照）．

(1) 新たなトレードオフが産み出す効果

乱択計算のように新たな計算モデルを考えると，これまでになかった価値基準と代償と効果の間の新たなトレードオフ関係が導入され，従来の枠組みでは思いつかなかった効果を見だせる場合がある．乱択計算の重要性にもこの側面がある．乱択アルゴリズムでは乱数を利用してランダムな選択を行う．そのために，乱数の出目が悪く，悪い選択をしてしまう場合もある．しかし，その可能性が低いのであれば，それを許容することにより，別の意味で良い計算を行える場合がある．このトレードオフが新たな効果を産み出している．

数列の整列アルゴリズムとして有名なクイックソートの乱択版がその一例である．クイックソートは，配列に与えられた数の列を小さい順に並べ替えるアルゴリズムである．決定性のクイックソートは，大抵の入力列ならば高速に整列化できる反面，効率が極端に悪くなる入力列があることも知られている．それに対し，計算過程にランダム性を導入することで，苦手な入力列をなくすようにしたのが乱択版クイックソートである．どのような列が与えられたとしても高い確率で十分高速に整列化が可能となるのである．ただし，その代わりに失うものもある．決定性では確実に高速に処理できる入力列に対しても，ランダムの出方によっては処理が遅くなる可能性が 0 ではなくなったのである．このような運の悪い計算が（小さな確率で）起きることを認めることにより，苦手な入力列を解消でき，アルゴリズムがより安定的に働くことが保証できたのである．

トレードオフ関係は誤りと効率の間にも現れる．乱数の出目が悪いと誤りを起こす可能性もあるが，それを許すことで計算効率を大幅に改善できる場合があり，その有効性を生かした乱択アルゴリズムも多く提案されている．その例が Rabin-Miller 型の素数判定アルゴリズムである．このアルゴリズムでは，与えられた整数 N に対し，ある範囲内からランダムに選んだ乱数 x を用いた簡易判定テストを行う．この簡易判定テストは高速に行うことができる．N が素数の場合には，乱数 x の値にかかわらず，簡易判定テストで正しく「素数」と判定される．一方，N が合成数の場合には，x の値に応じて簡易判定テストの結果が変わる．正しく「合成数」と判定される場合もあれば，合成数なのに「素数」と判定されてしまう場合もある．ただし，そのような誤答確率は 1/4 以下であることが保証できるので，その程度の誤

りを許せば*，決定性のものよりはるかに高速な判定を行うことができるのである．

(2) 乱択計算の技術的な効果

新たな価値基準だけでなく，技術的にも乱数の様々な性質が計算に生かされている．その代表例の二つを紹介する．

一つ目は乱数の一様性の利用である．対象とする問題や実現したい計算の完全な解明が難しい場合がある．そのような場合でも，多くの選択肢で正しい計算が行えることさえ分かれば，乱択アルゴリズムが設計可能である．選択肢のなかから一つを乱数を用いて選べば，乱数の一様性から，ある程度の確率で正しい計算への選択肢が選ばれることが保証できるからである．先の素数判定アルゴリズムの場合がその一例である．与えられた N に対して，妥当な x を用いれば，N の素数判定を正しく行うことができる．ただ，その x を特定することは現在の数学では難しい．しかし，多くの x が妥当であることは保証できたので，ランダムに x を選んでテストする乱択アルゴリズムを提案できたのである．

二つ目は乱数の予測不可能性の利用である．予測不可能性とは，次に出てくる乱数が何であるかが予測できない，という性質である．この性質は，コンピュータゲームで戦略を決めるとき，あるいは暗号通信の際の暗号鍵を決めるときなど，相手（仮想敵）を想定した計算では重要な性質であり，情報セキュリティ関連のアルゴリズムで用いられている．更にその考え方を発展させたアルゴリズムの設計手法が，対話型証明系〔本章 6-5〕や確率的検査可能証明〔本編 7 章 7-2〕の基礎となるアルゴリズムを産み出している．

6-3-2 乱択計算の複雑さ

乱択計算が決定性計算に比べて本質的に有効であるか否かは，計算の複雑さの重要な研究課題の一つである．特に多項式時間計算の枠組みのなかでは，P や NP などの計算量クラスや擬似乱数生成器などと関連して，乱択計算の計算量クラスの位置づけが深く研究されてきた．その代表的なものを紹介する（詳しくは文献 3, 4) を参照)．

(1) 多項式時間乱択計算量クラス

計算の複雑さの理論では，様々な計算モデルの能力の比較をする際に，対応する計算量クラスの関係を調べる．ここでも，まず多項式時間乱択計算量クラスとして妥当と思われるものをいくつか定義しよう．

乱択アルゴリズムによって記述される乱択計算のモデルとして乱択チューリング機械を考えることができる．一言でいえば，従来の決定性チューリング機械に，0 と 1 の二値の乱数を発生させる装置が付加された機械と考えればよい．このため乱択チューリング機械の実行結果は，この乱数の系列に依存した確率変数となる．

ほかの計算量クラスと同様，乱択計算量クラスを考える際には，問題を判定問題あるいは，ある適当なアルファベット Σ 上の言語の認識問題に限って考えるのが普通である．その場合，チューリング機械 M も，任意の入力 $x \in \Sigma^*$ に対して，実行結果 $M(x)$ が受理または拒否のいずれかとなる認識機械に限定される．ただし，M が乱択チューリング機械の場合には，$M(x)$

* 1/4 の誤答確率は許しがたいかもしれない．しかし，同じテストを独立に選んだ乱数を用いて 5 回行い，すべての判定が「素数」のときのみ「素数」と判定すれば，誤答確率は一気に 1/1024 以下になる．この種のアルゴリズムは，一般に複数回独立に実行して，その結果を総合して結果を出すことで，誤答確率を急速に小さくし，正答確率を限りなく 1 に近づけることができる．この手法を正答確率増幅法という．

は実行中に使用した乱数の系列に依存した確率変数である．この確率変数を用いて M が認識する言語 $L(M)$ は以下のように定義される．

$$L(M) = \{ x \mid \Pr[\, M(x) = \text{受理} \,] > 1/2 \} \tag{6・1}$$

この意味で多項式時間乱択チューリング機械により認識される言語のクラスがクラス PP である．ただし，この基準だけでは誤答確率が大きく，実際的な乱択計算からは程遠い計算も含んでしまっているため，PP は多項式時間乱択計算量クラスとしては妥当ではない．クラス PP は，むしろ計数クラス #P〔本編 7 章 7-8〕の判定問題版とみなした方が自然である．

妥当な乱択計算を議論するには誤答確率を考慮する必要がある．一般に，言語の認識器としての乱択チューリング機械 M の入力 x 対する誤答確率 $\mathrm{err}(x; M)$ は，

$$\mathrm{err}(x; M) = \begin{cases} \Pr[\, M(x) = \text{拒否} \,], & x \in L(M) \text{ のとき} \\ \Pr[\, M(x) = \text{受理} \,], & x \notin L(M) \text{ のとき} \end{cases} \tag{6・2}$$

と定義される．更に，M の正負の最大誤答確率 $\mathrm{err}_+(M), \mathrm{err}_-(M)$ を以下のように定義し，全入力を通しての最大誤答確率を $\mathrm{err}(M) = \max(\mathrm{err}_+(M), \mathrm{err}_-(M))$ と定義する．

$$\mathrm{err}_+(M) = \max_{x \in L(M)} \mathrm{err}(x; M), \quad \mathrm{err}_-(M) = \max_{x \notin L(M)} \mathrm{err}(x; M)$$

乱択チューリング機械 M を，その最大誤答確率 $\mathrm{err}(M)$ により分類する．定義から常に $\mathrm{err}(M) \le 1/2$ が成り立つが，適当な定数 $\varepsilon < 1/2$ に対して $\mathrm{err}(M) \le \varepsilon$ となる乱択チューリング機械 M を限定誤答確率をもつ機械と呼ぶ．このような機械で表される乱択計算を妥当と考える．$\mathrm{err}(M) \le \varepsilon$ であれば，正答確率増幅法を用いて誤答確率を急速に小さくさせることが可能だからである．M によっては，$\mathrm{err}_-(M) > 0$ だが $\mathrm{err}_+(M) = 0$ となる場合もある．つまり正の入力に対しては誤らない場合である．このような機械を負の片誤り機械と呼ぶ．例えば素数判定を行う Rabin-Miller 型乱択アルゴリズムは，負の片誤り機械に対応する．正の片誤り機械も同様に定義できる．これらに対しても正答確率増幅法を使えるので妥当な乱択機械である．以上のような限定された誤答確率をもつ多項式時間乱択チューリング機械を用いて定義されるのが，以下の計算量クラスである．これらを妥当な多項式時間乱択計算量クラスとみなすことができる．

$$\begin{aligned} \mathrm{BPP} &= \{ L(M) \mid M \text{ は多項式時間の限定誤答確率機械} \} \\ \mathrm{RP} &= \{ L(M) \mid M \text{ は多項式時間の負の片誤り機械} \} \\ \text{co-RP} &= \{ L(M) \mid M \text{ は多項式時間の正の片誤り機械} \} \\ \mathrm{ZPP} &= \mathrm{RP} \cap \text{co-RP} \end{aligned} \tag{6・3}$$

最後のクラス ZPP は，ゼロ誤答確率クラスとも呼ばれている．$L \in \mathrm{ZPP}$ に対しては，それを認識する負の片誤り機械 M_- と正の片誤り機械 M_+ の両方が存在するので，その両者が同じ答えを出すまで繰り返し実行すれば，誤答確率を 0 にすることができるからである．ただし，多項式時間内に止まらないこともあるので，それだけでは P に等しいとはいえない．

(2) 乱択計算量クラスの解析

以上のように定義した乱択計算量クラスについて，クラス間の関係やほかのよく知られている計算量クラスとの関係を示しながら，乱択計算の特徴や能力について考えてみよう．

まず定義より簡単に導ける関係を整理すると以下のようになる．

$$\mathrm{ZPP}\,(\ =\ \mathrm{RP}\cap\mathrm{co\text{-}RP})\ \subseteq\ \mathrm{RP}\cup\mathrm{co\text{-}RP}\ \subseteq\ \mathrm{BPP}\ \subseteq\ \mathrm{PP}$$

$$\mathrm{P}\ \subseteq\ \mathrm{RP}\ \subseteq\ \mathrm{NP}\ \subseteq\ \mathrm{PP},\quad \mathrm{P}\ \subseteq\ \mathrm{co\text{-}RP}\ \subseteq\ \mathrm{co\text{-}NP}\ \subseteq\ \mathrm{PP}$$

この関係からも分かるように，片誤り乱択計算は決定性計算と非決定計算の中間に位置している．一方，限定誤答率の乱択計算も実質的な妥当性からみると決定性計算に準じる計算とみなせるが，計算量クラスとして BPP ⊆ NP が成立するかは，いまのところ分かっていない．

計算量クラス BPP の上界として今のところ知られている結果は以下の関係である（各式の右辺の計算量クラスについては本編 5 章 5-3，本章 6-1 参照）．

$$\mathrm{BPP}\ \subseteq\ \mathrm{SIZE[poly]},\quad \mathrm{BPP}\ \subseteq\ \Sigma_2^{\mathrm{p}}\cap\Pi_2^{\mathrm{p}}$$

これらの証明は自明ではないが，その基本は正答確率増幅法である．誤答確率を非常に小さくすることで，同じサイズのすべての入力を正答に導く万能な乱数系列の存在を示すことができる．乱択計算のこの特徴づけから上記の関係が導けるのである．

最後に「乱択は計算効率に本質的か？」という根本問題を多項式時間乱択計算の枠組みのなかで考えてみる．例えば「BPP はどのくらい P に近いか？」という問いである．この問いの解明への重要な糸口が実は現代暗号の基礎理論から得られている．現代暗号には様々な計算論的な技術が用いられているが，その一つが暗号的に安全な擬似乱数生成器である．一般に，擬似乱数生成器は短いシードから乱数列のように見える列を生成する決定性アルゴリズムである．決定性アルゴリズムが生成する列なので本当の乱数列ではない．しかし，暗号的に安全な擬似乱数生成器が生成した擬似乱数列に対しては，どのような多項式時間アルゴリズムも見抜くことができないのである．こうした擬似乱数生成器で乱数列を供給すれば，乱択計算も結局は決定性計算とみなすことができる．

暗号的に安全な擬似乱数生成器は，暗号的に安全な一方向関数（例えば安全であることが保証された公開鍵暗号）から構成可能であることが知られている．従って，何らかの公開鍵暗号の安全性が確実に保証できれば，暗号的に安全な擬似乱数生成器の存在が示せ，そこから BPP は決定性でもたかだか弱指数関数時間クラス以下であることが証明できる．

一方向関数と擬似乱数列生成器の関係からも想像できるように，問題の計算困難性のより精密な解析が，より強力な擬似乱数列生成器の存在性を示す鍵になっている．実際，上記の議論を更に発展させ次のような結果も得られている：もしも決定性指数時間計算量クラス E が回路計算量的にみても指数関数的に難しければ，BPP = P である（つまり乱択計算は本質的ではない）．

以上の結果は多項式時間計算という枠組みのなかでは，乱択計算の効果は本質的でないことを示唆している．しかし，それは多項式時間という大ざっぱな括りのなかでの議論だからかもしれない．より粒度の低い効率化や実計算では乱択計算が本質的になる場面も出てくると思われる．また，対話型証明や分散計算など，通常とは異なる環境でも乱択が不可欠な場

合があるだろう.

■参考文献

1) R. Motwani and P. Raghavan, “Randomized Algorithms,” Cambridge Univ. Press, 1995.
2) 玉木久夫, “乱択アルゴリズム,” 共立出版, 2008.
3) “Handbook of Theoretical Computer Science, Vol.A: Algorithms and Complexity,” ed. by J. van Leeuwen, Elsevier, 1990.
4) M. Sipser, “Introduction to the Theory of Computation, 2nd ed.,” PWS Pub., 2005.

■6 群 - 2 編 - 6 章

6-4 量子計算

（執筆者：山下　茂）[2008 年 12 月 受領]

量子状態をコントロールすることによって計算を行う方式を**量子計算**と呼ぶ．有意義な計算ができるほどの大規模な量子計算はまだ実現されていないが，その計算能力は現在の計算方式（以下，古典計算と呼ぶ）を凌駕する可能性があるため次世代の計算方式として注目を集めている．本節では，量子計算のモデルとその計算量クラスに関して説明する．

6-4-1 量子計算のモデル

現在の計算機をモデル化するチューリングマシンで量子状態を扱えるように拡張した**量子チューリングマシン（quantum Turing machine）**により量子計算をモデル化することが可能である．本節では，量子チューリングマシンよりも物理的な動作イメージが理解しやすい**量子回路（quantum circuit）**と呼ばれる量子計算のモデルを説明する．量子回路は，「回路」と呼ばれているが，物理的に配置されたゲート間を配線によって情報を伝達するようなものではなく，**ある量子計算のアルゴリズムが量子状態への操作を行う操作の列を記述したプログラム図**である．量子回路の構成要素は以下の二つである．

量子ビット（quantum bit）　2 量子状態をとる物理系の状態を抽象化したもの．量子力学の公理より，$\alpha|0\rangle+\beta|1\rangle$ という状態（0 と 1 の値の重ね合せ）となることが許されている．ここで，α 及び β は $|\alpha|^2+|\beta|^2=1$ を満たす複素数である．この状態を観測すると，$|\alpha|^2$ の確率で $|0\rangle$，$|\beta|^2$ の確率で $|1\rangle$ となる．

量子ゲート（quantum gate）　（一つまた複数の）量子ビットへのある特定の量子的な操作を抽象化したもの．

量子ゲートには多くの種類が考えられているが，以下の 3 種類の量子ゲートと量子状態の観測及び量子状態の初期化の操作を組み合わせれば，任意の量子計算を任意の精度 $\varepsilon>0$ で近似可能な量子回路を $\mathrm{poly}(\log(1/\varepsilon))$ のゲート数で実現することが可能である[1]．そのため，以下の 3 種類のゲート集合を万能なゲート集合と呼ぶ．本節では，量子回路のゲート数により量子計算量のクラスを定義するが，そこで使われるゲートは以下の 3 種類のゲートのみとする．万能なゲートの集合は複数考えられるが，入力数が定数のゲートを用いる限り，どのような万能なゲート集合を用いたとしても計算量の議論に違いは生じない．

トフォリゲート（Toffoli gate）　トフォリゲートは 3 量子ビットに次のように作用する操作である．$T:|a\rangle|b\rangle|c\rangle\mapsto|a\rangle|b\rangle|c\oplus ab\rangle$．

アダマールゲート（Hadamard gate）　アダマールゲートは 1 量子ビットに次のように作用する操作である．$H:|a\rangle\mapsto\frac{1}{\sqrt{2}}|0\rangle+\frac{(-1)^a}{\sqrt{2}}|1\rangle$．

位相ゲート（phase-shift gate）　位相ゲートは 1 量子ビットに次のように作用する操作である．$P:|a\rangle\mapsto i^a|a\rangle$．

上記の表記のなかで，a,b,c は 0 または 1 を意味する．一般の量子状態 $\alpha|0\rangle+\beta|1\rangle$ に対して

これらのゲートの操作を行った結果は，$|0\rangle$ 及び $|1\rangle$ にゲートの操作を行ったそれぞれの結果を α 及び β の重みで線形結合した量子状態となる．例えば，$\alpha|0\rangle + \beta|1\rangle$ に対してアダマールゲートを適用した結果の量子状態は，

$$\alpha\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \beta\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

となる．

6-4-2 量子計算量

もし量子計算機が実現すれば，BQP（Bounded-error Quantum Polynomial time）と呼ばれる計算量クラスに属す問題は（少しのエラーを許容して）現実的な時間で計算可能になると考えられている．BQP は，古典計算における BPP に対応するクラスであり，BPP を真に包含すると予想されている．例えば，素因数分解は BPP に属さないであろうと予想されているが BQP に属すことが Shor によって示されている[2)]．

決定問題のインスタンス x を量子回路の入力に与えた計算結果の量子状態において，ある決められた一つの量子ビットを観測したときに 1 を得た場合には x を受理，0 を得た場合には x を拒否するものとして，BQP は以下のように定義される．

定義 1 受理すべき入力列の集合が A_{yes} で，拒否すべき入力列の集合が A_{no} である決定問題 $A = (A_{yes}, A_{no})$ に対して，以下の二つの条件を満たすような多項式サイズの量子回路 Q が決定性チューリングマシンで多項式時間で生成可能な場合，$A \in \mathrm{BQP}(a, b)$ とする．ここで，a, b は $[0, 1]$ の任意の実数とする．

1. もし $x \in A_{yes}$ ならば，$\Pr[Q \text{ が } x \text{ を受理}] \geq a$.
2. もし $x \in A_{no}$ ならば，$\Pr[Q \text{ が } x \text{ を受理}] \leq b$.

このとき，計算量クラス BQP は，$\mathrm{BQP} = \mathrm{BQP}(2/3, 1/3)$ と定義される．

古典計算の場合と同様に，ある量子アルゴリズムの成功確率は，それを繰り返すことによりいくらでも増幅することが可能であるため，実際には上記の 2/3 の成功確率は 1/2 より大きい任意の定数であっても差し支えない．

定義より $\mathrm{BPP} \subseteq \mathrm{BQP}$ は自明であるが，それ以外に BQP に関して知られている主要な結果は以下の通りである．

- $\mathrm{BQP}^{\mathrm{BQP}} = \mathrm{BQP}$.
- $\mathrm{PP}^{\mathrm{BQP}} = \mathrm{PP}$.

BQP 以外にも多くの量子計算量クラスが定義されており，例えば，NP の量子計算への自然な拡張である QMA（Quantum Merlin–Arthur）[3)]等に関しても数多くの研究が行われている．

量子計算量に関する研究は，量子計算機の性能を現在の計算機の性能と比較することにつながるので，量子アルゴリズムの研究と同様に重要な研究であると考えられている．

■参考文献

1) M.A. Nielsen and I.L. Chuang, “Quantum Computation and Quantum Information,” Cambridge University Press, 2000.
2) P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comput., vol.26, no.5, pp.1484-1509, 1997.
3) A.Yu. Kitaev, A.H. Shen, and M.N. Vyalyi, “Classical and Quantum Computation,” American Mathematical Society, 2002.

■6 群 - 2 編 - 6 章

6-5 対話型証明系

（執筆者：小林弘忠）［2009 年 1 月 受領］

本編 5 章 5-1 で定義された計算量クラス NP は，適切な証拠を与えられれば誤りなしに効率よく検証できる問題のクラスと考えることもできる．一方，本章 6-3 の乱択計算の見地からは，誤りがあっても高い精度で検証できれば実用上十分であるといえる．この考え方を更に発展させ，“効率のよい検証” という概念を最大限に一般化したものが対話型証明である．本節では，計算量理論，及び現代暗号理論において中心的な役割を果たす対話型証明に関して概説する．

6-5-1 対話型証明

対話型証明（interactive proof systems）は**証明者**（prover）と**検証者**（verifier）の二者間の通信モデルとして定義される．証明者は全能であり，自分の主張の正当性を検証者に納得させるためには常に最適な戦略がとれる．一方，検証者は証明者に質問を繰り返し，その回答を基に証明者の主張の正当性を確率的に効率良く確かめようとする．より正確には，言語 L が対話型証明をもつとは，L に対する検証者の確率的多項式時間プロトコルが存在して，すべての入力 x に対し，$x \in L$ であれば，証明者のある戦略が存在して検証者に x を確率が 2/3 以上で受理させることが可能であり（完全性），$x \notin L$ であれば，証明者がいかなる戦略を用いても検証者が x を受理する確率は 1/3 以下となるような場合（健全性）をいう．

対話型証明は Goldwasser，Micali，Rackoff[6] により暗号理論的見地から，Babai[1] により組合せゲーム理論的見地から，独立に定義された．特に前者は現代暗号理論において重要な**ゼロ知識証明**（zero-knowledge proof systems）を同時に定義しており，その基礎となるモデルとして対話型証明を導入している．厳密には，Babai のモデルにおいては検証者は**公開コイン投げ**（public-coin）の結果のビット列のみを証明者への質問とし，それ以外の乱数は使えないという制約が課せられている．しかし，Goldwasser と Sipser[7] によって公開コイン投げモデルと一般モデルの能力の等価性が示されている．

対話型証明をもつ言語クラスは，当初は NP よりはやや大きいが co-NP を含むほどではなく，あまり大きくはないであろうと予想されていた．しかし，Lund，Fortnow，Karloff，Nisan[14] により導入された代数的手法を用いて，Shamir[17] は多項式領域計算量クラス PSPACE との等価性という対話型証明の驚くべき強力性を示した．一方，本編 5 章 5-3 の多項式時間階層が縮退しない限り，PSPACE に対する定数回の通信ラウンドの対話型証明は存在しないことも分かっている[1]．

6-5-2 多証明者対話型証明

Ben-Or，Goldwasser，Kilian，Wigderson[3] は**多証明者対話型証明**（multi-prover interactive proof systems）という非常に重要な対話型証明の変種を定義した．このモデルは本来暗号理論的見地から導入されたが，のちに 本編 7 章 7-2 で述べられる**確率的検査可能証明**（probabilistically checkable proofs）の概念を生み出し，**近似不可能性理論**（inapproximability theory）という新分野を開拓したことで特に有名である．多証明者対話型証明においては，検証者は複数の証明者と通信することにより検証を行う．各証明者はほかの証明者たちと物理的に隔離され

ており，証明者間の通信は許されない．このため，検証者は証明者間の矛盾をより容易に引き出すことができ，検証能力が高まると期待される．

Babai，Fortnow，Lund[2] はこのモデルが非決定性指数時間計算量クラス NEXP と同等の莫大な能力をもつことを示した．更に究極的には，Feige と Lovász[5] により 2 人の証明者に同時に 1 回の質問を送るだけの最も制限されたモデル（2 証明者 1 ラウンド対話型証明）が最も一般的な多証明者対話型証明と同等の能力をもつことも示された．2 証明者 1 ラウンド対話型証明の並列繰り返しにより受理確率を指数的に下げることができるか否かは大きな難問であったが，こちらも Raz[16] により肯定的に解決された．なお，多証明者対話型証明の公開コイン投げモデルは通常の単一証明者対話型証明と同等であることは自明であり，従って NEXP = PSPACE でない限り一般の多証明者対話型証明と同等にはならない．

6-5-3 量子対話型証明

対話型証明を本章 6-4 の量子情報の世界に一般化したものが**量子対話型証明**（quantum interactive proof systems）であり，Watrous[18] により初めて定式化された．量子対話型証明においては，検証者，証明者ともに量子的な操作を行うことができ，両者の間の通信にも量子通信が用いられる．証明者は物理法則に従う限りのすべての操作を行うことができるが，検証者は量子多項式時間で高い確率で正しく検証しなくてはならない．

Watrous[18] は PSPACE に対する 3 回の通信（1.5 ラウンド）の量子対話型証明を構成し，量子モデルの優位性を示す強い証拠を提示した．Kitaev と Watrous[12] は更に，3 回の通信の量子対話型証明に限定しても能力は変わらないこと，その能力は決定性指数時間計算量クラス EXP を超えないことなど，多くの重要な性質を示した．Marriott と Watrous[15] は量子対話型証明の公開コイン投げモデルを定義し，通常モデルとの能力の等価性を示した．Jain，Ji，Upadhyay，Watrous[9] は量子対話型証明の公開コイン投げモデルの能力が PSPACE を超えないことを示し，Marriott と Watrous[15]の結果と合わせ，検証可能な言語クラス自体は量子対話型証明と古典対話型証明で変わらないことを示した．

6-5-4 量子多証明者対話型証明

量子情報が多証明者対話型証明にどのような影響を与えるかはいまだよく解明されておらず，量子情報理論及び計算量理論における最重要課題の一つとなっている．多証明者対話型証明の量子版としては主に 二つのモデルが考えられている．一つは Kobayashi と Matsumoto[13] によって導入された**量子多証明者対話型証明**（quantum multi-prover interactive proof systems）と呼ばれるもので，検証者とすべての証明者に量子操作を許し，通信は量子通信であり，更に証明者間に任意の事前エンタングルメントを許す．もう一つは Cleve，Høyer，Toner，Watrous[4] により定義された**量子証明者多証明者対話型証明**（multi-prover interactive proof systems with entangled provers）で，検証者と通信は従来の古典モデルと変わらないが，証明者の量子操作と証明者間の任意の事前エンタングルメントを許す．証明者間の事前エンタングルメントは検証能力を強化する可能性を秘める一方，不正直な証明者らの事前エンタングルメントを用いた攻撃を考慮すると，古典モデルにおけるプロトコルの健全性証明が破綻する．

Kobayashi と Matsumoto[13] は正直な証明者らが超多項式個の事前エンタングルした量子ビットを共有しない限り，量子モデルは古典モデルの能力を超えないことを示した．Kempe，

Kobayashi, Matsumoto, Toner, Vidick[10] は NEXP や PSPACE に対するプロトコルにおいて，不正直な証明者らの無制限の事前エンタングルメントを用いた攻撃の限界を初めて与えた．Ito, Kobayashi, Matsumoto[8] は，PSPACE に属するすべての言語は不正直な証明者らに任意の事前エンタングルメントを許しても健全な古典 2 証明者 1 ラウンド対話型証明をもつことを示し，不正直な証明者らのみが量子情報を扱える場合でも多証明者モデルは単一証明者モデルに優ることを示す証拠を与えた．一方，Kempe, Kobayashi, Matsumoto, Vidick[11] は証明者間の事前エンタングルメントを検証者が有効利用できる可能性を初めて示し，量子多証明者対話型証明の公開コイン投げモデルが通常の量子多証明者対話型証明と同等の能力をもつという非常に興味深い性質のほか，任意の量子多証明者対話型証明は証明者数を増やすことにより 1 ラウンドまで並列化できることなどを示した．なお，事前エンタングルメントがない場合には量子モデルは古典モデルと能力が変わらないことが分かっている[13]．

■参考文献

1) L. Babai, “Trading group theory for randomness,” in Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing, pp.421-429, 1985.
2) L. Babai, L. Fortnow, and C. Lund, “Non-deterministic exponential time has two-prover interactive protocols,” Computational Complexity, vol.1, no.1, pp.3-40, 1991.
3) M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson, “Multi-prover interactive proofs: How to remove intractability assumptions,” in Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, pp.113-131, 1988.
4) R. Cleve, P. Høyer, B. Toner, and J. Watrous, “Consequences and limits of nonlocal strategies,” in Nineteenth Annual IEEE Conference on Computational Complexity, pp.236-249, 2004.
5) U. Feige and L. Lovász, “Two-prover one-round proof systems: Their power and their problems (extended abstract),” in Proceedings of the Twenty-Fourth Annual ACM Symposium on the Theory of Computing, pp.733-744, 1992.
6) S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof systems,” SIAM J. Comput., vol.18, no.1, pp.186-208, 1989.
7) S. Goldwasser and M. Sipser, “Private coins versus public coins in interactive proof systems,” in Randomness and Computation, volume 5 of Advances in Computing Research, ed. by S. Micali, pp.73-90, JAI Press, 1989.
8) T. Ito, H. Kobayashi, and K. Matsumoto, “Oracularization and two-prover one-round interactive proofs against non-local strategies,” in 24th Annual IEEE Conference on Computational Complexity, pp. 217-228, 2009.
9) R. Jain, Z. Ji, S. Upadhyay, and J. Watrous, “QIP = PSPACE,” arXiv.org e-print archive, arXiv:0907.4737, 2009.
10) J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick, “Entangled games are hard to approximate,” SIAM J. Comput., to appear. A preliminary version appeared in 49th Annual Symposium on Foundations of Computer Science, pp.447-456, 2008.
11) J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick, “Using entangled in quantum multi-prover interactive proofs,” Computational Complexity, vol.18, no.2, pp.273-307, 2009.
12) A. Kitaev and J. Watrous, “Parallelization, amplification, and exponential time simulation of quantum interactive proof systems,” in Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, pp.608-617, 2000.

13) H. Kobayashi and K. Matsumoto, “Quantum multi-prover interactive proof systems with limited prior entanglement,” J. Comput. System Sci., vol.66, no.3, pp.429-450, 2003.
14) C. Lund, L. Fortnow, H. Karloff, and N. Nisan, “Algebraic methods for interactive proof systems,” J. ACM, vol.39, no.4, pp.859-868, 1992.
15) C. Marriott and J. Watrous, “Quantum Arthur-Merlin games,” Computational Complexity, vol.14, no.2, pp.122-152, 2005.
16) R. Raz, “A parallel repetition theorem,” SIAM J. Comput., vol.27, no.3, pp.763-803, 1998.
17) A. Shamir, “IP = PSPACE,” J. ACM, vol.39, no.4, pp.869-877, 1992.
18) J. Watrous, “PSPACE has constant-round quantum interactive proof systems,” Theoretical Comput. Sci., vol.292, no.3, pp.575-588, 2003.